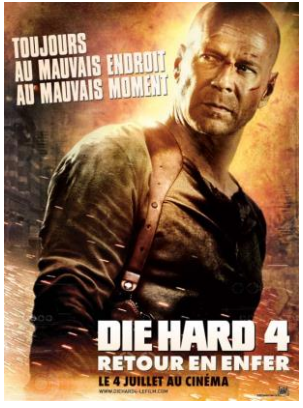
NMAP Session

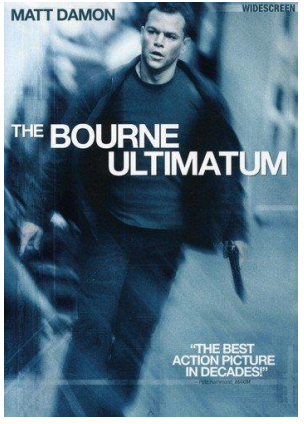
Outline

- Intro
- Who uses it?
- The Set Up
- Deep Dive
  - Syntax
  - Network Discovery
  - OS and Service Detection
  - NMAP Scripting Engine
  - Vulnerability Scanning
  - Evasion
  - ...
- Tales from the trenches
- Wrap Up
- Useful Resources

Intro

- Acronym: Network Mapper
- Free and open source (license) utility for network discovery and security auditing
- Runs on
  - Linux, Mac, Windows*
- Even featured in famous Hollywood movies.



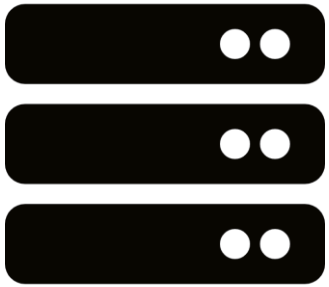


Who uses it?

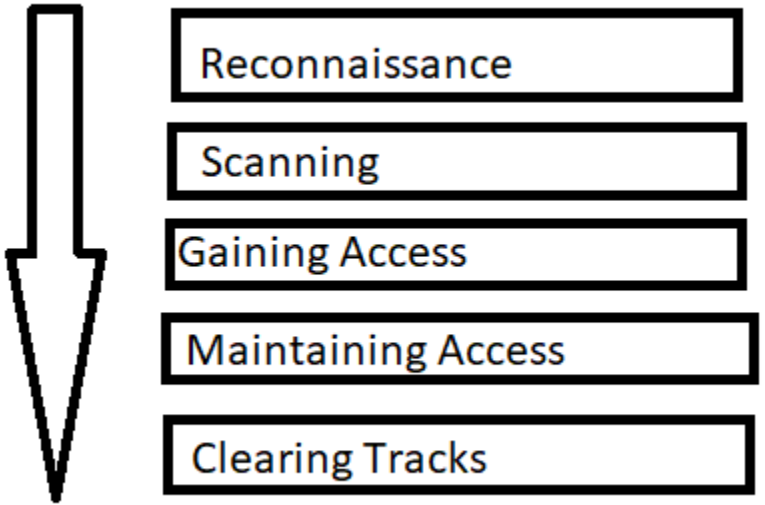
- Security Professionals
- Network Administrators
- System Administrators
- Hackers
- Developers?

What can it scan?

