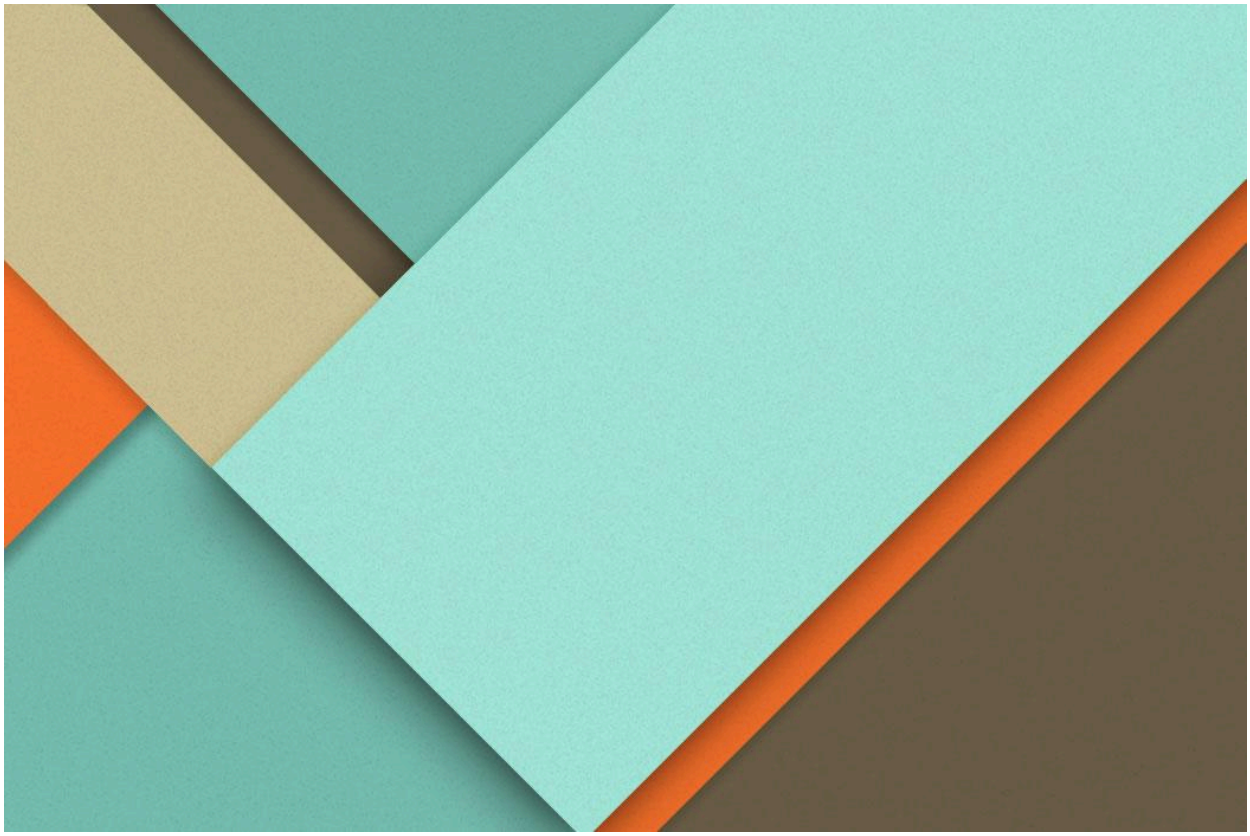

ENUMERATION PROJECT.

20.01.2025

MUHAMMED SAFAYATH
STUDENT AT INTELLIPAAT
KERALA
suhailariyallur1@gmail.com

Overview

Enumeration on local network and deep researching on target and scannug.

