**Sri Lanka Institute of Information Technology**

A blue and orange logo

Description automatically generated

**Applied Information Assurance - IE3022**

**Network Scanning and Reconnaissance Test**

**Lab sheet 04**

**IT22560094**

**R.A.D.T.M. Ranasinghe**

Table of Contents

[Nmap - Network Scanning and Reconnaissance 3](#_Toc175946528)

[Exercise 1: Host Discovery 3](#_Toc175946529)

[Exercise 2: Port Scanning 5](#_Toc175946530)

[Exercise 3: Service and Version Detection 8](#_Toc175946531)

[Nikto - Network Scanning and Reconnaissance 9](#_Toc175946532)

[Exercise 1: Web Server Scanning 9](#_Toc175946533)

[The Harvester - Network Scanning and Reconnaissance 12](#_Toc175946534)

[Exercise 1: Information Gathering 12](#_Toc175946535)

[Maltego - Network Scanning and Reconnaissance 15](#_Toc175946536)

[Exercise 1: Visual Link Analysis 15](#_Toc175946537)

[Angry IP Scanner-Network Scanning and Reconnaissance 17](#_Toc175946538)

[Exercise 1: Quick Network Scanning 17](#_Toc175946539)

[Conclusion Questions 18](#_Toc175946540)

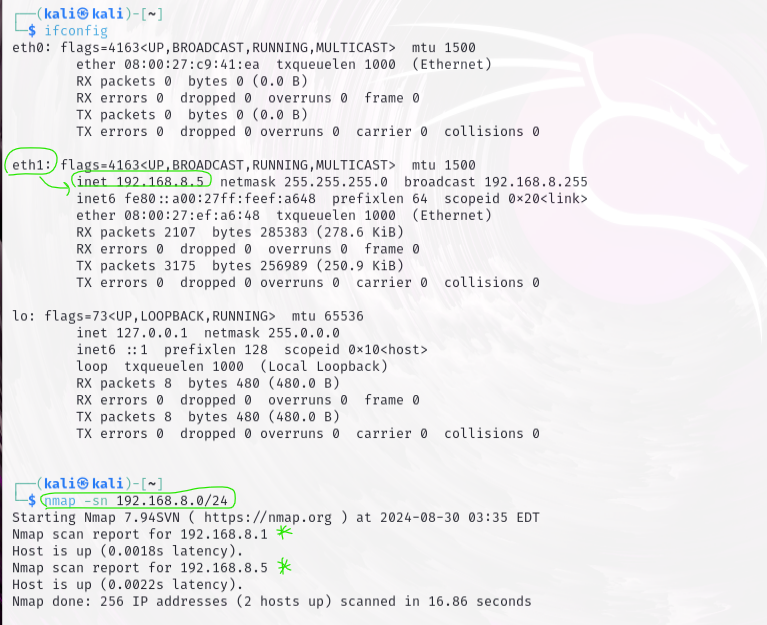
# Nmap - Network Scanning and Reconnaissance

Nmap is an open-source network scanning tool which has a GNU General public license.

Nmap was developed by Gordon "Fyodor" Lyon and continues to be actively maintained by a community of volunteers.

My current Nmap version is Nmap version 7.94SVN.

## Exercise 1: Host Discovery



Questions:

1. What command did you use for host discovery?

* Nmap –sn 192.168.8.0/24
* After running the command, Nmap will output a list of active IP addresses on your network

1. List the IP addresses of the discovered hosts.

* 192.168.8.1
* 192.168.8.5

1. What are the possible reasons if a host is not detected in the scan?

|  |  |
| --- | --- |
| Reason | Explanation |
| Firewalls | If the host is using a firewall which blocks ICMP (Internet control Message Protocol) echo requests which commonly known as ping requests. |
| Host is offline | If the host is powered off or disconnected to the network Nmap cannot detect them. |
| Different subnet | If the host is in a different subnet that will not be included in my scan range. |
| Network configurations | If the host has misconfigured network settings, the host will prevent responding to the network requests. |
| Stealth mode | If the hosts use stealth mode to intentionally avoid responding ping requests. |

## Exercise 2: Port Scanning

Perform a TCP SYN scan on one of the discovered hosts. Document the command used and the results.

