**(A1) Are We Safe?**

**Netwok System Security**

**Unit-9 Managing Network**

**Submitted to**

**SAGARMATHA NATIONAL COLLEGE**

**Sanepa, Lalitpur, Nepal**

**By**

**Biplov Shrestha (02)**

**Under the Guidance of**

**MR. Keshav Dulal**

**Faculty of BTEC, SNC**

**Hand Out Date:**

**Hand In Date:**

Scenario

You work for the IT support department of an organization. The managers have asked for a review of their network security procedures, starting with an overview of current threats and how to protect against them.

**Task**

* Describe how networks can be attacked
* Discuss recent network threats
* Describe how networked systems can be protected
* Explain the operation of different intruder detection systems

**Declaration**

This report has been prepared on the basis of my own work. Where other published and unpublished source materials have been used, these have been acknowledged.

Student Name: Biplov Shrestha

Date of Submission: 14/04/2017

**Task1**

**Describe how networks can be attacked**

Attack

In computer and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset. An attack usually is perpetrated by someone with bad intentions: black hatted attacks falls in this category, while other perform penetration testing on an organization information system to find out if all foreseen controls are in place. Some attacks are physical like theft or damage of computers and other equipment. Others are attempts to force changes in the logic used by computers or network protocols in order to achieve unforeseen (by the original designer) result but useful for the attacker. Software used to for logical attacks on computers is called malware.

Some of the attacks are explained bellows: -

DOS

Also known as Denial of Service is a type of an attack that is done to make network service unavailable or disable of any company. This is basically done to shut down a servers, websites or normal servers. When attacker sends number of request that limits the server and other clients can’t access it. When the large amount of useless data is sent to the network it overloads and flood the network to a point that it slows down and would not be able to handle the traffic and crashes as it cannot handle the amount of traffic. These attacks do not provide any benefit to an attacker, but if server of a big company goes down it can damage the reputation of the company and it will also cost a lot of money to fix.

DDOS

Distributed Denial of Service is pretty much similar to DOS attack however this attack can be done is many different ways. Like sending too many mails to upload to a large number of files. This attack is done by someone infecting many computers with a zombie virus and turning it whenever they want to bring down a network by using all of the infected computers which will add extra traffic to the attack.

BACKDOOR

When attacker infects the system of client’s or member of a company to hack and get access of the servers.

BRUTEFORCE

This is an attack where hacker uses numbers of passwords till the correct password is found. This attack usually takes long time to finish because without the proper information of any characters used in the password and also the longer the password, the longer it will take to crack the password. This attack can be prevented by limiting the amount of password trial.

**Task2**

**Discuss recent network threats**

Ransomware

Ransomware is an attack where hackers infiltrate your system or network and then encrypt your files and information, then hold the data as a hostage until their requirement or payment has been extorted. The present day ransomware can not only hack your machine more profoundly but it can also infect numbers of machines at a time. The ransomware of 2017 has the capability to lock out whole small groups and absolutely freeze up full departments of massive businesses.

This new ransomware is spread between customers like the common cold. Instead of concentrated on a singular source, the ransomware infects then germinates, inflicting a chain response of infection. As one hacked computer interfaces with another, the ransomware spreads. Often, ransomware cloaks itself in mundanity to surpass your network security: it arrives unassuming as an electronic mail attachment or a shared link. Once the email has been opened, or the link has been followed, the ransomware has invaded. Be cautious when opening suspicious emails or clicking funky links: you don’t choose your essential information to be taken or held for ransom.

Some of the latest ransomware attacks are-

**Petya/NotPetya/Nyetya/Goldeneye (June 2016)**

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system.

**WannaCry (May 12th 2017)**

WannaCry leveraged a vulnerability in Windows OS, first discovered by the NSA, and then publicly revealed to the world by the Shadow Brokers. In the first few hours, 200,000 machines were infected. Big organizations such as Renault or the NHS were struck and crippled by the attack.

**Cloudbleed (February 2017)**

On February 17, 2017, the "Cloudbleed" security bug was discovered. This bug affected Cloudflare's CDN product, which is used by millions of websites. For any websites that use Cloudflare, it is possible that users' private data may have been exposed to the public, including passwords, personally identifiable information, credit card numbers, etc.

