6G4Z1902: Computing Fundamentals

Coursework 1

Student Name, Student ID

Contents

[Contents 1](#_Toc526924516)

[Section A – In Class Test 2](#_Toc526924517)

[Section B – System Audit 2](#_Toc526924518)

[Computer Misuse Act 1990 2](#_Toc526924519)

[Port Scanning & the TCP Handshake 2](#_Toc526924520)

[Vulnerability Assessment of Metasploitable Virtual Machine 3](#_Toc526924521)

[Common Vulnerabilities and Exploits Identified 3](#_Toc526924522)

[Section C – Mitigation 3](#_Toc526924523)

[Firewalls Background 3](#_Toc526924524)

[IP Tables Background and Deployment 4](#_Toc526924525)

[Additional Mitigation Approaches 4](#_Toc526924526)

# Section A – In Class Test

Please attend the in class test during the week commencing 12th November 2018

# Section B – System Audit

**Use the subheadings in this section to structure your work. You may remove this text.**

## Computer Misuse Act 1990

**Approximately 100 words**

Explain what the Computer Misuse Act 1990 is, explain how the use of virtualisation can be used to prevent an accidental breach of the act during security testing.

Company’s take the utmost importance in securing there networks as breach of the information it manages can bring upon an unholy amount of legal battles and fees. Network security testing is an integral part of security, it works by highlighting a systems vulnerabilities and exposures. This information could compromise a system and is the reason why security testing a non-permitted network is a breach of the computer misuse act.

DESCRIPTION OF THE MIS USE ACT.

“One of the core features of network virtualization is isolation”, virtual networks have complete independence from other virtual networks and the underlying physical network therefore security testing is a lot safer on virtual networks.

----------------------

## Port Scanning & the TCP Handshake

**Approximately 200 words**

Define what a port scan is explaining the goals and mechanisms employed by port scanners, ensure you fully explain how port scanners misuse the TCP three-way handshake.

TCP short for transmission control protocol is the industry standard for reliable data transfer as before any data is transferred it must complete a three way handshake. A three way handshake is designed so two hosts attempting to communicate can negotiate parameters, setting up a reliable session for data transfer.

The steps of a three way handshake:

1. Host A sends an SYN packet to Host B
2. Host B receives the SYN packet and responds with an SYN-ACK packet
3. Host A receives the SYN-ACK packet and responds with an ACK packet
4. Host B receives the ACK packet, A TCP socket connection is created

Port scanning boasts the ability to fingerprint a system, identifying open, closed, filtered and unfiltered ports as well as security implementations such as firewalls which control service communications. Its aims are to reveal common vulnerabilities and exposures (CVE) which are used to reinforce the system so it can’t be taken advantage off.

A port scanner works by looping through a set range of ports sending a SYN packet to each port, this is how the three way handshake is used. Then depending on the response the state of the port is revealed but no ACK packet is ever sent back, this is how the three-way handshake Is misused.

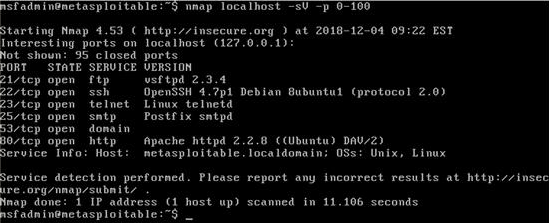
|  |  |
| --- | --- |
| State | Response |
| CLOSED, UNFILTERED | RST packet, ACK packet reached host B |
| OPEN, UNFILTERED | SYN-ACK, a successful 1st step of the three-way handshake |
| FILTERED | No response, SYN packet was blocked from reaching host B |

## Vulnerability Assessment of Metasploitable Virtual Machine

**Approximately 100 words**

**C:\Users\morganp\Documents\!exams\computer-fundementals\nmap_command.png**

The command run is nmap localhost –sV –p 0-100. Localhost is the target system, -sV probes for the service/version and -p 0-100 scans from port 0 to 100.

****

The command reveals ports: 21, 22, 23, 25, 53 and 80 are all open and gives the service and version of that service running on them.

## works by

## Common Vulnerabilities and Exploits Identified

**Approximately 200 words**

Access the CVE Mitre website (https://cve.mitre.org/find/ ) and lookup a CVE for two of the services you identified on the vulnerable virtual machine. Explain in your own words how the vulnerability could affect the confidentiality, integrity, or availability of the system, and what the implications would be for a business.

# Section C – Mitigation

**Use the subheadings in this section to structure your work. You may remove this text.**

## Firewalls Background

**Approximately 200 words** <https://img.itch.zone/aW1hZ2UvMjg0NDI2LzEzODUyMDgucG5n/original/1fg6dU.png>

A through explanation of what firewalls are and how they work.

Research firewalls and explain how they can be used to increase the security of a computer system.

A firewalls sole purpose is to “prevent unauthorized Internet users from accessing private networks”. A firewall can either be hardware or software but the ideal practice would consist of both.

Firewalls work by examining all messages entering and leaving the network, messages will only pass through if it reaches the specified security rules. Rules set up properly have the power to remove all common vulnerabilities and exposures a system may have, they are rigid and set up have a strict set of requirements for which a message must reach all before it is accepted.

Firewalls increase the security of a system by filtering between the messages that can meet the requirements. “It would actually be more accurate if firewalls were called ‘firefilters’ because they’re not built to keep everything out Instead, firewalls are designed to filter threatening communications.” This quote by Norton security possibly one of if not the largest firewall manufacturers sums up how firewalls work to the tee.

Difference in firewalls:

|  |  |
| --- | --- |
| Hardware | Software |
| More expensive & harder to configure | Less expensive & easier to configure |
| Protects an entire network | Protects a single computer |
| Implemented at router level | Implemented software on the computer |

## UFW Background and Deployment

**Approximately 100 words**

Research the use of UFW (Uncomplicated FireWall) and create a rule that filters one or more ports on the vulnerable virtual machine, ensure you leave port 80 open, and explain why

First ufw needs to be enabled so “sudo ufw enable” is ran. Then for port 80 to be open “sudo ufw allow 80” is ran, sudo is run in coherent with all commands as to enable a ufw firewall it requires administrator privileges.

## Additional Mitigation Approaches

**Approximately 200 words**

There are many additional approaches that can be taken to secure a system, the most obvious ones relate to users and password. I would suggest having separate privileged accounts each with separate usernames and passwords, setting a bios password and disable root log on this will ensure even by accident or on purpose

PASSWORD, privileged accounts with different passwords, encrypt the hard drive, set bios password, limit access to sudo/root privileges, ssh authentication key, disable root log on, change ssh port 22 to a different port.

LINKS

TCP THREE WAY HANDSHAKE <https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml>

FIREWALL QUOTE https://www.webopedia.com/TERM/F/firewall.html

FIREWALL QUOTE 2 <https://us.norton.com/internetsecurity-how-to-how-do-firewalls-prevent-computer-viruses.html>

VIRTUALAZATION https://www.infoworld.com/article/2609571/networking/4-ways-network-virtualization-improves-security.html