- Anything that has an IP Address

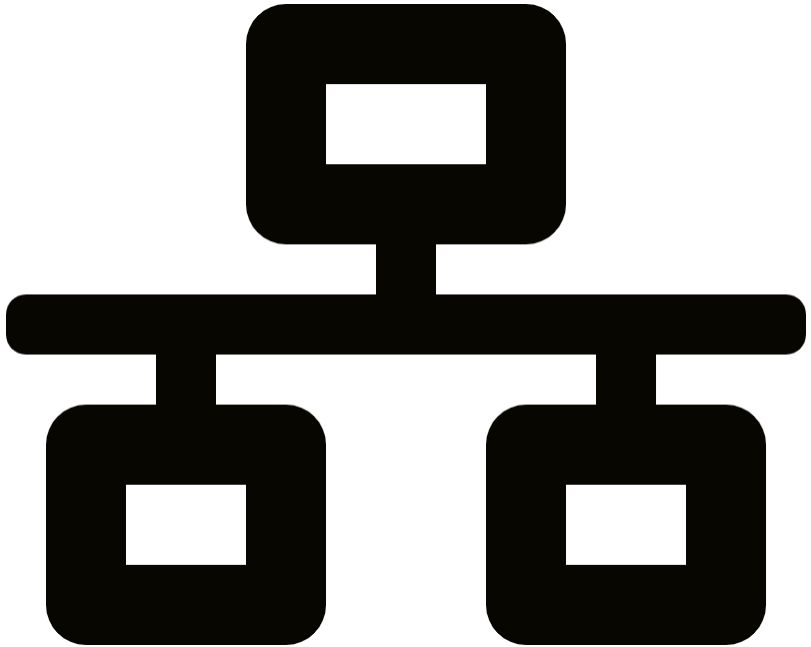


It is applicable to majority of the hacking stages



The Set up

VMWARE Workstation



Kali Linux

192.168.3.137

Metasploitable2

192.168.3.136

NAT/Host Only Adaptor

Disclaimer!

Everything discussed here is for informational and educational purposes only.

The Syntax

Recommended OS: Debian
Avoid using WSL and Windows in general

```
apt-get install nmap
yum install nmap
brew install nmap
```

```
nmap [Scan Type(s)] [Options] {target specification}
```

Network Discovery

```
root@kali:~# nmap -sn 192.168.3.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 13:56 EDT
Nmap scan report for 192.168.3.2
Host is up (0.00044s latency).
MAC Address: 00:50:56:E1:92:4E (VMware)
Nmap scan report for 192.168.3.136
Host is up (0.00055s latency).
MAC Address: 00:0C:29:FB:C3:E4 (VMware)
Nmap scan report for 192.168.3.254
Host is up (0.00071s latency).
MAC Address: 00:50:56:FB:89:76 (VMware)
Nmap scan report for 192.168.3.137
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.29 seconds
root@kali:~#
```

Port Scanning

Scans Popular Ports

```
root@kali:~# nmap 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 13:57 EDT
Nmap scan report for 192.168.3.136
Host is up (0.0027s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
root@kali:~#
```

All ports

```
root@kali:~# nmap -p- 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 13:59 EDT
Nmap scan report for 192.168.3.136
Host is up (0.0025s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35281/tcp open  unknown
46648/tcp open  unknown
47328/tcp open  unknown
58524/tcp open  unknown
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
root@kali:~#
```

Version Detection

```
root@kali:~# nmap -sV 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 14:04 EDT
Nmap scan report for 192.168.3.136
Host is up (0.0018s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
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  rmiregistry 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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FB:C3:E4 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.84 seconds
root@kali:~#
```

OS Detection

```
root@kali:~# nmap -O 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 14:07 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00090s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FB:C3:E4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds
root@kali:~#
```