Botnets

A botnet is a collection of internet-connected devices, which may also include PCs, servers, mobile devices and internet of things devices that are contaminated and controlled through a common type of malware. Users are regularly unaware of a botnet infecting their system. The term botnet is derived from the words robot and network. A bot in this case is a device infected with the aid of malware, which then turns into part of a network, or net, of infected units controlled by a single attacker or attack group.

One of the latest botnet attack is: -

**BetaBot (Malware) (2017April)**

Beta Bot is a Trojan that infects computers and attempts to prevent users from accessing security websites while also disabling their antivirus and malware scan software. To accomplish this, the bot creates a pretend Microsoft Windows message field with the heading "User Account Control." It asks users to allow the "Windows Command Processor" to make administrator-level changes, and claims it is verified by way of Microsoft. If changes are approved, Beta Bot modifies a user's pc to steal log-in credentials and economic records whilst additionally disabling protection software program access.

**Task 3**

**Describe how networked systems can be protected**

Prevent ransomware attacks

As mention above it is an attack where hackers infiltrate your system or network and then encrypt your files and information, then hold the data as a hostage. So what we can do to protect our files and data is: -

When Using system

* Not storing important data only on system, we can store either on external drives or in the cloud (Dropbox – Google Drive).
* Also keeping security software’s up to date.
* If we are using browsers removing the plugins from the browsers and setting the rule like asking if you want to activate the plugins.
* Using increased protections for browser’s security and privacy settings
* Only keeping the ones that used on a daily basis and keeping them updated to the latest version.
* Using an ad-blocker to avoid the threat of potentially malicious ads.

When Using Internet

* Not opening spam emails or emails from unknown senders.
* Not downloading attachments from spam emails or suspicious emails.
* Try avoiding click links in spam emails or suspicious emails.

Using Anti-ransomware security tools

* Using a reliable, paid antivirus product that includes an automatic update module and a real-time scanner.
* Having some knowledge of a traffic-filtering solution that can provide proactive anti-ransomware protection.

Prevent BetaBot (Malware) Attacks

As we know that botnet is malware that controls the internet-connected devices. But it is easier to prevent it from being infected and letting it be a part of a botnet then it is to detect when it’s too late and try to save it. So what we can do to prevent it is to follow simple rules: -

* Keeping all your software’s up to date which can lock out 65% of attack vectors that target the applications.
* Making sure that firewall is on and setting it to maximum security level.
* Having a good antivirus and antispyware software from well-known source.
* Checking if unusual internet activity like high network usage.

**Task4**

**Explain the operation of different intruder detection systems**

IDS

In network security no other tools are valuable as Intrusion Detection. The ability to locate and identify malicious activity on network by examining network traffic in real time which gives you visibility unravel by any other detective control. IDS are available in Network and Host forms. HOST dictation is installed as an agent on a machine which you wish to protect and monitor. NETWORK IDS examines traffic between host looking for patterns or signatures and anomaly baseline. There are two types of IDS active/reactive, one which keeps log and takes actions (it shut down when someone force or is bombarded by threats), or passive, which only keeps the log for user to monitor (if user does not check then threats can pass through). Some of the known IDS software’s are SNORT and ALIEN VAULT

SNORT

Snort is a free and open source network Intrusion Detection System. It has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three fundamental modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will examine community packets and display them on the console. In packet logger mode, the software will log packets to the disk. In intrusion detection mode, the program will screen community traffic and analyze it towards a rule set described by the user. The program will then perform a precise action based on what has been identified.

Firewalls

Firewalls are designed to prevent unauthorized get admission to a pc or network. You can put in force a firewall in both hardware and software, or a mixture of both. A firewall will reveal records packets coming in and out of the community it is defending and will put into effect the company's community protection policy. It filters out the packets that appear suspicious and do not meet the unique security criteria. Most companies use firewalls to guard their community from the Internet.

There are a few different types of firewall, these are:

* Packet Filtering Firewall
* Stateful Inspection Packet Filtering Firewall
* Proxy Firewall

Refrence

<https://www.networkdepot.com/top-7-threats-network-security-2017/>

<https://heimdalsecurity.com/blog/what-is-ransomware-protection/>

<https://en.wikipedia.org/wiki/Snort_(software)>