**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) 2. Smurf Attack 3. Ping of Death 4. LAND Attack 5. Teardrop Attack |
| Malware computer program | 1. Computer Worm 2. Computer Virus 3. Trojan Horse |
| Spoofing attacks | 1. ARP Spoofing 🡪 Will be discussed below 2. IP Address Spoofing 3. MAC Spoofing |
| Others | 1. Session Hijacking 2. Buffer Overflow 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 ? * What it did ? | |
| **Mitigation options :** | |
| 1. The idea method to do the protection is 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 in big network architecture. | |
| **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.
* Step 2 : Fill in the following form for the security auditor network attack tool selected.
* Step 3 : Reflection

1. 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?
2. 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?
3. What steps can you take to protect your own PC or laptop computer?