Assignment 2 – System and Network Security (CYBR 371)

Due Date – 09/05/2021

1. Follow the instructions in this document.
2. Write answers to the questions in the order they appear in a separate document file (full name-studentid.pdf) e.g. 1A, 1B, 1C, 2, 3, 4….8A, 8B…
3. **Write the answers using technical terms. Avoid vague (and mostly true) statements such as: Firewalls can protect a network by blocking attackers!**
4. For the programming questions provide:
    a. Scapy code with comments.
    b. Steps taken to launch the attack.
    c. Screen shots of the attack.
5. In the context of this assignment, please pay attention to the following keywords and answer accordingly. Please refer to the marking criteria for more information.
    a. **List**: a simple list of answers with minimum explanations.
    b. **Briefly**: Provide the answer in minimum 1 -2 summarised lines (can be longer if you need).
    c. "**Explain**", "**Describe**", "**Explain in detail**": Provide the answer in minimum 1- 2 paragraphs (can be longer). You may also include diagrams or figures for improved clarification.
    d. **Demonstrate**: Explain using a combination of steps, figures, diagrams and screenshots.
6. Submit the file using the ECS submission system. https://apps.ecs.vuw.ac.nz/submit/CYBR371

*** It is a student's responsibility to manage their time and workload. Please make sure to start this assignment early and submit on time. Additional extensions will **only** be granted due to **EXTREME** circumstances, which does not include workload due to other courses, cold or flu in 2 weeks leading to the submission deadline, work and family commitments etc.

Part 1: Network Attacks and Vulnerabilities (56 Marks)

Following the instructions in the attached **3VMSetup.pdf** document, create three virtual machines on your system and complete the following tasks. Your demonstration must include the following:

- The topology of your environment including Host name, IP and MAC addresses of each VM.
- The tools and commands used in the process with a brief description of each tool/command.
- List of the steps taken to produce the results.
- A screenshot to confirm the results.

1. [**14 Marks Total**] Demonstrate ARP cache poisoning attack using the following ARP messages. (Note: For ARP response and Gratuitous message attacks to work, the target machine(s) should already have an ARP entry for the victim machine).

    A. [**6 Marks**] ARP response message
    B. [**6 Marks**] ARP Gratuitous message
    C. [**2 Marks**] There are multiple ways (direct and indirect) to create an ARP entry into ARP cache). List two methods to create and maintain an ARP entry in the target machine(s).

2. [**6 Marks**] Demonstrate Man-In-The-Middle attack using session hijacking where an attacker captures the existing session between two machines on a local network and creates a folder with their name in the target machine.

3. [**4 Marks**] Explain in detail, how session hijacking from within a LAN is different from session hijacking by a remote attacker?

4. [**4 Marks**] List four methods by which session hijacking can be prevented and, explain two in detail.

5. **[4 Marks]** Many attacks on the TCP/IP stack exist because of assumptions that no longer hold for the modern Internet. Describe two attacks (excluding encryption but can be of any protocol) and identify which assumptions make these attacks possible.

    e.g. *Encryption*
    Assumption: Internet is secure
    Attack: Telnet is a plain-text protocol which means the data between the two communicating parties is transferred in clear text, including the login credentials. This

allows an attacker to potentially perform a man in the middle attack by capturing the traffic between the two communicating devices and extract the login credentials.

6. **[4 Marks]** Explain the term “Backscatter traffic” and why it is generated by some but not all types of Distributed Denial of Service DOS attacks.

7. **[8 Marks]** Imagine you are an attacker who wishes to launch an Amplification attack on a target host, but you do not want to utilise DNS servers. List and explain four criteria to select an alternative set of servers to utilise in your attack?

8. **[12 Marks Total]** In a TCP SYN flooding attack, the attacker’s goal is to flood and fill the TCP connection requests table of a target system. If the table is filled, the target system is unable to respond to legitimate connection requests.

   Consider a target system with a table which holds 512 connection requests. The target system will retry to send the SYN-ACK packet (In response to Attacker’s SYN packets) 5 times if it fails to receive an ACK packet in response. Each retry SYN-ACK packet will be sent at 15 second intervals. If no replies are received, it will purge the request from its table. Assume that the attacker has already filled the TCP connection request table on the target with an initial flood.

   A. [**2 Marks**] At what rate must the attacker continue to send TCP connection requests to the target in order to make sure that the table remains full? Provide the answer with the necessary calculations.
   B. [**2 Marks**] How much bandwidth does the attacker consume to continue this attack, if each TCP SYN packet is 80 bytes in size? Provide the answer with the necessary calculations.
   C. [**8 Marks**] What countermeasures can be used to minimise or mitigate TCP SYN flooding attacks? list two and explain each in detail.

Part 2 Firewalls and Proxy Servers [34 Marks]

9. [**14 Marks Total**] As a system/network engineer you have been asked to create a firewall ruleset for a Server. The server has the following services and characteristics:
    - Operating system: Ubuntu 20.04.2 LTS
    - Server's IP address: 10.10.4.1/24
    - Clients' networks: 10.10.5.0/24, 10.10.6.0/24, 10.10.7.0/24, 10.10.8.0/24
    - Update server: us.archive.ubuntu.com Port 80
    - Services: SSH, Apache and PureFTPd

    Requirements:

    a. Provide service for clients' incoming FTP requests.
    b. Provide service for clients' incoming HTTP and HTTPS requests. Drop inbound traffic to port 80 (http) from source ports less than 1024.
    c. Protect the server against ICMP ping flooding.
    d. Provide remote SSH service for administrator from a remote system with an IP address of 10.10.8.1/24
    e. Protect the server against SSH dictionary attack.
    f. Drop all incoming packets from reserved port 0 as well as all outbound traffic to port 0.
    g. The server is not allowed to create any new outgoing connections, except for the installation of security updates.

    A. [**7 Marks**] Create a firewall policy table using the information above
    B. [**7 Marks**] Write the appropriate set of iptables (Netfilter) rules to fulfil the requirements

10. [**2 Marks**] Write an iptables rule to direct all the DNS requests from your internal network to Google's 8.8.8.8 IP address and associated port.

11. [**2 Marks**] Briefly explain why the DROP default policy is recommended in a Packet filtering firewall such as iptables.

12. [**4 Marks**] Write a Squid proxy rule to authorise clients in the 10.10.7.0/24 subnet to access the Intranet website (i.e. ecs.vuw.ac.nz), by prompting for their username and passwords. The usernames and passwords are matched against a file on the local drive. For instance, if David and James are legitimate users with proper credentials, they system should only grant them access if they provide proper user name and password and only if they are connecting to the proxy from the client's 10.10.7.0/24 subnet. The username and passwords are kept in the following file: *~/usernames.txt* . Squid should also log each authentication attempt.

13. [**2 Marks**] Write a Squid rule to block HTTP access to clients accessing a list of domains, during peak hours. The peak hours are between 9-11 am and 2-5 pm during Weekdays and 8-10 am on the weekends. The rule should block any websites having any instance of the words (i.e. lower letter and UPPER LETTER). The domains are stored in the file: "*~/blockeddomains.txt".* The Clients' subnets are: 10.10.5.0/24, 10.10.6.0/24, 10.10.7.0/24 and 10.10.8.0/24

    e.g. blockeddomains.txt
    www.youtube.com
    Youtube.com
    http://facebook.com
    FACEBOOK.com
    faceBook.com

14. [**2 Marks**] Write a rule to block a client with a specific MAC address (i.e. 12:34:56:78:9A:BC) from downloading .exe files. All other clients must be able to download .exe files.

15. [**8 Marks**] Explain the capability and the process (i.e. procedure/steps) by which popular packet filtering firewalls such as iptables can be used to reduce the speed **slow down** (NOT stop!) the spread of worms and self-propagating malware?

Grading Criteria

The criteria for grading are:

- Completeness – Did you complete all the tasks and **how comprehensively**? There is no word limit to the report. You are encouraged to include diagrams with brief explanations where (if) necessary. Example:
    - Did you name the right firewall feature and explain how it manages to achieve it with detailed technical information?
- Accuracy - How well did you complete the tasks? Did you use the right terminologies?
- Presentation - Did you use the right terminology? Please check for readability, we mark a lot of these and generally we look more favorably on well-structured and well-written ones.

Letter grades

A-range:

Complete, accurate, and well presented. Shows excellent knowledge and understanding of concepts and terminologies. Well-argued. Where required, contains good original input from the student.

- Example. Code is documented and well structured.

B-range:

Mostly complete, mostly accurate, and well presented. Shows a good knowledge and good understanding of the methods but either fails to complete some parts of the tasks or is unclear or is poorly argued.

C-range:

Satisfactory performance although some errors in accuracy and/or problems with presentation. Shows only some basic knowledge of the material or fails to understand some important parts of it, or does not provide solutions to a significant portion of the tasks.

D-range:

Poor performance overall, some evidence of learning but very problematic in all aspects mentioned above.

E-range:

Well below the required standard.