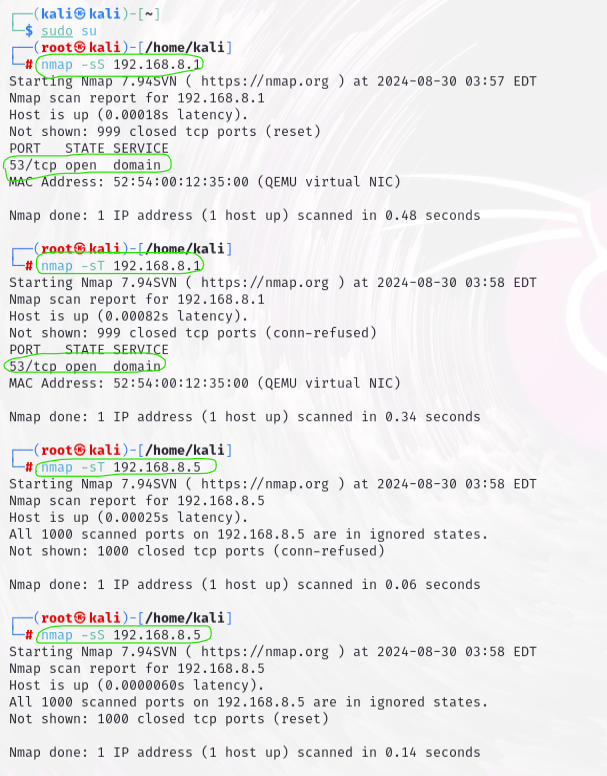
nmap -sS [target-ip]

Questions:

1. What command did you use for port scanning?

* nmap -sS 192.168.8.1

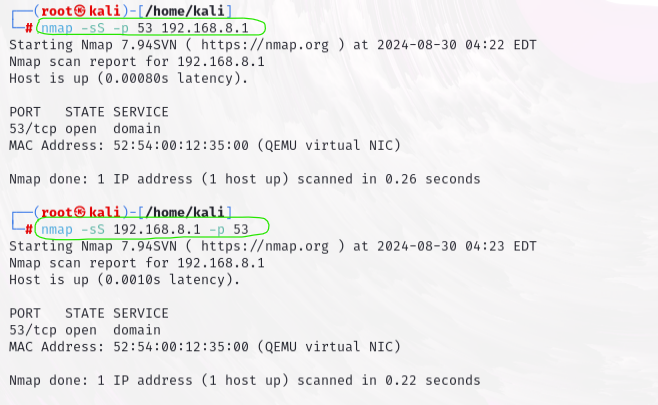
1. List the open ports and services found on the target host.



1. Explain the difference between a SYN scan and a CONNECT scan.

|  |  |  |
| --- | --- | --- |
| Aspect | SYN Scan (-sS) | CONNECT Scan (-sT) |
| Scan Type | Half-open scan | Full connection scan |
| TCP Handshake | Does not complete the TCP handshake (only sends SYN, receives SYN-ACK, and then sends RST) | Completes the full TCP handshake (SYN, SYN-ACK, ACK) |
| Stealth | Stealthier (less likely to be detected or logged) | Less stealthy (more likely to be detected and logged) |
| Speed | Faster | Slower |
| Resource Usage | Uses fewer resources on the target system | Uses more resources on the target system |
| Detection | Harder  Don’t complete the full TCP handshake they don’t send the final ACK packet.  So less likely to trigger alarms in Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) systems. | Easier  Because a CONNECT scan completes the full three-way TCP handshake, it generates more network activity and triggers the Intrusion Detection System (IDS)/Intrusion Prevention System (IPS). |
| Use Case | Preferred when you want to avoid detection | Used when SYN scan is not possible (e.g., due to restrictions) |
| Operating System | Typically requires root/administrator privileges | Can be run by regular users without special privileges |

1. How can you use Nmap to scan for specific ports or service types?



* Scan ports we can use ‘-p’ before or after the ip address.
* Scan specific service type we can use ‘--service’

Exercise 3: Service and Version Detection

Run a service and version detection scan on the same host. Document the command used and the output.

