

hello, this is a proof of concept for my script,  
network mapping for open ports, services,  
vulnerabilities, and weak passwords + usernames

1.Starting the tool as regular user , aka not root:

```
(kali㉿kali)-[~/Desktop/pentestProject]
$ ./Vulner\27-03-22\).sh
[*] Please run the script as sudo. [*]
Usage: sudo ./vulner {Network Range}

Your Input: ./Vulner(27-03-22).sh

Vulner: 2.6V (CyberChef)
SRV_DHCP:
(kali㉿kali)-[~/Desktop/pentestProject]
$
```

2. now that you've ran the script as root ,you'll get an  
update, and couple of tools installed (nmap ,masscan)

```
affix ip6tables-save
affrecover ip6tables-transla
affsegment ipcmk
affsign ipcrm
(kali㉿kali)-[~/Desktop/pentestProject]
$ sudo ./Vulner\27-03-22\).sh
[sudo] password for kali:
Root Access Granted

Making sure you're up-to-date with all the tools needed
Hit:1 http://kali.download/kali kali-rolling InRelease

```

3. if the user, didn't give the script a input of ip address , the script will show the following message

```
File Edit View Help
Your Input: 1.2.3.4
Netmask not present or invalid
Must Input a subnet mask for the IP address to set the Network Range
Try Again
Please Enter A Valid Network Range Expl: 10.0.0.0/24 , 172.16.0.0/12 etc.
Usage: sudo ./vulner {Network Range}
Vulner: 2.6V (CyberChef)
(kali㉿kali)-[~/Desktop/pentestProject]
$
```

4. now we will run the script on a LAN network range.

```
(kali㉿kali)-[~/Desktop/pentestProject]
$ sudo ./Vulner\ (27-03-22\).sh 10.1.1.10/24
```

5.the script didn't find any IP address that responded to him thouse for it didn't follow trough with the scan.

```

Vulner.

[*] MAKE SURE YOU RUN Vulner AS sudo
[*] sudo ./vulner {networkrange} [*]

File system: This tool should be used with caution

Please note that the network traffic the tool generates **MAYBE ILLEGAL**
USE WITH CAUTION!

[+] Mapping the range 10.1.1.10/24
[+] Directory created: 10.1.1.10

vulner2.0.sh

[6] Additional information about the given Network range
IPADDR=10.1.1.10      000010100000000010000000100001010
NETMASK=255.255.255.0 111111111111111111111111100000000
NETWORK=10.1.1.0      000010100000000010000000100000000
BROADCAST=10.1.1.255  000010100000000010000000111111111

256 ← Potential Hosts In Network Range

Logging Scan timestamp: 5:40:30
Sunday-03/27/22

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-27 09:40:30 GMT
Initiating ICMP Echo Scan
Scanning 256 hosts

0 ← Online Hosts In Network Range

[*] Starting Scan on 0 Hosts [*]

[*] Host's IPs found:

No Hosts Found

Make sure that you entered a right network range
Please Enter A Valid Network Range Expl: 10.0.0.0/24 , 172.16.0.0/12 etc.
```

6.now we will enter a valid ip address that we are connected to.

```

valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group de
link/ether 00:0c:29:35:b5:77 brd ff:ff:ff:ff:ff:ff
inet 10.1.1.104/24 brd 10.1.1.255 scope global dynamic noprefixroute eth0
valid_lft 691194sec preferred_lft 691194sec
inet6 fe80::20c:29ff:fe35:b577/64 scope link noprefixroute
valid_lft forever preferred_lft forever

$ sudo ./Vulner\27-03-22\).sh 10.1.1.10/24
```

7.the script then run's automatically scanning the network range you input .

```
SPY DHCP...

[*] Mapping the range 10.1.1.10/24
[+] Directory created: 10.1.1.10

vulnnet 2.0.0

[8] Additional information about the given Network range
IPADDR=10.1.1.10      000010100000000010000000100001010
NETMASK=255.255.255.0 11111111111111111111111100000000
NETWORK=10.1.1.0      000010100000000010000000100000000
BROADCAST=10.1.1.255  000010100000000010000000111111111

256 ← Potential Hosts In Network Range

Logging Scan timestamp: 5:43:49
Sunday-03/27/22

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-27 09:43:49 GMT
Initiating ICMP Echo Scan
Scanning 256 hosts

2 ← Online Hosts In Network Range

[*] Starting Scan on 2 Hosts [*]

[*] Host's IPs found:
10.1.1.10
10.1.1.11

[*] Tshark Starting [*]
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
** (tshark:48022) 05:43:57.769021 [Main MESSAGE] -- Capture started.
** (tshark:48022) 05:43:57.769101 [Main MESSAGE] -- File: "10.1.1.10/SCAN/Scan.pcap"

[*] Starting Nmap TCP SCAN. [*]
```

