

6G4Z1104: Computer Forensics and Security Fundamentals

Coursework 1

Karan Nihalani, 17023122

Contents

Task 1 – Multiple Choice Exam	2
Task 2 – System Audit	2
Computer Misuse Act 1990	2
Port Scanning & the TCP Handshake	2
Vulnerability Assessment of Metasploitable Virtual Machine	2
Common Vulnerabilities and Exploits Identified	3
Task 3 – Mitigation.....	3
Firewalls Background	3
IP Tables Background and Deployment	4
Additional Mitigation Approaches	5
References	7

Task 1 – Multiple Choice Exam

Remember to attend your scheduled lab sessions on the week commencing 23rd October 2017.

You will undertake a multiple-choice exam, based on the content covered in the unit to date. You may remove this text.

Task 2 – System Audit

Computer Misuse Act 1990

This Act was developed in 1990, and is used to allow citizens with access to technology to prepare beforehand for securing computer data, facing unauthorized access, attacks or changes to the computer data. Offences normally include “Unauthorized access to computer material”, “Unauthorized acts causing, or creating risk of, serious damage”, and even acts with the idea to “impair” the functionality of a computer (Crown, 2008).

Virtualization can prevent breaches and even accidental ones, as we were able to or allowed to only use our local IP address, minimising the probability of creating a breach on another machine. This is only if they have been configured in the correct manner and due to its flexibility, allowing systems to be shared, not having to expose “critical information across the systems” (J. Kizza, 2015).

Port Scanning & the TCP Handshake

Port Scanning is a method that is used to detect and “identify the open ports”, (Palo Alto Networks, Inc., 2017) and other different services accessible on a computer network. They can be performed from outside or inside a specific tested network. The main goal of port-scanning is to find out whether ports in a network are open, filtered or closed. Performing the port scan, you can try and clarify the vulnerabilities in the system’s network, for the system to be “patched.”

The mechanisms normally employed by port-scanners are TCP (J. Postel, 1980) (and/or UDP (J. Postel, 1980)), as they’re “the transport mechanism used by such applications as FTP, Simple Mail Transfer Protocol (SMTP), Dynamic Host Configuration Protocol (DHCP) and HTTP,” where TCP tends to be more reliable when connecting two hosts, in contrast with UDP, a “connectionless protocol,” which means that it doesn’t ensure that the data packets have reached their correct ports or destination. (A. Whitaker, D. Newman, 2006).

A TCP handshake is traditionally performed in three steps. The first step is usually when one computer (Computer A) sends a SYN request to the other computer (Computer B). Once this is done, Computer B acknowledges the request and sends back an ACK, setting up a SYN flag, as well. Finally, the third and final step is when Computer A acknowledges the SYN flag by Computer B, sending back an ACK to the other computer. A way the TCP 3-way handshake is misused by port-scanners using a SYN scan. It’s a more sly approach, sending the SYN request to the server and the server responding with the SYN-ACK, only if there is an open port. An RST is sent back if the port is closed, making sure that the connection is dropped; therefore, the SYN method goes undiscovered by some firewalls.

Vulnerability Assessment of Metasploitable Virtual Machine

Below, in Fig.1, we can see a screenshot, demonstrating a port scan carried out, utilising nmap, allowing to scan the network (G. Lyon, 2011) on the localhost, using the local IP address and, where the results specify the number of ports open after performing the port scan, using the Metasploitable Virtual Machine. Here, the port scan is carried out for the first one hundred ports on the local network only, using 'localhost' as the domain, as we don't want to access any other ports

outside of our network. We can also observe the different services of the various ports in the network, such as, FTP (A.K. Bhushan, 1971), SSH (S. Lehtinen, C. Lonvick, Ed., 2006), Telnet (J.T. Melvin, R.W. Watson, 1971), SMTP (D. Mills, 1992) and HTTP (T. Berners-Lee, R. Fielding, H. Frystyk, 1996). Out of the 100 ports, 95 of them are closed and only these 5 are left open.

