A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 4**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

***REFLECTION QUESTIONS TASK 1***

1. Explain what is defence in-depth and how to relate to the host security?

* Defense in depth means using many layers of protection to keep a system safe. Host security, which is about protecting individual computers, involves steps like physical security, controlling network access, and using secure software practices. The idea is to make it hard for attackers by having multiple layers of defense.

1. Based on your understanding, explain why host security is important?

* Data Protection: It keeps sensitive information safe.
* System Availability: It prevents disruptions to computer services.
* Compliance: It ensures adherence to rules and regulations.
* Business Continuity: It helps a company keep running smoothly.
* Threat Prevention: It guards against various types of cyber threats.
* Lateral Movement Prevention: It stops attackers from moving easily within a network.

***REFLECTION QUESTIONS TASK 2***

1. Is there any security issue with the ping command? If so explain briefly.

No.

***REFLECTION QUESTIONS TASK 3***

1. Scanning can be done without proper consent. Why?

* Scanning can happen without proper permission because someone might do it without knowing they need permission, or, in some cases, with bad intentions to find weaknesses.

1. At your organization, is there any statement in the security policy related to scanning activity? Please state it here.

***REFLECTION QUESTIONS TASK 4***

1. Why security baseline is important to be applied to a particular host in the enterprise or any company?

* Keeps security consistent across all hosts.
* Reduces the risk of cyber attacks by addressing vulnerabilities.
* Helps meet industry standards and compliance requirements.
* Makes security management more efficient.
* Enables quick responses to emerging threats.

1. Explain 5 security techniques to properly secure a virtualhost machine

* **Hypervisor Security**: Secure the virtualization software to prevent unauthorized access.
* **Network Segmentation**: Isolate virtual machines to limit potential security breaches.
* **Regular Patching**: Keep the virtual host and guest operating systems updated for security.
* **Virtual Machine Isolation**: Restrict unnecessary services and access for virtual machines.
* **Secure Virtual Disk Encryption**: Encrypt virtual machine disks to protect sensitive data.

1. Explain 5 ways to manage host security

* **Regular Audits**: Check and fix vulnerabilities on the host regularly.
* **Endpoint Protection**: Use antivirus and anti-malware tools to prevent malicious activities.
* **User Education**: Train users on security practices and how to recognize threats.
* **Incident Response Planning**: Have a plan to handle security incidents effectively.
* **Access Controls**: Limit user permissions and use strong authentication methods.

