

This project focuses on gathering network information using tools like dnsrecon for DNS enumeration, Nmap for scanning ports and services, and Nessus for vulnerability scanning. It provides essential skills for identifying live hosts, open ports, and potential vulnerabilities in a network. Here's a summary of the key components and steps:

DNS Enumeration

Understanding DNS: Learn how DNS resolves hostnames to IP addresses, zones, and resource records.

Using DNSmap

```
(kali@kali)-[~]
$ dnsmap duckduckgo.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for duckduckgo.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

ac.duckduckgo.com
IP address #1: 52.149.246.39

beta.duckduckgo.com
IP address #1: 52.149.246.39

blog.duckduckgo.com
IP address #1: 52.149.246.39

chat.duckduckgo.com
IP address #1: 20.81.5.168

email.duckduckgo.com
IP address #1: 52.146.152.248

ff.duckduckgo.com
IP address #1: 52.149.246.39

go.duckduckgo.com
IP address #1: 40.88.50.215
```

Performing Enumeration:

Use dnsrecon and host commands to gather DNS records for a target domain.

Practice zone transfer using tools like host and dnsenum.

```
(kali@kali)-[~/Downloads]
$ dnsrecon -d microsoft.com
[*] std: Performing General Enumeration against: microsoft.com ...
[-] DNSSEC is not configured for microsoft.com
[*] SOA ns1-39.azure-dns.com 150.171.10.39
[*] SOA ns1-39.azure-dns.com 2603:1061:0:10::27
[*] NS ns2-39.azure-dns.net 150.171.16.39
[*] NS ns2-39.azure-dns.net 2620:1ec:8ec:10::27
[*] NS ns3-39.azure-dns.org 13.107.222.39
[*] NS ns3-39.azure-dns.org 2a01:111:4000:10::27
[*] NS ns4-39.azure-dns.info 13.107.206.39
[*] NS ns4-39.azure-dns.info 2620:1ec:bda:10::27
[*] NS ns1-39.azure-dns.com 150.171.10.39
[*] NS ns1-39.azure-dns.com 2603:1061:0:10::27
[*] MX microsoft-com.mail.protection.outlook.com 52.101.42.0
[*] MX microsoft-com.mail.protection.outlook.com 52.101.8.49
[*] MX microsoft-com.mail.protection.outlook.com 52.101.11.0
[*] MX microsoft-com.mail.protection.outlook.com 52.101.40.26
[*] MX microsoft-com.mail.protection.outlook.com 2a01:111:f403:f90e::
[*] MX microsoft-com.mail.protection.outlook.com 2a01:111:f403:f804::
[*] MX microsoft-com.mail.protection.outlook.com 2a01:111:f403:f905::
[*] MX microsoft-com.mail.protection.outlook.com 2a01:111:f403:f911::1
```

Network Scanning

Discover Live Hosts:

Use tools like ping, arp-scan, and Nmap.

```
(kali@kali)~$ ping 192.168.1.100 -c 4
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.741 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.794 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.735 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=0.559 ms

— 192.168.1.100 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.559/0.707/0.794/0.088 ms
```

Basic and Advanced Nmap Scans:

Conduct scans to identify open ports, services, and operating systems.

Use options like -sS, -sU, -sV, and the NSE scripting engine.

-sS scans a range of IP addresses

```
(kali@kali)~$ nmap -sS 192.168.1.1 - 192.168.1.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 19:36 EST
Failed to resolve "-".
Bare '-': did you put a space between '--'?
Nmap scan report for pfSense.home.arpa (192.168.1.1)
Host is up (0.0017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:27:BE:9E (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 6.29 seconds
```