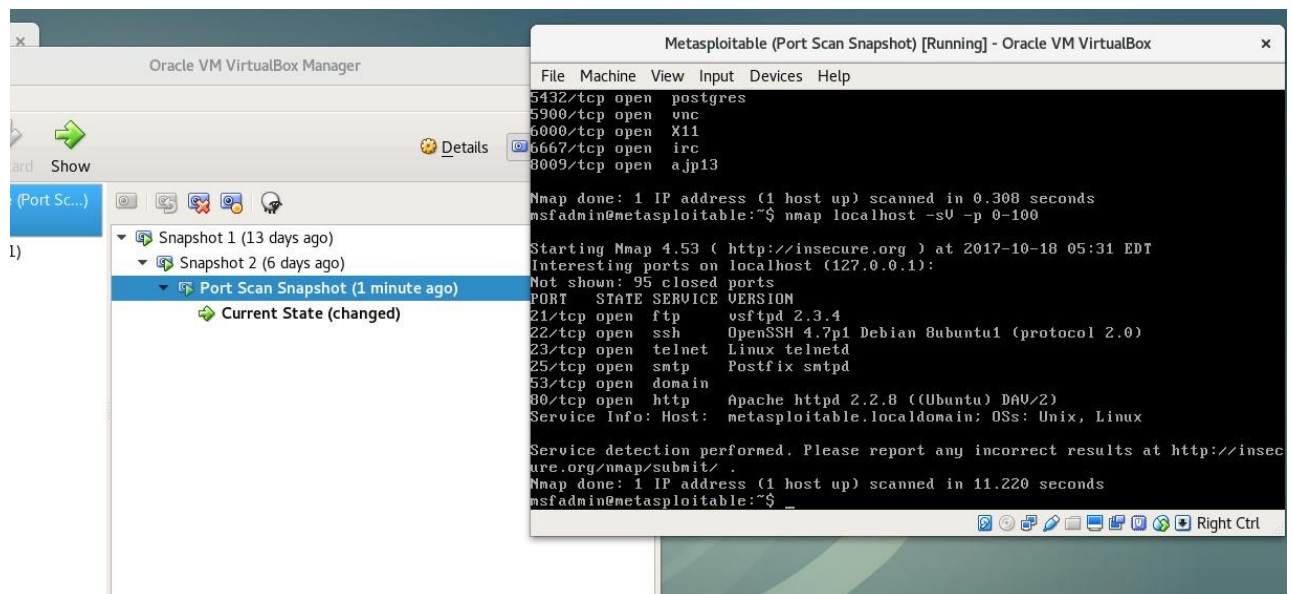


Fig.1

Common Vulnerabilities and Exploits Identified

One of the services identified is the 'HTTP Apache httpd 2.2.8,' which permits hackers or attackers to read data that is normally kept secret from the process memory of a system. The attacker would send an unauthenticated HTTP request, in order to gain access to read certain "secret data." It is clear that this vulnerability allows there to be a "partial impact" to the system, when talking about Confidentiality, as "there is considerable informational disclosure." (The Mitre Corporation, CVE-2017-9798, 2017) Although there is a breach in Confidentiality, there isn't any impact at all to the Integrity and Availability to the system. Businesses, here, would have to implement methods of cryptography to cipher the data and access control, preventing attackers from viewing information.

Another service identified is the 'FTP vsftpd 2.3.4,' which "allows users to cause a denial of service." There isn't any effect on the Confidentiality and Integrity of the whole system, although there is a slight consequence on the Availability, as the Availability for resources and the system's performance is decreased or disrupted. Business would have to use the approach of disk redundancies, an example being RAID, where data would be stored in many hard disks for future data protection and making use of Firewalls and its iptables allow there to be a higher level security and mitigating these vulnerabilities would be much easier to perform.