7.

```
[*] Starting Nmap TCP SCAN. [*]

Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-27 05:44 EDT
Nmap scan report for 10.1.1.10
Host is up (0.00089s latency).
Not shown: 8337 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
MAC Address: 00:0C:29:35:DE:A1 (VMware)

Nmap scan report for 10.1.1.11
Host is up (0.00067s latency).
Not shown: 8345 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
MAC Address: 00:0C:29:CC:BD:4D (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.08 seconds

[*] Starting Masscan UDP SCAN. [*]

Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-27 09:44:07 GMT
Initiating SYN Stealth Scan
Scanning 2 hosts [50001 ports/host]

Open Ports Found. Starting Nmap VersionScanner For Open Ports Found, Sit Tight
[*] _____ [*]

NOTICE:Nmap Version Scan is an aggressive scan which can take time to perform well.
```

8. open ports are being scanned for Versionb of the service running on that port . plus additional info such as OS , etc'

```
Open Ports Found. Starting Nmap VersionScanner For Open Ports Found, Sit Tight
[*] _____ [*]

NOTICE:Nmap Version Scan is an aggressive scan which can take time to perform well.

    Fetching OS info
[*] _____ [*]

    NSE Is Scanning For Vulnerabilities
[*] _____ [*]
```



9. searchsploit will that the output and suggest the user with a list of available vulnerabilities.

```
[i] SearchSploit's XML mode (without verbose enabled). To enable: searchsploit -v --xml...
[i] Reading: 'ServiceVersion.xml'

[i] /usr/bin/searchsploit -t --id domain
[-] Skipping output: domain (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t --id domain)

[-] Skipping term: http (Term is too general. Please re-search manually: /usr/bin/searchsploit -t --id http)

[i] /usr/bin/searchsploit -t --id kerberos sec
[i] /usr/bin/searchsploit -t --id microsoft windows kerberos
[i] /usr/bin/searchsploit -t --id msrpc
[i] /usr/bin/searchsploit -t --id microsoft windows rpc
[i] /usr/bin/searchsploit -t --id netbios ssn
[i] /usr/bin/searchsploit -t --id microsoft windows netbios ssn
[i] /usr/bin/searchsploit -t --id ldap
[i] /usr/bin/searchsploit -t --id microsoft windows active directory ldap
[i] /usr/bin/searchsploit -t --id microsoft ds
[-] Skipping output: microsoft ds (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t --id microsoft ds)

[i] /usr/bin/searchsploit -t --id microsoft windows server 2008 r2 2012 microsoft ds
[i] /usr/bin/searchsploit -t --id kpasswd5
[i] /usr/bin/searchsploit -t --id ncacn http
[i] /usr/bin/searchsploit -t --id microsoft windows rpc over http
[i] /usr/bin/searchsploit -t --id tcpwrapped
[i] /usr/bin/searchsploit -t --id microsoft httpapi httpd
[i] /usr/bin/searchsploit -t --id mc nfm
[i] /usr/bin/searchsploit -t --id net message framing
[i] /usr/bin/searchsploit -t --id microsoft iis httpd
[i] /usr/bin/searchsploit -t --id http rpc epmap
[i] /usr/bin/searchsploit -t --id ldapssl
[i] /usr/bin/searchsploit -t --id globalcatldap
[i] /usr/bin/searchsploit -t --id globalcatldapssl
[i] /usr/bin/searchsploit -t --id adws

[*] SearchSploit Found 124 Potential Exploits Available [*]
[*] Full Exploit list can be found Inside SearchSploit Directory [*]
[*] _____ [*]
You may also use SearchSploit manually
Nmap XML VersionScan can be found inside the XML Files Directory Created by Vulner
```