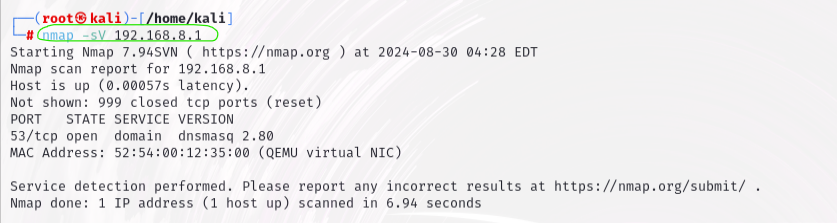
nmap -sV [target-ip]

Questions:

1. What command did you use for service and version detection?

* Nmap –sV 192.168.8.1

1. Provide details about the services and versions detected on the target host.



1. Why is it important to detect service versions during a network scan?

* Knowing the version helps to find specific vulnerabilities linked to that version.
* It helps to check if the service is up to date with security patches, which helps to keep the system secure.

1. How can version information be useful in identifying potential vulnerabilities?

* Known Issues: By knowing the version of the service (e.g., dnsmasq 2.80), we can check if that specific version has known security issues.
* Exploit Databases: Version information allows us to look up the version in exploit databases to see if there are any known exploits targeting that version.
* Update Recommendations: It helps determine if the service is outdated and needs to be updated or patched to fix security problems.

# Nikto - Network Scanning and Reconnaissance

## Exercise 1: Web Server Scanning

Scan a web server using Nikto. Document the command used and the findings.

Nikto commands can be used for scanning web applications.

|  |  |
| --- | --- |
| Command | Description |
| nikto -h http://foo.com | Scans the specified host |
| nikto -h http://foo.com -Tuning 6 | Uses a specific Nikto scan tuning level |
| nikto -h http://foo.com -port 8000 | Scans the specified port |
| nikto -h http://foo.com -ssl | Scans for SSL vulnerabilities |
| nikto -h http://foo.com -Format html | Formats output in HTML |
| nikto -h http://foo.com -output out.txt | Saves the output to a file |

nikto -h http://[target-ip]



Questions:

1. What command did you use for the web server scan?

Nikto –h courseweb.sliit.lk

1. List any vulnerabilities or issues detected by Nikto.

* The anti-clickjacking X-Frame-Options header is not present
* The X-Content-Type-Options header is not set

1. Explain how Nikto’s scan results can be used to improve web server security.

* Nikto can find web server softwares that is outdated and needs updating.
* It can detect known security vulnerabilities on the web server.
* It can finds default or leftover files that could be exploited by attackers.
* By using those results legitimate owners can reduce attack surfaces.

1. What are some limitations of Nikto in web vulnerability assessments?

|  |  |
| --- | --- |
| False Positives | Nikto might show a directory as potentially dangerous because it contains certain files, but those files might be harmless or created for a legitimate purpose.  It could report an outdated software version as a vulnerability even if security patches have been applied but if they forgot to update the version number. |
| Limited Coverage | Nikto scanning's can leads to cause some missing vulnerabilities because it primarily looks for known issues in common web servers |
| No Exploitation | It might find a potential SQL injection point but won't test if it's exploitable, leaving you uncertain of the real risk. |
| Basic Scanning | Advanced threats like zero-day vulnerabilities, which have no known fix or public knowledge, are likely to be missed by Nikto's scanning methods. |

# The Harvester - Network Scanning and Reconnaissance

## Exercise 1: Information Gathering

Use TheHarvester to gather information about a domain. Document the command used and summarize the results.

theharvester -d [domain] -l 500 -b google



|  |  |
| --- | --- |
| Command | Description |
| theHarvester -d example.com -l 500 | Gathers the first 500 results for the domain example.com. |
| theHarvester -d example.com -b google | Uses Google as the search engine to gather information on example.com |
| theHarvester -d example.com -b all | Uses all available search engines for information gathering on example.com |
| theHarvester -d example.com -f report.html | Saves the results in an HTML report named report.html |
| theHarvester -d example.com -v | Enables verbose mode, showing more detailed output during the scan |
| theHarvester -d example.com -c | Checks the validity of found emails |
| theHarvester -d example.com -s 0 | Starts searching from the first result (useful for large queries) |
| theHarvester -d example.com -b bing -l 200 -f results.xml | Uses Bing, limits results to 200, and saves the output in XML format. |