Task 3 – Mitigation

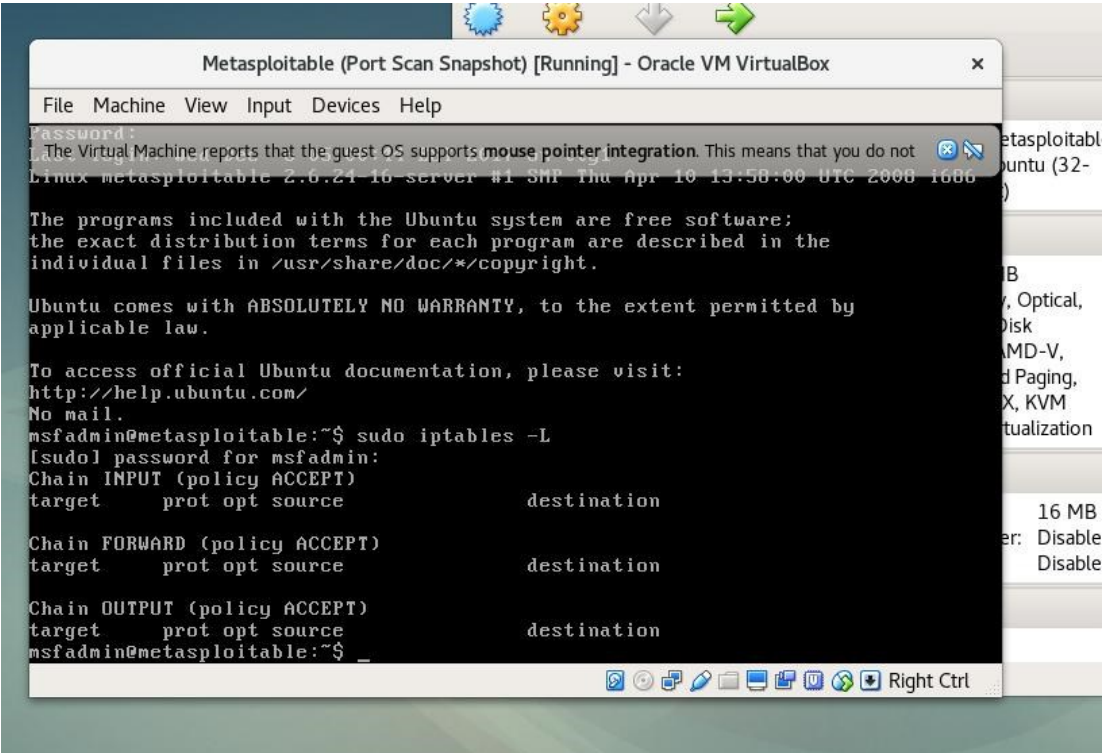
Firewalls Background

Firewalls are hardware or software devices used to "monitor incoming and outgoing network traffic", (Cisco, 2017), using a specific set of in-built rules, in order to be able to block malicious software from corrupting a computer system. The firewalls are able to "block all traffic to and from a particular IP address," (Microsoft Technologies, 2017), only if the IP address is known.

To be able to help improve security, they tend to use different kinds of filters, the most common one being the domain name filter, allowing certain domain names to be blocked or been given conditional access. Furthermore, a firewall could be configured more in depth, as it is able to restrict access to other network protocols, such as, TCP, UDP, HTTP, etcetera, on the user's network it's guarding.

IP Tables Background and Deployment

IP Tables are basically used to be able to control the traffic of data packets to and from the ports on that system's network. Fig.2, shows the command, "sudo iptables -L" to demonstrate the IP Tables you could make use of to filter out ports, Fig.3, displays a screenshot of the port scan before the ports had been filtered out and only port 80 was left open and in Fig.4, a screenshot of a port scan is shown after the iptables rules to drop all the ports, except for port 80 had been implemented.



The screenshot shows a terminal window titled "Metasploitable (Port Scan Snapshot) [Running] - Oracle VM VirtualBox". The terminal displays the following text:

```
msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$
```