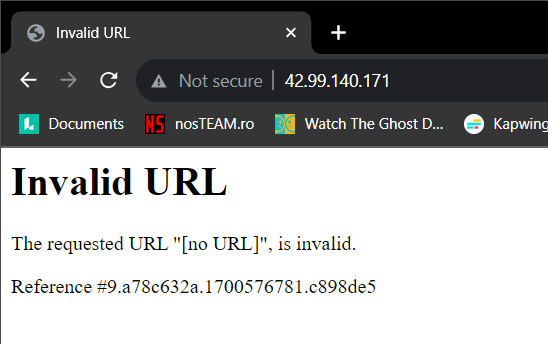
TASK 1

A screenshot of a computer

Description automatically generated

A screenshot of a computer

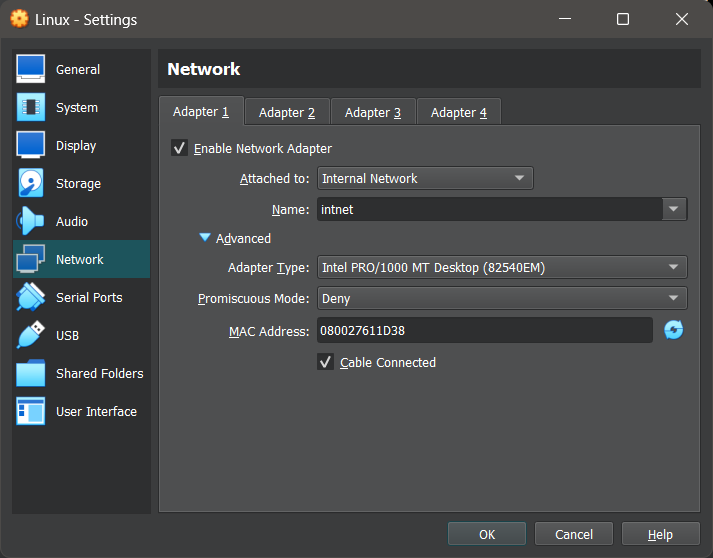
Description automatically generated



A screenshot of a computer error

Description automatically generated

TASK 2



A screenshot of a computer

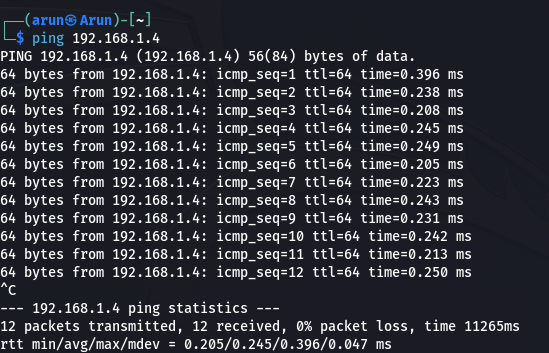
Description automatically generated

A computer screen with white text

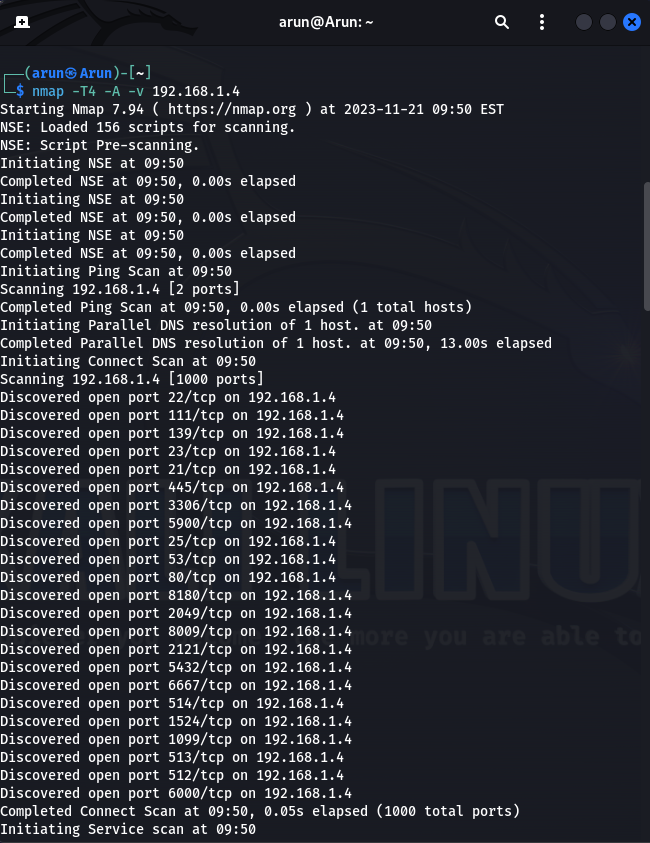
Description automatically generated

A computer screen shot of white text

Description automatically generated



TASK 3

 23 OPEN PORTS

|  |  |
| --- | --- |
| Port Number | Related Service |
| 22 | Secure Shell (SSH) protocol |
| 111 | SUN Remote Procedure Call |
| 139 | NetBIOS |
| 23 | telnet |
| 21 | FTP |
| 445 | Microsoft DS |
| 3306 | MySQL |
| 5900 | VNC Server |
| 25 | SMTP |
| 53 | DNS |
| 80 | HTTP |
| 8180 | Application Service Controller RESTful APIs |
| 2049 | NFS |
| 8009 | AJP |
| 2121 | FTP Proxy |
| 5432 | PostgreSQL |
| 6667 | IRC |
| 514 | Syslog |
| 1524 | Ingreslock |
| 1099 | RMI |
| 513 | rlogin |
| 512 | rexec |
| 6000 | X11 |

TASK 4

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