Goals

1. How to enumerate and penetrate into system if it is vulnerable.
2. Smb and network enumeration.

Tasks to be performed:-

1. Network Discovery: Identify a target network or system for your assignment. This can be a virtual lab environment, a specific IP address range, or a predefined network.
2. Scanning with Nmap:
● Use Nmap to perform an initial network scan. Identify open ports and running services on the target network/system.
● Document the results of your Nmap scan and identify any potential targets for further enumeration.
3. SMB Enumeration with smbclient and enum4linux:
● Based on the Nmap results, focus on the SMB service. Use smbclient to connect to SMB shares and enum4linux to gather information about the target's Windows environment.
● Enumerate shares, users, groups, and other valuable information related to the SMB service
4. Email Enumeration with theHarvester:
● Utilize theHarvester to search for email addresses and associated information related to the target network or organization.

● Document the email addresses and any other relevant information you discover.

5. Vulnerability Scanning with Nessus:

● Perform a vulnerability scan on the target network/system to identify potential security vulnerabilities.
● Document the vulnerabilities, their severity, and any recommendations provided by Nessus.

Note:-

Ensure that you have proper authorization to perform network enumeration on the chosen target. Always follow ethical and legal guidelines when conducting security assessments. The target could be any authorized domain or any of the domains from the below list:

1. www.certifiedhacker.com
2. www.moviescope.com
3. www.goodshopping.com
4. Testphp.vulnweb.com
5. Machine IP from your Lab Setup

Solutions:-

1:- Network Discovery:-

Can use Angry ip scanner.

fping -a -g 192.168.1.0/24

nmap -sn 192.168.1.0/24

nmap -sn 192.168.1.0/24 | grep "Nmap scan report" | awk '{print $NF}'

netdiscover -r 192.168.1.0/24

Practical given in netdiscover.txt

2:- Scanning with Nmap:

nmap -sV -O 192.168.1.0/24

Practical provided

3:-SMB Enumeration with smbclient and enum4linux:

ENUMERATE SMB USING NMAP FIRST

nmap -p 139,445 -sV -oN smb_scan.txt <target_ip>

nmap -p 139,445 --script=smb-enum-shares,smb-enum-users,smb-os-discovery -oN smb_enum.txt <target_ip>

USE ‘nmap -A’ command which uses almost possible sm scripts to get comprehensive details about smb including smb-system-info script.

Can explicitly try to enumerate users or shares with CrackMapExec using anonymous access.

```
crackmapexec smb 192.168.0.112 --shares -u '' -p ''
```

crackmapexec smb 192.168.0.112 -u '' -p '' --shares

Crackmapexec smb 192.168.0.112 -u “msfadmin” -p “msfadmin” –-users

Crack smb password using Hydra:-

hydra -L usernames.txt -P passwords.txt smb://192.168.0.112

THEN CONNECT TO SMB SHARES USING SMBCLIENT

smbclient -L //<target_ip>

smbclient //<target_ip>/<share_name>

smbclient -L //<IP_ADDRESS> -U <USERNAME>

- `-L`: List available shares on the specified server.
- `<IP_ADDRESS>`: Replace with the target IP address.
- `<USERNAME>`: If anonymous access is allowed, use `-U ""` for anonymous login.

smbclient -L //192.168.1.100 -U ""

smbclient //<IP_ADDRESS>/<SHARE_NAME> -U <USERNAME>

Use `rpcclient` to manually enumerate users and groups. First, connect to the SMB service:
bash
CopyEdit

```
rpcclient -U "" 192.168.0.112
```

enum4linux -U 192.168.0.112

enum4linux -a <IP_ADDRESS>

`-a`: Perform a comprehensive enumeration.

Practical provided

4:- Email Enumeration with theHarvester:

```
theharvester -d <domain> -b <data_source>
```

- `-d`: Specifies the domain to search.
- `-b`: Specifies the data source (e.g., Google, Bing, LinkedIn, etc.).

5:-Vulnerability Scanning with Nessus:

Start the Nessus service:

```
sudo systemctl start nessusd
```

Access Nessus Web Interface:

- Open a browser and go to `https://<your-ip-address>:8834` to configure and start using Nessus.

Use basic network scan Template.

Practical provided

Thank you.