Fig.2

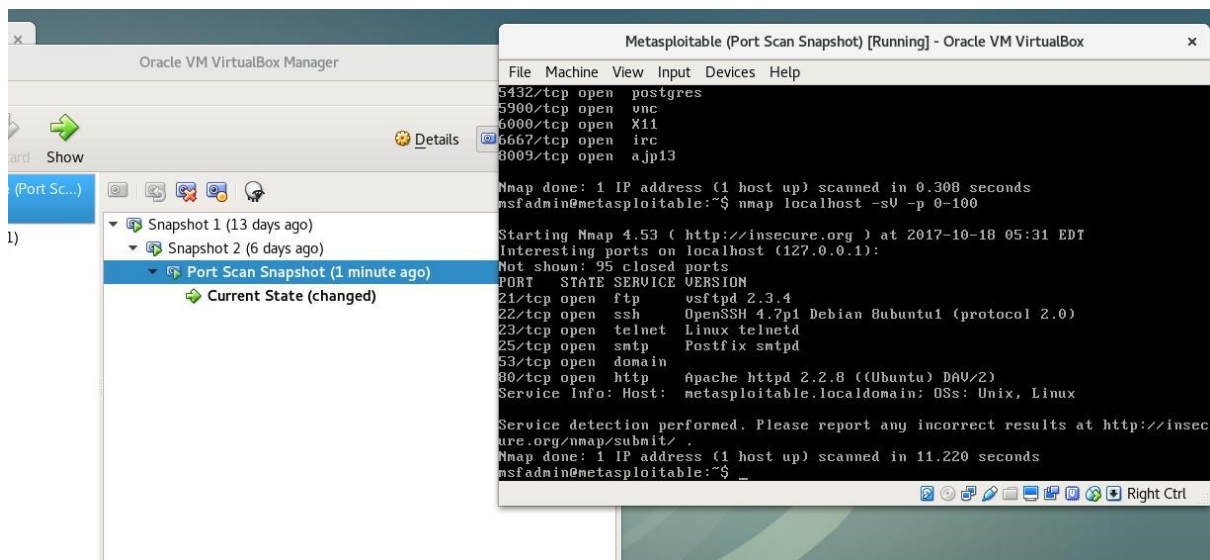


Fig.3

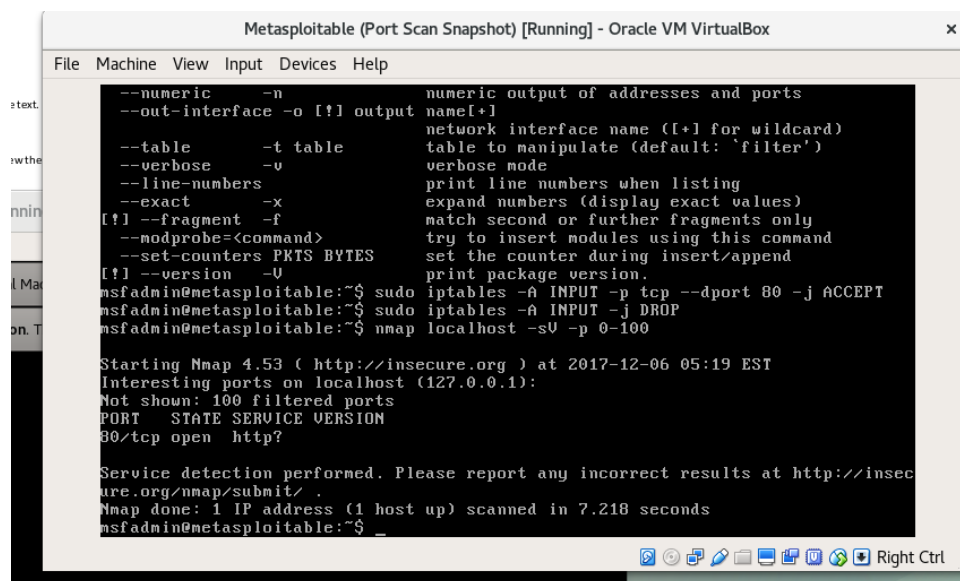


Fig.4

It is important to leave port 80 open, because it offers communication on the protocol HTTP. If it is closed, no traffic would be able to travel to the web server the local host wants to send a request to. Therefore, we could say that closing port 80, would prevent the web server from functioning, as the web server wouldn't be able to establish a connection with the host computer.