Questions

1. What command did you use for harvesting information?

* theHarvester -d hackthissite.org -l 500

1. List the email addresses, subdomains, and any other information collected.



1. How can harvested email addresses be used in social engineering attacks?

|  |  |
| --- | --- |
| Social engineering attack type | Description |
| Phishing Attacks | Attackers can send tricky emails that appear legitimate, tricking recipients into providing sensitive information, such as passwords or credit card details. |
| Spear Phishing | Targeted phishing where attackers customize emails to specific individuals using personal information, related topics which make the attack more convincing and harder to detect. |
| Credential Stuffing | Using harvested email addresses, attackers may attempt to log in to various accounts with commonly used or previously leaked passwords and try to brute force attacks. |
| Impersonation | Attackers can impersonate a trusted colleague, boss, or company using the email address, if attackers able to gain access to those mails. |

1. What steps can be taken to mitigate the risk associated with the information gathered by TheHarvester?

* Give Awareness Training related to these phishing, spear phishing, and other email-based threats.
* Use email authentication protocols like SPF, DKIM, and DMARC.
* Encourage the use of strong, unique passwords for all accounts and implement MFA (Multi factor authentication).
* Continuously monitor network traffic and update security protocols and firewalls.

# Maltego - Network Scanning and Reconnaissance

## Exercise 1: Visual Link Analysis

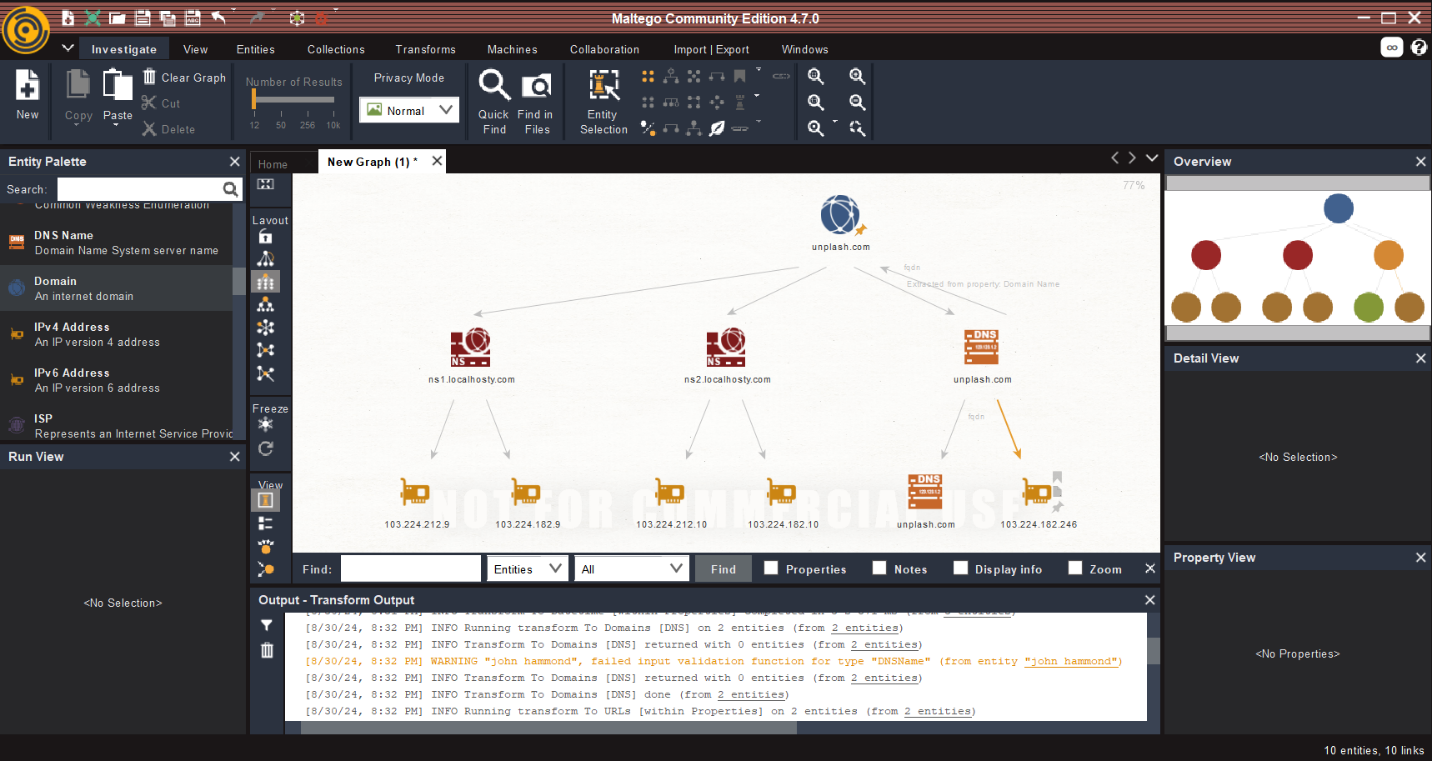
Set up Maltego and create a new graph with an entity (e.g., domain or IP address). Perform a transformation to gather additional data. Document the process and your findings.

Questions:

1. Describe the entity you used and the transformation performed.

* Entity: Domain – unplash.com
* Transformation: DNS name

1. Provide a screenshot of the graph created and summarize any key relationships or data points.



1. How does Maltego’s graphical representation assist in understanding network relationships?

* Maltego creates visual graphs that map out the relationships between domains, Ip addresses, email addresses and people which helps to quickly identify how those different components are connected.

1. What are some practical applications of Maltego in a penetration testing scenario?

* Reconnaissance and Information Gathering
* Mapping Organizational Structure
* Social Engineering Attacks
* Identifying Vulnerabilities in a network
* Tracking Digital Footprints

# Angry IP Scanner-Network Scanning and Reconnaissance

## Exercise 1: Quick Network Scanning

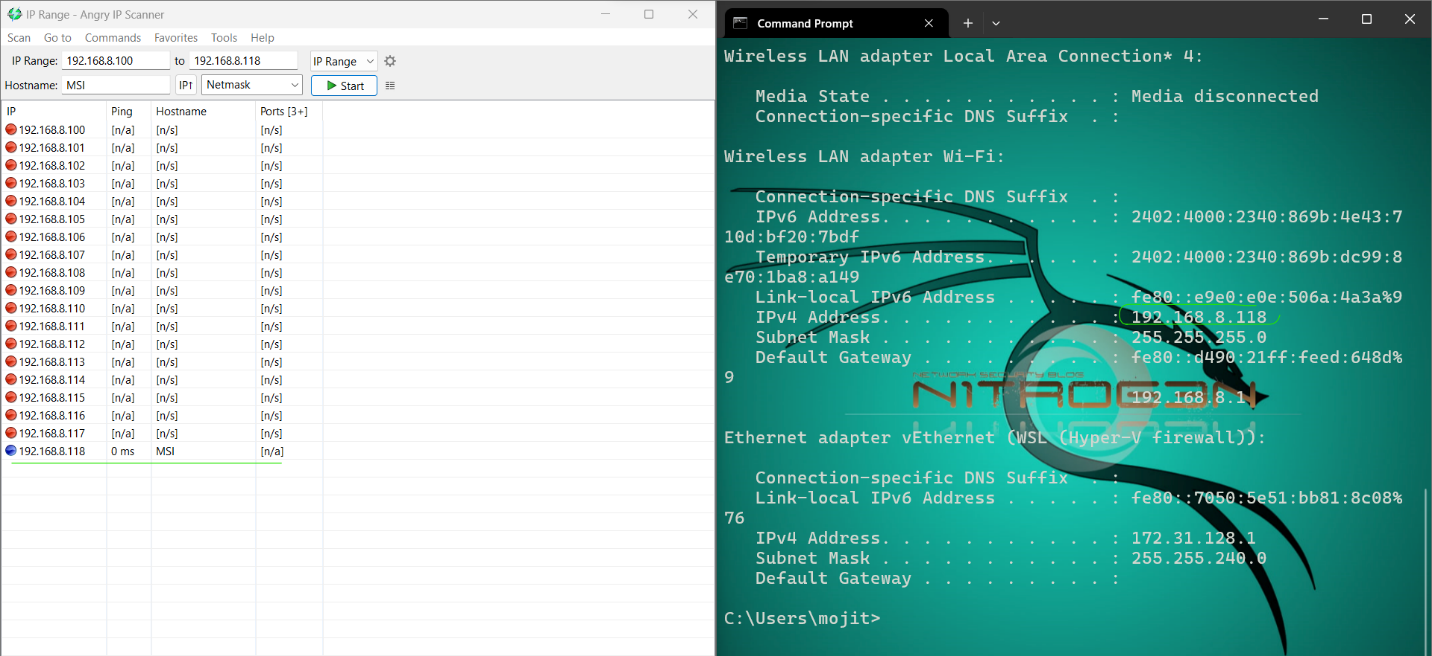
Scan your network range using Angry IP Scanner. Document the IP range scanned and the results.

Questions:

1. What IP range did you scan?

* 192.168.8.100 -> 192.168.8.118

1. List the IP addresses, open ports, and any other information gathered.



1. How does Angry IP Scanner compare to Nmap in terms of features and usability?

|  |  |  |
| --- | --- | --- |
| Feature/Aspect | Angry IP Scanner | Nmap |
| Ease of Use | User-friendly interface, suitable for beginners. | Command-line based, requires some IT knowledge. |
| Speed | Generally faster for basic scans due to simplicity. | Can be slower, especially with complex or deep scans. |
| Customization | Limited customization, primarily IP scanning. | Highly customizable with extensive options and code scripts. |
| Network Discovery | Effective for quick discovery of live hosts. | Can perform detailed network discovery and mapping. |
| Community Support | Smaller community, fewer resources. | Large community with bigger support. |

1. What are the benefits and drawbacks of using Angry IP Scanner for network reconnaissance?

* Benefits- ease of use and higher speed.
* Drawbacks-Limited features for network scanning and basic output as a report.

# Conclusion Questions

1. Compare the functionalities and use cases of Nmap, Nikto, TheHarvester, Maltego, and Angry IP Scanner.

|  |  |  |
| --- | --- | --- |
| Tool | Functionality | Use case |
| Nmap | Scan networks.  Service detection.  OS fingerprinting. | Comprehensive network mapping.  Vulnerability detection. |
| Nikto | Web server vulnerability scan. | Know vulnerability detection. |
| TheHarvester | Information gathering. | Open-source intelligence (OSINT) |
| Maltego | Visual mapping between digital entities. | Analyse and understand complex networks. |
| Angry IP Scanner | Quick Ip and port scanning. | Basic network scanning. |

1. Discuss how combining the results from these tools can provide a more comprehensive understanding of network security.

* Enhance coverage by using Nmap for identifying open ports and services and while Nikto can uncover web server vulnerabilities. TheHarvester gathers external information that could be used in attacks, and Maltego visualizes the relationships between entities.
* Using multiple tools like that allows for cross-validation of results not only that, but it also increases the accuracy of the security assessment.

1. Reflect on any ethical considerations when using these tools in real-world scenarios.

* Always get permission from websites and network owners before conducting these scans.
* Avoid collecting, storing or sharing those collected scan results without permission from legitimate owners.
* Once we find vulnerabilities inform those issues to affected parties.

1. Based on the tools used, what are some best practices for conducting a thorough network and web application assessment?

|  |  |
| --- | --- |
| Use Multiple Tools | Combine these scanning tools and cover different aspects of security like network scanning, vulnerability detection and information gathering. |
| Conduct regular scans | Regularly using these tools helps to maintain ongoing network changes. |
| Validate and Cross-Check Findings | Once gather information using these tools need to validate those results and make sure those are not false positive values. |
| Follow Ethical Guidelines | Always take permissions before doing scanning and avoid potential legal issues. |