Networking Tools & Port Scanning

Overview

In this lab session you will be introduced to computer networks. The aim of the lab is to provide a practical overview of how computers communicate via networks. A more advanced unit on computer networks is studied as a part of Computer Networks and Operating systems on some pathways.

In addition to introducing the fundamentals of computer network communication, this lab session introduces the concept of a basic vulnerability assessment. Vulnerability assessments identify potential vulnerabilities in computer networks, to enable remedial action to be taken, ideally before the vulnerabilities have been exploited.

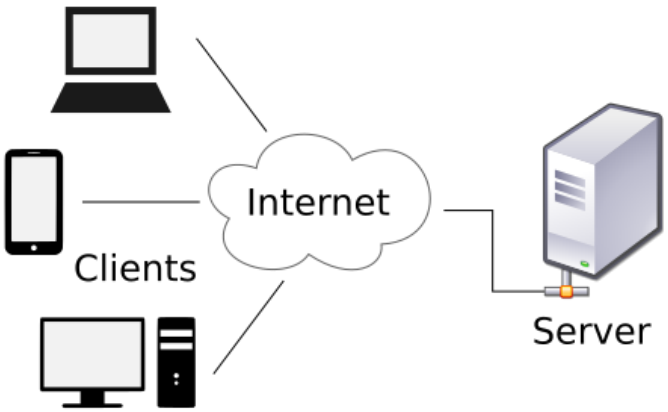
Learning Outcomes

Upon completion of this lab you will be able to:

1. Identify the network interfaces on a computer
2. Use tools to analyse the structure of packets, and describe the basic components of a packet
3. Use network tools to transfer data between hosts via a network
4. Use industry standard tools to identify vulnerable computer systems on a network

Task 1 – The Client Server Model

The client server model is a fundamental model for network communication. Clients communicate with servers, typically via the Internet (or local area network).



Client Server Model

By Gnome-fs-client.svg: David VignoniGnome-fs-server.svg: David Vignoniderivative work: Calimo (talk) - Gnome-fs-client.svgGnome-fs-server.svg, LGPL, https://commons.wikimedia.org/w/index.php?curid=15782858

Clients send requests to servers, who reply with responses. The type of request and response varies from protocol to protocol. However, the basic request/response model remains the same;
An application on the server listens on a predefined port number for a request from a client, and provides a response based on the request, and processing by the application on the server. This combination of an application and port is known as a service.

The most commonly used service on the Internet is web browsing. Client machines use a web browser, to request web pages from a web server on port 80. Servers can host many applications simultaneously (there are 65535 ports available).

To demonstrate the client server model, you will browse the website served by metasploitable, using the Kali virtual machine.

1. Start both the Metasploitable and Kali virtual machines.
2. Determine the IP address of the Metasploitable virtual machine.
3. Open a web browser on the Kali virtual machine and input the IP address of the Metasploitable virtual machine in the address bar.
    a. Research what DNS is, and how it is used.

Research the RFC 4253 and explain what it used for. The Metasploitable virtual machine is running an SSH (Secure Shell) service, you will use this service to upload a file to the Metasploitable virtual machine using SCP (Secure Copy).

The Apache server on Metasploitable serves files stored in /var/www/ to clients. You will use SSH to access the Metasploitable virtual machine, and copy the file you uploaded via over SCP to this directory.

1. On the Kali virtual machine open a terminal and;
    a. Create a file with your name as the file name and .html as the extension.
    b. Use SCP to copy the file to the Metasploitable virtual machine e.g.

```
scp rob.html msfadmin@METASPLOITABLE_IP_ADDRESS:/home/msfadmin
```

    c. ssh onto the Metasploitable virtual machine:

```
ssh msfadmin@METASPLOITABLE_IP_ADDRESS
```

    d. Move the file you created to /var/www using admin privileges:

```
sudo mv rob.html /var/www/
```

2. On the Kali virtual machine open the web browser and input the IP address of the Metasploitable virtual machine in the address bar, followed by the filename of the file you uploaded to the web server e.g:
    a. http://10.0.2.6/rob.html

Task 2 – Identifying Vulnerable Machines on a Network

Port scanning is a technique used to identify hosts with open ports on a network. Open ports on servers are used to provide services, they provide access to the applications running on the server. The presence of open ports can be used to profile a system, and with further probing (grabbing banners from ports) it is possible to identify weaknesses in a system or the services hosted by the system. You will use a port scanner to identify vulnerable services on the Metasploitable VM.

1. Start your Metasploitable virtual machine and login using msfadmin for both the username and password.

2. Access the man page for nmap using the following command "`man nmap`" From the man page identify how you can display the software versions of running services identified by a scan.
    - Tip: Look for the Service/Version Detection heading.

3. Use the following resource to learn more about port scanning:
    - http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3

4. Conduct a port scan against localhost 127.0.0.1 on your Metasploitable virtual machine, limit the port scan to the first 100 ports using the -p parameter.

5. Once the scan has complete search the CVE website https://www.cvedetails.com/ for one or more of the services running on the machine and identify a vulnerability. Some of the explanations will be very technical, take some research the meaning of the explanations, relate the what you find to either confidentiality, integrity, and/or availability.

6. Repeat the above proves from your Kali virtual machine, by targeting the IP address of the metasploitable virtual machine. Explore the additional tools provided by Kali for this task, see what results they generate.

Task 3 - Analysing Packets Using Wireshark

Research IP addresses, MAC Addresses, and packets. Document your findings. Wireshark is a tool used to capture and analyse network traffic. It allows the user to view the IP addresses, MAC addresses, protocols and packets used to transmit data via a computer network.

It is an offence under the computer misuse act to capture packets from a network without permission from the owner and/or users of the network.

1. Start Wireshark on the lab computer and download the packet capture from Moodle.
2. Open the packet capture supplied on Moodle and review the contents of the capture. The capture contains a naïve port scan. Describe how you would identify such a port scan, make a note of its key features.

Extended Task / Homework

Document the vulnerabilities discovered of the virtual machine, explain the likely impact they would have on a business and consider how they could be mitigated.