Additional Mitigation Approaches

Further on, looking into Mitigation approaches, the concept of defence in depth is implied. This is a method used in networks, using multiple layers of security. It is said that these layers, used to secure data, consists of typically three elements: "prevention, detection and response." (J. Breithaupt, M.S. Merkow, 2014) In general, firewalls are used in these mitigation approaches, but are not typically

trusted as the only element to provide security, therefore, a "network based IDS" would be used to be able to "identify scans or traffic patterns that indicate an attack." (K. Nelson, SANS Institute, 2011)

Another approach to mitigating vulnerabilities in the system is the approach of using, "patching," in the system's operating system and so, this would repair certain vulnerabilities that would normally allow an attacker to infiltrate the computer. A more logical method would be to implement a "Password Policy," as regularly most user IDs and various passwords are known and shared between a range of people in higher levels of the systems hierarchy. Different user IDs and passwords for every network login would be utilised, which contrasts with the lack of security of a common username and password, providing more structural strength. Furthermore, one of the most important approaches or methods that could also be used is User Education, which is basically, one of the more simplest and efficient ways to mitigating certain vulnerabilities in a system, as the user's would be able to identify these vulnerabilities with no external help.

References

- Crown. (2008) Computer Misuse Act 1990. [Online] [Accessed on 14th October 2017]
<https://www.legislation.gov.uk/ukpga/1990/18/section/1>
- J. Kizza. (2015) 'Virtualization Security.' *Guide to Computer Network Security, Springer-Verlag*, pp. 473-490.
http://books.google.com/books?id=sbA_AAAAQBAJ&pgis=1
- P. Mateti. (2011) Port Scanning: It's Not Just an Offensive Tool Anymore. [Online] [Accessed on 18th October 2017]
http://www.garykessler.net/library/is_tools_scan.html
- Palo Alto Networks, Inc. (2017) What is a Port Scan? [Online] [Accessed on 18th October 2017]
<http://whatismyipaddress.com/port-scan>
- J.Postel. (1980) Transmission Control Protocol [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc761.txt>
- J. Postel (1980) User Datagram Protocol [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc768.txt>
- G.Lyon (2011) nmap (1) – Linux man page [Online] [Accessed on 13th December 2017]
<https://linux.die.net/man/1/nmap>
- A.K. Bhushan (1971) A File Transfer Protocol [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc114.txt>
- S. Lehtinen, C. Lonvick, Ed. (2006) The Secure Shell (SSH) Protocol Assigned Numbers [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc4250.txt>
- J.T. Melvin, R.W. Watson (1971) A First Cut At A Proposed Telnet Protocol [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc97.txt>
- D. Mills (1992) Simple Network Time Protocol [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc1361.txt>
- T. Berners-Lee, R. Fielding, H. Frystyk (1996) Hypertext Transfer Protocol – HTTP/1.0 [Online] [Accessed on 13th December 2017]
<https://www.rfc-editor.org/rfc/rfc1945.txt>
- A. Kak. (2015) Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection and Penetration Testing. [Online] [Accessed on 15th November 2017]
<https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf>
- A. Whitaker, D. Newman (2006) Penetration Testing and Network Defence: Performing Host Reconnaissance. [Online] [Accessed on 15th November 2017]
<http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3>
- Cisco (2017) What is a Firewall? [Online] [Accessed on 18th November 2017]

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

Microsoft Technologies (2017) Firewall: What It Is and How It Works [Online] [Accessed on 18th November 2017]

<https://www.microsoft.com/en-us/safety/pc-security/firewalls-what-is.aspx>

The Mitre Corporation (2017) CVE - CVE-2017-9798 [Online] [Accessed on 27th November 2017]

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9798>

The Mitre Corporation (2011) CVE – CVE-2011-0762 [Online] [Accessed on 1st December 2017]

<http://www.cvedetails.com/cve/CVE-2011-0762/>

J. Breithaupt, M.S. Merkow (2014) Principle 3: Defense in Depth as Strategy [Online] [Accessed on 8th December 2017]

<http://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=4>

ISA (2006) Mitigations for Security Vulnerabilities Found in Control System Networks [Online] [Accessed on 8th December 2017]

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf

SANS Institute, K. Nelson (2011) InfoSec Reading Room [Online] [Accessed on 8th December 2017]

<https://uk.sans.org/reading-room/whitepapers/basics/defense-in-depth-525>