10. Brute force stage.

(please note that Tshark is running in the background at the ending giving the user two pcap files , one for the scanning stage and another for the brute force stage \*only\*

11. Lastly the user gets a log of all the info the tool gathered

## [\*]IP Addresses SCANNED [\*]

10.1.1.10  
10.1.1.11

## [\*] Services Found [\*]

```
Nmap scan report for 10.1.1.10
53/tcp ← PORT SERVICE→ domain?
88/tcp ← PORT SERVICE→ kerberos-sec Microsoft Windows Kerberos (server time: 2022-03-27 09:44:49Z)
135/tcp ← PORT SERVICE→ msrpc Microsoft Windows RPC
139/tcp ← PORT SERVICE→ netbios-ssn Microsoft Windows netbios-ssn
389/tcp ← PORT SERVICE→ ldap Microsoft Windows Active Directory LDAP (Domain: tc.local, Site: Default-First-Site-Name)
445/tcp ← PORT SERVICE→ microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: TC)
464/tcp ← PORT SERVICE→ kpasswd5?
593/tcp ← PORT SERVICE→ ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp ← PORT SERVICE→ tcpwrapped
3268/tcp ← PORT SERVICE→ ldap Microsoft Windows Active Directory LDAP (Domain: tc.local, Site: Default-First-Site-Name)
3269/tcp ← PORT SERVICE→ tcpwrapped
5985/tcp ← PORT SERVICE→ http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp ← PORT SERVICE→ mc-nmf .NET Message Framing
47001/tcp ← PORT SERVICE→ http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 10.1.1.11
80/tcp ← PORT SERVICE→ http Microsoft IIS httpd 10.0
135/tcp ← PORT SERVICE→ msrpc Microsoft Windows RPC
139/tcp ← PORT SERVICE→ netbios-ssn Microsoft Windows netbios-ssn
445/tcp ← PORT SERVICE→ microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp ← PORT SERVICE→ http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp ← PORT SERVICE→ http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

## [\*]PC Names.[\*]

WINSRV-DC

## [\*]Operating system Found.[\*]

Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)

## [\*]Vulnerabilities Nmap Found.[\*]

```
# Nmap 7.92 scan initiated Sun Mar 27 05:47:10 2022 as: nmap -sT -sU -sC -T4 -iL IP_Hosts -pT:135,139,3268,3269,389,445,464,47001,53,593,5985,636,80,88,9389,U:137,53 -o X NmapVulneFound.xml -oN NmapVulneFound.nmap
Nmap scan report
→10.1.1.10
Host is up (0.00024s latency).

PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    closed http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```

Hostnames: WINSRV-DC

interfaces:

10.1.1.10

MAC Address: 00:0C:29:35:DE:A1 (VMware)

Host script results:

```
_clock-skew: mean: -59m59s, deviation: 1h43m55s, median: 0s
|_ smb-os-discovery:
| OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
| Computer name: WINSRV-DC
| NetBIOS computer name: WINSRV-DC\x00
| Domain name: tc.local
| Forest name: tc.local
| FQDN: WINSRV-DC.tc.local
| System time: 2022-03-27T12:47:13+03:00
|_ nbstat: NetBIOS name: WINSRV-DC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:35:de:a1 (VMware)
|_ smb2-security-mode:
| 3.1.1:
|_ Message signing enabled and required
|_ smb2-time:
| date: 2022-03-27T09:47:13
| start_date: 2022-03-27T06:25:43
|_ smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
```

Nmap scan report

→10.1.1.11

Host is up (0.00042s latency).

```
PORT      STATE SERVICE
53/tcp    closed domain
80/tcp    open  http
|_ http-title: IIS Windows Server
|_ http-methods:
|_ Potentially risky methods: TRACE
88/tcp    closed kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   closed ldap
445/tcp   open  microsoft-ds
464/tcp   closed kpasswd5
593/tcp   closed http-rpc-epmap
636/tcp   closed ldapsst
3268/tcp  closed globalcatLDAP
3269/tcp  closed globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  closed adws
47001/tcp open  winrm
53/udp    open|filtered domain
137/udp    open  netbios-ns
```

|\_ nbns-interfaces:

| hostname: WINSRV-RTR

| interfaces:

| 10.10.250.136

| 10.1.1.11

MAC Address: 00:0C:29:CC:BD:4D (VMware)

Host script results:

