# COM 5335 : NETWORK SECURITY ASSIGNMENT#2

108064535 陳文遠 WEN-YUAN CHEN (Chris)

## ● Part 1. Researching Network Attacks

In Part 1 of this assignment, you research various network attacks that have actually occurred and select one on which to report. Fill in the form below based on your findings.

### - Step 1 : Research various network attacks.

The following table list some kinds of attack that I find in my research.

| Table 1. Some common network attacks | |
|---|---|
| **Type of attack** | **List of attack** |
| **Denial of service** | 1. TCP SYN (SYN Flood)<br>2. Smurf Attack<br>3. Ping of Death<br>4. LAND Attack<br>5. Teardrop Attack |
| **Malware computer program** | 1. Computer Worm<br>2. Computer Virus<br>3. Trojan Horse |
| **Spoofing attacks** | 1. ARP Spoofing → Will be discussed below<br>2. IP Address Spoofing<br>3. MAC Spoofing |
| **Others** | 1. Session Hijacking<br>2. Buffer Overflow<br>3. SQL Injection |

In this step, I just only list the term of some kinds of network attacks, but in the next step, I will choose one attack situation from the table1 to detail its relative information.

- **Step 2 : Fill in the following form for the network attack selected.**

| Table 2. The details of ARP Spoofing | |
|---|---|
| **Name of attack :** | ARP Spoofing |
| **Type of attack :** | A malicious actor sends falsified ARP messages over a local area network. |
| **Dates of attacks :** | March 2019 |
| **Computers / Organizations affected :** | The home page of Taiwan MSN website was attacked by forwarding. |

**How it works and what it did :**

✎ **How it works ?**

Network devices always send ARP request broadcast packet to LAN to ask for the corresponding information of IP and MAC address. Hacker receives the packet, he(she) will try to counterfeit the packet and throws it back to LAN again. When network devices receive the forged ARP reply, they will amend their own ARP table. The result will be an ARP table information error.

✎ **What it did ?**

1. If hacker receive the ARP request and discard it rather than send it back to LAN, the network devices will disconnect the internet.
2. If hacker receive the ARP request and send it back to LAN, he(she) will can eavesdrop on network devices.

**Mitigation options :**

1. The idea method to do the protection is to change the ARP of each computer to static, but it doesn't work in big network architecture because it need to usually update the ARP table of each computer.

2. Another method is to use DHCP snooping. Network devices can put aside the MAC address of every computers in the network. Then they can detect the exception when someone sends forged ARP packets.

3. Also, there has some software can monitor ARP reply from network. If the software detect some abnormal changes, it will send message by such as email.

**References and info links :**


[1] My own paper : https://drive.google.com/open?id=18T2mlb7a5YTckWAk3vK7lA4-3mvXDO1k

[2] The home page of Taiwan MSN website was attacked by forwarding : https://www.ithome.com.tw/news/96787

[3] ARP spoofing : https://en.wikipedia.org/wiki/ARP_spoofing

## Part 2. Researching Security Audit Tools

In Part 2 of this assignment, you research network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

### - Step 1 : Research various security audit and network attack tools

| Table 3. Security audit and network attack tool | |
|---|---|
| **Type of tool** | **Name** |
| **Security audit tools** | 1. Namp (Network Mapper)<br>2. Comodo HackerProof<br>3. OpenVAS<br>4. Nexpose Community<br>5. Nikto<br>6. Tripwire IP360<br>7. Wireshark<br>8. Aircrack<br>9. Nessus Professional<br>10. Retina CS Community |
| **Network attack tools** | 1. Dsniff<br>2. Metasploit Framework<br>3. Ettercap<br>4. Sslstrip<br>5. Evilgrade<br>6. Sqlmap<br>7. Aircrack-ng<br>8. Cain and Abel<br>9. OclHashcat<br>10. Ncrack |

- **Step 2 : Fill in the following form for the security auditor**

| Table 4. One of security audit tools | |
|---|---|
| **Name of tool :** | Nmap (Network Mapper) |
| **Developer :** | Gordon Lyon |
| **Type of tool (character-based or GUI) :** | Character-based (Command Line Interface) |
| **Used on (network device or computer host) :** | Both network device and computer host |
| **Cost :** | Open source (Free) |
| **Description of key features and capabilities of product or tool :** | |
| Nmap is a go-to software for network managers. It can be used to scan some information such as host, port, type of service, operation system, type of device and so on. Nmap can scan not only single device but also whole computer network, then you can analyze the scanned information to find the vulnerabilities. | |
| **References and info links :** | |
| [1] Nmap Github : https://github.com/nmap/nmap<br>[2] Nmap.org : https://nmap.org/download.html<br>[3] My own paper : https://drive.google.com/open?id=18T2mlb7a5YTckWAk3vK7lA4-3mvXDO1k | |

- **Step 3 : Reflection**

**a. What is the prevalence of network attacks and what is their impact on an organization's operation? What are some key steps organizations can take to help protect their networks and resources?**

Due to the progress of network, network attack events occur every day. Small losses may lose some unimportant data, but large losses may lose several thousands of dollars. The First step that organizations can take is to activate both hardware and software firewalls protect your computer and don't open unclear files or links. The second step is to utilize some famous security audit tools that I mention above to help you ensure the network security.

**b. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact to the organization and what did they do about it?**

Take my laboratory, WCIS Lab as an example, our server was hacked and changed the root password a few weeks ago. Although It didn't cause large losses, but it also brings us trouble. In case we have some important information or data in that server, it will cause a lots losses.

**c. What steps can you take to protect your own PC or laptop computer?**

The following steps I will take to protect my personal devices :

1. Use firewall
2. Regularly update the operation system
3. Check ports if be monitored by someone or not.
4. Use the security audit tools I mentioned above.
5. Avoid opening unclear files or links.
6. Use static DHCP to avoid someone changing my ARP table.