22nd February 2012

Network Enumeration and Reconnaissance - a cheatsheet

This is a work in progress, additions, suggestions and constructive feedback are welcome.
The purpose of these cheatsheets is to, essentially, save time during an attack.

Network Scanning and Mapping

Network Service Discovery

Nmap

nmap -sSV -vv -PN --send-ip -A -O -oG <address-range>_`date +%Y-%m-%d_%H:%M` <address-range>nmap -A -vv -PN --send-ip -oG <address-range>_`date +%Y-%m-%d_%H:%M` <address-range>

Unicorn Scan

us -H -msf -Iv <address> -p 1-65535

us -H -mU -Iv <address> -p 1-65535

Layer 2 - Arp - netdiscover

netdiscover -i <interface> -r <address-range>

TCPDump Sniffing

tcpdump -s0 -xxXX -vv -i eth0 'host <address> and (dst port <num> or <num>)' | tee <address>_<service>_`date +%Y-%m-%d_%H:%M`.txt

or save the pcap file with additional flag (filename shortcut):

-w <address>_<service>_`date +%Y-%m-%d_%H:%M`.pcap

Locate VLAN Tags

tcpdump -vv -i <interface> -s &ltsnap-length> -c <num-packet-count> 'ether[20:2] == 0x2000'

Specific Service Queries

DNS TCP:53/UDP:53

DNS TCP and UDP 53 - DNS walking and Zone transfers

dig <domain> @<dns-server> AXFR | tee dns_<domain>_axfr._`date +%Y-%m-%d_%H:%M`.txt

DNS TCP and UDP 53 - DNS cache poisoning check

dig +short @<dns-server> porttest.dns-oarc.net txt

porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.

"<dns-server> is GREAT: 26 queries in 4.4 seconds from 26 ports with std dev 22336"

HTTP Web applications TCP 80,8000

nikto -h -p -C all -Display D -output nikto_<target-server><port>_`date +%Y-%m-%d_%H:%M`.txt -Format txt

DirBuster

cd /pentest/web/dirbuster && java -jar DirBuster-0.12.jar

WFuzz

wfuzz.py -c -z file,<wordlist> --hc 404 -o <html|magictree> http://<site-url>/FUZZ

e.g.

./wfuzz.py -c -z file,/pentest/passwords/wordlists/combined --hc 404 -o html http://<site-url>/FUZZ 2> /dev/null

HTTP commands for webserver enumeration

nc <target-address> <port>

HEAD / HTTP/1.0

or

OPTIONS / HTTP/1.0

or

TRACE / HTTP/1.0

WebDAV

IIS 6.0

HTTPS/SSL TCP 443

openssl s_client -connect <target-server>443 -state -debug

HEAD / HTTP/1.0

CONNECTED(00000003)

SSL_connect:before/connect initialization

... ... cut ... ...

SSL_connect:SSLv3 write client key exchange A

... ... cut ... ...

HTTP/1.1 302 Found

Date: Mon 02 Apr 2012 06:53:49 GMT

Server IBM_HTTP_Server/6.0.2.33 Apache/2.0.47 (Unix)

... ... cut ... ...

SNMP commands UDP 161

SNMPWalk

```
snmpwalk -c public -v[1|2c] <target-server> | tee <address>_snmp_`date +%Y-%m-%d_%H:%M`.txt
SNMPv2-MIB::sysDescr.0 = STRING: hp AlphaServer ES80 7/1000, VMS V7, MultiNet(R) for OpenVMS V4.4, Copyright (c) 2001 Process Software
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.58.1.1.1.2.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (24030770) 2 days, 18:45:07.70
SNMPv2-MIB::sysContact.0 = STRING: System contact unknown at this time
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING: System location unknown at this time
SNMPv2-MIB::sysServices.0 = INTEGER: 72
... ... ...
```

SNMPEnum

```
/snmpenum.pl public linux.txt
   UPTIME... ... ...
   HOSTNAME... ... ...
   RUNNING SOFTWARE PATHS
... ... ...
   RUNNING PROCESSES... ... ...
   MOUNTPOINTS... ... ...
   SYSTEM INFO
... ... ...
   LISTENING UDP PORTS
... ... ...   LISTENING TCP PORTS
```

OneSixtyOne

```
./onesixtyone -c <dictionary-file> -i <hosts-file> -o <address-range>_snmp_`date`.log -w
./onesixtyone <target-address>
Scanning 1 hosts, 2 communities [public] hp AlphaServer ES80 7/1000, VMS V7, MultiNet(R) for OpenVMS V4.4, Copyright (c) 2001 Process Software
```

SNMPCheck

```
./snmpcheck-1.8.pl -c <community-name> -v <version 1,2> -t <address-range>
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)
 [*] Try to connect to
 [*] Connected to
 [*] Starting enumeration at 2011-07-25 10:32:58
 [*] System information
 ----------------------------------------------------------------------------------------
 Hostname              :
 Description           : hp AlphaServer ES80 7/1000, VMS V7, MultiNet(R) for OpenVMS V4.4,
Copyright (c) 2001 Process Software
 Uptime system         : 0.00 seconds
 Uptime SNMP daemon    : 2 days, 18:17:07.01
 [*] Network information
... ... ...
```

[*] Network interfaces

... ...

[*] Routing information

... ...

[*] Listening TCP ports and connections

... ...

Samba/CIFS/NETBIOS TCP 135,139,445

nbtscan -v -s : -r <address-range> | tee <address-range>_nbtscan_`date +%Y-%m-%d_%H:%M`.txt

SMBClient - Discover and mount shares

smbclient -L \\\<target-address>\\ -U <Username>

smbclient -U <Username> -W <Workgroup> \\\\<target-address>\\\<sharename>

RPC, PortMapper and NFS TCP/UDP:111

rpcinfo -p >target-address> | tee <address>_rpcinfo_`date +%Y-%m-%d_%H:%M`.txt

showmount -e <ip-address>

mount <ip-address>:<exported_path> <local_path>

Tunnelling and Pivoting

SSH Tunnelling and pivoting

ssh -v -f -N -L <localIP>:<local-port>:<dest-ip>:<dest-port> <user>@&ltpivot-host> -i <authentication-key-file>

Verbosity (-v), Background (-f), No command execution (-N), Local port forwarding (-L)

Forward localhost port 25 to the localhost of 192.168.1.6 using ssh DSA key

ssh -v -f -N -L 127.0.0.1:25:127.0.0.1:25 user@192.168.1.6 -i /dsa/1024/f1fb2162a02f0f7c40c210e6167f05ca-16858

Proxy Chains

Dual-honed proxies or for proxying some port-scans

Edit the configuration file:

/etc/proxychains.conf

Under the ProxyList section:

[ProxyList]

http <proxy-server-ip> <port>

Execute with:

proxychains &ltsocket-aware command>

e.g

proxychains nmap -sT -vv --send-ip -pT:21,22,25,80,443,445,3389 <target-address>

Posted 22nd February 2012 by Tim Arneaud

Labels: backtrack, dns, enumeration, http, Linux, network, nmap, oscp, pwb, samba, security, smb, snmp, ssh

0 Add a comment