Lab Network Scanning Tips

Presented By:
Joe McCray

joe@strategicsec.com
http://www.linkedin.com/in/joemccray
http://twitter.com/j0emccray

Traditional Scanning Methodology

The Methodology

- Ping Sweep
- Port Scan
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process????

Ok, the process is great but what can go wrong and why?

Normal Headaches

These are the normal road blocks

- Routers/Firewalls/IPS between subnets
- Multi-layer switches between subnets (ACLs/VLANs/routed segments)
- Remote sites joined via VPN (network filtering/compression)
- Remote sites joined via MPLS
- Remote sites joined via leased lines (CSU/DSU)

Gov/Military…

If you do tactical communications security (example for DoD)….

- Multi-plexers
- Encryption Devices TACLANES/KIVs
- Bandwidth limitations

Connect to the lab network

How to connect to the VPN
https://infosecaddictsfiles.blob.core.windows.net/files/Strategic-Security-2017-VPN-Info.pdf

Now let's see your kung fu….
sudo nmap -sP 172.31.6.0/24
sudo nmap -sL 172.31.6.0/24

cd ~/toolz
wget --no-check-certificate https://raw.githubusercontent.com/BenDrysdale/ipcrawl/master/ipcrawl.c

gcc ipcrawl.c -o ipcrawl

chmod -x ipcrawl

./ipcrawl 172.31.6.1 172.31.6.254

…..and with all of these we got…….**NOTHING!!!**

Simple Process – Ping Sweep

The Methodology

- **Ping Sweep Alternative 1**
  - **If you pings are blocked – maybe try a list scan -sL**
  - nmap -sL 172.31.6.*
  - nmap -sL 172.31.6.1/24
  - nmap -sL 172.31.6.1-254

- Port Scan
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process – Ping Sweep

The Methodology

- **Ping Sweep Alternative 2**
  - **If you pings are blocked – maybe try a metasploit arp_sweep**
  - msf > use auxiliary/scanner/discovery/arp_sweep
  - msf auxiliary(arp_sweep) > show options
  - msf auxiliary(arp_sweep) > set RHOSTS 172.31.6.1-254
  - msf auxiliary(arp_sweep) > set THREADS 10
  - msf auxiliary(arp_sweep) > run
- Port Scan
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process – Port Scan

The Methodology

- Ping Sweep
- **Port Scan**
  - nmap -sS 172.31.6.15
  - nmap -sS -p 21,23,25,80,8080,1433,1521,3306 172.31.6.15
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process – Port Scan
- Reality Check -

The Methodology

- Ping Sweep
- **Port Scan (Intrusion Prevention or other Active Filter)**
  - nmap -sS -T 5 -p 21,23,25,80,8080,1433,1521,3306 172.31.6.13
  - nmap --scan-delay 15s -p 21,23,25,80,8080,1433,1521,3306 172.31.6.13
    - 1 probe every 15 seconds
  - nmap --max-rate 0.1 -p 21,23,25,80,8080,1433,1521,3306 172.31.6.13
    - 1 packet every 10 seconds
  - nmap -f -p 21,23,25,80,8080,1433,1521,3306 172.31.6.13
    - 8 Byte Fragment packets
  - nmap --mtu 16 -p 21,23,25,80,8080,1433,1521,3306 172.31.6.13
    - 16 Byte Fragment packets
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process – Port Scan
- Reality Check -

The Methodology

- Ping Sweep
- **Port Scan (Intrusion Prevention or other Active Filter)**
  - What to be thinking about…..
    - How long did it take to get blocked????
      - Immediately = IPS
      - 2-4 hours = IDS/SIEM/SOC
      - Following day = Admin looking at logs
- Bannergrab
- Vulnerability Research
- Exploit

Simple Process – Bannergrab

The Methodology

- Ping Sweep
- Port Scan
- **Bannergrab**
  - nc 172.31.6.15 80
    HEAD /HTTP/1.1 [ENTER][ENTER]
  - nmap -sV -p 21 172.31.6.15
  - HTTPS/IMAPS/POP3S
  - $ openssl s_client -connect 172.31.6.15:443 <-- HTTPS HEAD / HTTP/1.1 [enter][enter]
  - $ openssl s_client -connect 172.31.6.15:993 <-- IMAPS
  - $ openssl s_client -connect 172.31.6.15:995 <-- POP3S
- Vulnerability Research
- Exploit

Simple Process – Vulnerability Research

The Methodology

- Ping Sweep
- Port Scan
- Bannergrab
- **Vulnerability Research**
  - www.securityfocus.com/bid
  - www.exploit-db.com
  - www.packetstormsecurity.org