Scripting Engine

```
root@kali:~# ls /usr/share/nmap/scripts/
acarsd-info.nse                         hostmap-crtsh.nse                       ip-geolocation-geoplugin.nse    rpcinfo.nse
address-info.nse                        hostmap-ip2hosts.nse                    ip-geolocation-ipinfodb.nse     rsa-vuln-roca.nse
afp-brute.nse                           hostmap-robtex.nse                      ip-geolocation-map-bing.nse     rsync-brute.nse
afp-ls.nse                              http-adobe-coldfusion-apsa1301.nse      ip-geolocation-map-google.nse   rsync-list-modules.nse
afp-path-vuln.nse                       http-affiliate-id.nse                   ip-geolocation-map-kml.nse      rtsp-methods.nse
afp-serverinfo.nse                      http-apache-negotiation.nse             ip-geolocation-maxmind.nse      rtsp-url-brute.nse
afp-showmount.nse                       http-apache-server-status.nse           ip-https-discover.nse           rusers.nse
ajp-auth.nse                            http-aspnet-debug.nse                   ipidseq.nse                     s7-info.nse
ajp-brute.nse                           http-auth-finder.nse                    ipmi-brute.nse                  samba-vuln-cve-2012-1182.nse
ajp-headers.nse                         http-auth.nse                           ipmi-cipher-zero.nse            script.db
ajp-methods.nse                         http-avaya-ipoffice-users.nse           ipmi-version.nse                servicetags.nse
ajp-request.nse                         http-awstatstotals-exec.nse             ipv6-multicast-mld-list.nse     shodan-api.nse
allseeingeye-info.nse                   http-axis2-dir-traversal.nse            ipv6-node-info.nse              sip-brute.nse
amqp-info.nse                           http-backup-finder.nse                  ipv6-ra-flood.nse               sip-call-spoof.nse
asn-query.nse                           http-barracuda-dir-traversal.nse        irc-botnet-channels.nse         sip-enum-users.nse
auth-owners.nse                         http-bigip-cookie.nse                   irc-brute.nse                   sip-methods.nse
auth-spoof.nse                          http-brute.nse                          irc-info.nse                    skypev2-version.nse
backorifice-brute.nse                   http-cakephp-version.nse                irc-sasl-brute.nse              smb2-capabilities.nse
backorifice-info.nse                    http-chrono.nse                         irc-unrealircd-backdoor.nse     smb2-security-mode.nse
bacnet-info.nse                         http-cisco-anyconnect.nse               iscsi-brute.nse                 smb2-time.nse
banner.nse                              http-coldfusion-subzero.nse             iscsi-info.nse                  smb2-vuln-uptime.nse
bitcoin-getaddr.nse                     http-comments-displayer.nse             isns-info.nse                   smb-brute.nse
bitcoin-info.nse                        http-config-backup.nse                  jdwp-exec.nse                   smb-double-pulsar-backdoor.nse
bitcoinrpc-info.nse                     http-cookie-flags.nse                   jdwp-info.nse                   smb-enum-domains.nse
bittorrent-discovery.nse                http-cors.nse                           jdwp-inject.nse                 smb-enum-groups.nse
bjnp-discover.nse                       http-cross-domain-policy.nse            jdwp-version.nse                smb-enum-processes.nse
broadcast-ataoe-discover.nse            http-csrf.nse                           knx-gateway-discover.nse        smb-enum-services.nse
broadcast-avahi-dos.nse                 http-date.nse                           knx-gateway-info.nse            smb-enum-sessions.nse
broadcast-bjnp-discover.nse             http-default-accounts.nse               krb5-enum-users.nse             smb-enum-shares.nse
broadcast-db2-discover.nse              http-devframework.nse                   ldap-brute.nse                  smb-enum-users.nse
broadcast-dhcp6-discover.nse            http-dlink-backdoor.nse                 ldap-novell-getpass.nse         smb-flood.nse
broadcast-dhcp-discover.nse             http-dombased-xss.nse                   ldap-rootdse.nse                smb-ls.nse
broadcast-dns-service-discovery.nse     http-domino-enum-passwords.nse          ldap-search.nse                 smb-mbenum.nse
broadcast-dropbox-listener.nse          http-drupal-enum.nse                    lexmark-config.nse              smb-os-discovery.nse
broadcast-eigrp-discovery.nse           http-drupal-enum-users.nse              llmnr-resolve.nse               smb-print-text.nse
broadcast-igmp-discovery.nse            http-enum.nse                           lltd-discovery.nse              smb-protocols.nse
```

592 scripts as of today

User accounts enumeration

```
root@kali:~# nmap -p 445 --script smb-enum-users.nse 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-23 13:16 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00055s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Account disabled, Normal user account
```

DNS whois lookup

```
| Domain Name: CMU.EDU
|
| Registrant:
|       Carnegie Mellon University
|       Cyert Hall 216
|       5000 Forbes Avenue
|       Pittsburgh, PA 15213
|       US
|
| Administrative Contact:
|       Host Master
|       Carnegie Mellon University
|       Cyert Hall 216
|       5000 Forbes Ave
|       Pittsburgh, PA 15213-3890
|       US
|       +1.4122684357
|       host-master@andrew.cmu.edu
|
| Technical Contact:
|       Host Master
|       Carnegie Mellon University
|       Cyert Hall 216
|       5000 Forbes Ave
|       Pittsburgh, PA 15213-3890
|       US
|       +1.4122684357
|       host-master@andrew.cmu.edu
|
| Name Servers:
|       NSAUTH1.NET.CMU.EDU
|       NSAUTH2.NET.CMU.EDU
|       NY-SERVER-03.NET.CMU.EDU
|
| Domain record activated:    24-Apr-1985
| Domain record last updated: 26-Sep-2020
|_Domain expires:             31-Jul-2021
```

```
nmap --script whois-domain.nse cmu.edu
```