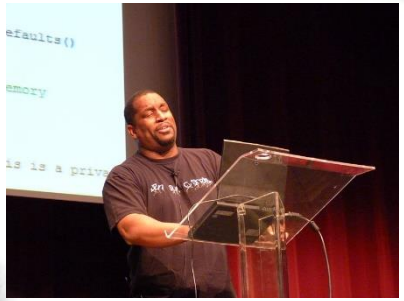
- Exploit

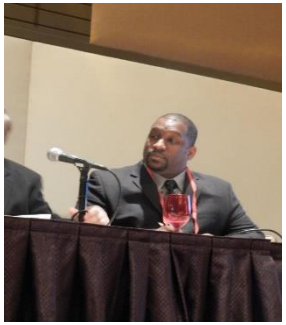
Simple Process - Exploit

The Methodology

- Ping Sweep
- Port Scan
- Bannergrab
- Vulnerability Research
- Exploit
  - gcc exploit.c -o exploit
    ./exploit
  - sh exploit.sh
  - perl exploit.pl
  - python exploit.py
  - METASPLOIT

What Would Joe Do?





The j0e way….

Nmap Tricks From Last Week

Let’s use some nmap tricks to help us find hosts

```
$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | grep open

$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | awk '/open/{print $2 " " $3}'

$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | awk '/open/{print $2}' | wc -l

$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | awk '/open/{print $2}'

$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | awk '/open/{print $2}'

$ sudo nmap -Pn -sV -T 5 -oG - -p 21,22,80,443,1433,3389 172.31.6.* | awk '/open/{print $2}' > ~/labnet-ip-list.txt
```

How Did I Do It?

I would use propecia (no not the hair loss product)

$ wget --no-check-certificate https://dl.packetstormsecurity.net/UNIX/scanners/propecia.c

$ gcc propecia.c -o propecia

$ sudo cp propecia /bin

$ sudo chmod 777 /bin/propecia

$ propecia 172.31.6 22

$ propecia 172.31.6 111

$ propecia 172.31.6 445

$ propecia 172.31.6 3389

How Did I Do It?

I would use propecia (no not the hair loss product)

$ wget --no-check-certificate https://dl.packetstormsecurity.net/UNIX/scanners/propecia.c

$ gcc propecia.c -o propecia

$ sudo cp propecia /bin

$ sudo chmod 777 /bin/propecia

$ propecia 172.31.6 22 Linux Hosts

$ propecia 172.31.6 111

$ propecia 172.31.6 445

$ propecia 172.31.6 3389

How Did I Do It?

I would use propecia (no not the hair loss product)

$ wget --no-check-certificate https://dl.packetstormsecurity.net/UNIX/scanners/propecia.c

$ gcc propecia.c -o propecia

$ sudo cp propecia /bin

$ sudo chmod 777 /bin/propecia

$ propecia 172.31.6 22

$ propecia 172.31.6 111

$ propecia 172.31.6 445 Windows Hosts

$ propecia 172.31.6 3389

Nmap NSE to the rescue

Here are some things you should try in the network

sudo nmap -Pn -n --open -p21 --script=banner,ftp-anon,ftp-bounce,ftp-proftpd-backdoor,ftp-vsftpd-backdoor 172.31.6.0/24

sudo nmap -Pn -n --open -p22 --script=sshv1,ssh2-enum-algos 172.31.6.0/24

sudo nmap -Pn -n -sU --open -p53 --script=dns-blacklist,dns-cache-snoop,dns-nsec-enum,dns-nsid,dns-random-srcport,dns-random-txid,dns-recursion,dns-service-discovery,dns-update,dns-zeustracker,dns-zone-transfer 172.31.6.0/24

sudo nmap -Pn -n --open -p111 --script=nfs-ls,nfs-showmount,nfs-statfs,rpcinfo 172.31.6.0/24

sudo nmap -Pn -n --open -p445 --script=msrpc-enum,smb-enum-domains,smb-enum-groups,smb-enum-processes,smb-enum-sessions,smb-enum-shares,smb-enum-users,smb-mbenum,smb-os-discovery,smb-security-mode,smb-server-stats,smb-system-info,smbv2-enabled,stuxnet-detect 172.31.6.0/24

sudo nmap -Pn -n --open -p1433 --script=ms-sql-dump-hashes,ms-sql-empty-password,ms-sql-info 172.31.6.0/24

sudo nmap -Pn -n --open -p1521 --script=oracle-sid-brute --script oracle-enum-users --script-args oracle-enum-users.sid=ORCL,userdb=orausers.txt 172.31.6.0/24

sudo nmap -Pn -n --open -p3306 --script=mysql-databases,mysql-empty-password,mysql-info,mysql-users,mysql-variables 172.31.6.0/24

sudo nmap -Pn -n --open -p3389 --script=rdp-vuln-ms12-020,rdp-enum-encryption 172.31.6.0/24

sudo nmap -Pn -n --open -p5900 --script=realvnc-auth-bypass,vnc-info 172.31.6.0/24

sudo nmap -Pn -n --open -p6000-6005 --script=x11-access 172.31.6.0/24

sudo nmap -Pn -n --open -p27017 --script=mongodb-databases,mongodb-info 172.31.6.0/24

Screenshot all web ports - 1

cd ~/toolz/

mkdir labscreenshots

cd labscreenshots/

Screenshot all web ports - 2

$ wget http://download.gna.org/wkhtmltopdf/0.12/0.12.4/wkhtmltox-0.12.4_linux-generic-amd64.tar.xz

$ tar xf wkhtmltox-0.12.4_linux-generic-amd64.tar.xz

$ cd wkhtmltox/bin/

$ sudo cp wkhtmltoimage /usr/local/bin/wkhtmltoimage-i386

Screenshot all web ports - 3

```
cd ~/toolz/
git clone git://github.com/SpiderLabs/Nmap-Tools.git
cd Nmap-Tools/NSE/
sudo cp http-screenshot.nse /usr/share/nmap/scripts/
    infosecaddicts

sudo nmap --script-updatedb
    infosecaddicts

cd ~/toolz/labscreenshots/
sudo nmap -Pn -T 5 -p 80 -A --script=http-screenshot 172.31.6.0/24 -iL
/home/infosecaddicts/labnet-ip-list.txt
    infosecaddicts
```

Screenshot all web ports - 4

vi screenshots.sh

```
#!/bin/bash
printf "<HTML><BODY><BR>" > labnet-port-80-screenshots.html
ls -1 *.png | awk -F : '{ print $1":"$2"\n<BR><IMG SRC=\""$1"%3A"$2"\"
width=400><BR><BR>"}' >> labnet-port-80-screenshots.html
printf "</BODY></HTML>" >> labnet-port-80-screenshots.html
```

Screenshot all web ports - 4

sh screenshots.sh

python -m SimpleHTTPServer

--- Now browse to the IP of your Linux machine on port 8000 (http://192.168.200.157:8000/labnet-port-80-screenshots.html):

http://Ubuntu-VM-IP:8000/labnet-port-80-screenshots.html

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
-- The Rule Section --
portrule = function(host, port)
    return port.protocol == "tcp"
            and port.number == 80
            and port.state == "open"
end

-- The Action Section --
action = function(host, port)
    return "CyberWar!"
end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse infosecaddicts.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"

-- The Rule Section --
portrule = shortport.http


-- The Action Section --
action = function(host, port)
    return "CyberWar!"
end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse infosecaddicts.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"

-- The Rule Section --
portrule = shortport.http


-- The Action Section --
action = function(host, port)
    return "CyberWar!"
end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse infosecaddicts.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"
local http = require "http"

-- The Rule Section --
portrule = shortport.http

-- The Action Section --
action = function(host, port)

    local uri = "/installing-metasploit-in-ubunt/"
    local response = http.get(host, port, uri)
    return response.status

end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse darkoperator.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"
local http = require "http"

-- The Rule Section --
portrule = shortport.http

-- The Action Section --
action = function(host, port)

    local uri = "/installing-metasploit-in-ubunt/"
    local response = http.get(host, port, uri)

    if ( response.status == 200 ) then
        return response.body
    end

end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse darkoperator.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"
local http = require "http"
local string = require "string"

-- The Rule Section --
portrule = shortport.http

-- The Action Section --
action = function(host, port)

    local uri = "/installing-metasploit-in-ubunt/"
    local response = http.get(host, port, uri)

    if ( response.status == 200 ) then
        local title = string.match(response.body, "Installing Metasploit in Ubuntu and Debian")
        return title
    end

end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse darkoperator.com -p 22,80,443

Intro to Nmap NSE

sudo vi /usr/share/nmap/scripts/intro-nse.nse

```
-- The Head Section --
local shortport = require "shortport"
local http = require "http"
local string = require "string"

-- The Rule Section --
portrule = shortport.http

-- The Action Section --
action = function(host, port)

    local uri = "/installing-metasploit-in-ubunt/"
    local response = http.get(host, port, uri)

    if ( response.status == 200 ) then
        local title = string.match(response.body, "Installing Metasploit in Ubuntu and Debian")

        if (title) then
            return "Vulnerable"
        else
            return "Not Vulnerable"
        end
    end
end
```

sudo nmap --script=/usr/share/nmap/scripts/intro-nse.nse darkoperator.com -p 22,80,443

Contact Me....

Toll Free: **1-844-458-1008**

Email: joe@strategicsec.com

Twitter: http://twitter.com/j0emccray

LinkedIn: http://www.linkedin.com/in/joemccray