Vulnerability Scanning

```
root@kali:~# nmap --script vuln 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 14:08 EDT
Nmap scan report for 192.168.3.136
Host is up (0.0018s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       http://osvdb.org/73573
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_sslv2-drown:
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
```

Let’s dig into the vsftpd vulnerability

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -p 21 --script ftp-vsftpd-backdoor.nse 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-23 13:31 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00050s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://osvdb.org/73573
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION#
```

Mysql root empty password

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -p 3306 --script mysql-empty-password 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-23 15:00 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00060s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-empty-password:
|_  root account has empty password
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
```

Brute Force

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap --script ftp-brute -p 21 -Pn 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-24 02:27 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00059s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 3688 guesses in 603 seconds, average tps: 6.1
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 603.09 seconds
```

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# ftp 192.168.3.136
Connected to 192.168.3.136.
220 (vsFTPd 2.3.4)
Name (192.168.3.136:root): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Malware Detection

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -sV --script=http-malware-host -p 80 192.168.3.136
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-24 02:54 EDT
Nmap scan report for 192.168.3.136
Host is up (0.00063s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-malware-host: Host appears to be clean
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 00:0C:29:FB:C3:E4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION#
```

WAF Detection

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -p80,443 --script http-waf-detect --script-args="http-waf-detect.aggro,http-waf-detect.detectBodyChanges" abdihakx.wordpress.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-24 05:21 EDT
Nmap scan report for abdihakx.wordpress.com (192.0.78.13)
Host is up (0.050s latency).
Other addresses for abdihakx.wordpress.com (not scanned): 192.0.78.12

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_abdihakx.wordpress.com:443/?p4yl04d=hostname%00

Nmap done: 1 IP address (1 host up) scanned in 20.86 seconds
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION#
```

Fingerprinting WAF

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -p80,443 --script http-waf-fingerprint --script-args http-waf-fingerprint.intensive=1 cloudflare.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-24 05:27 EDT
Nmap scan report for cloudflare.com (104.17.176.85)
Host is up (0.018s latency).
Other addresses for cloudflare.com (not scanned): 104.17.175.85 2606:4700::6811:b055 2606:4700::6811:af55

PORT    STATE SERVICE
80/tcp  open  http
| http-waf-fingerprint:
|   Detected WAF
|_    Cloudflare
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION#
```

Extracting Image Metadata

```
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION# nmap -p80,443 --script http-exif-spider javaop.com
Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-24 05:46 EDT
Nmap scan report for javaop.com (96.126.121.223)
Host is up (0.070s latency).
rDNS record for 96.126.121.223: li370-223.members.linode.com

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
| http-exif-spider:
|   https://javaop.com:443/Nationalmuseum.jpg
|     Make: Canon
|     Model: Canon PowerShot S100\xB4
|_    Date: 2003:03:29 13:35:40

Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
root@kali:~/CMU_AFRICA_SEC_CLUB_SESSION#
```

Let’s write our own script

```
git clone https://github.com/abdihakx/cmu_sec_club.git
```

Saving NMAP output

-oN: Normal
-oX: XML
-oG: Grepable format
-oA: Output in the three major formats at once

```
nmap 192.168.3.136 -oX metasploitable_scan.xml && xsltproc
metasploitable_scan.xml -o metasploitable_report.html
```

Everything we did so far was very noisy

Going stealth

-sS: Stealth Scan

```
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

Zenmap

- NMAP’s GUI version
- Runs on Windows as well
  - Misbehaves sometimes
    - BSOD

Things NMAP Can’t do very well

- Mass Scanning of IP addresses
  - Try Massscan
    - Does Asynchronous TCP Scanning

Automation?

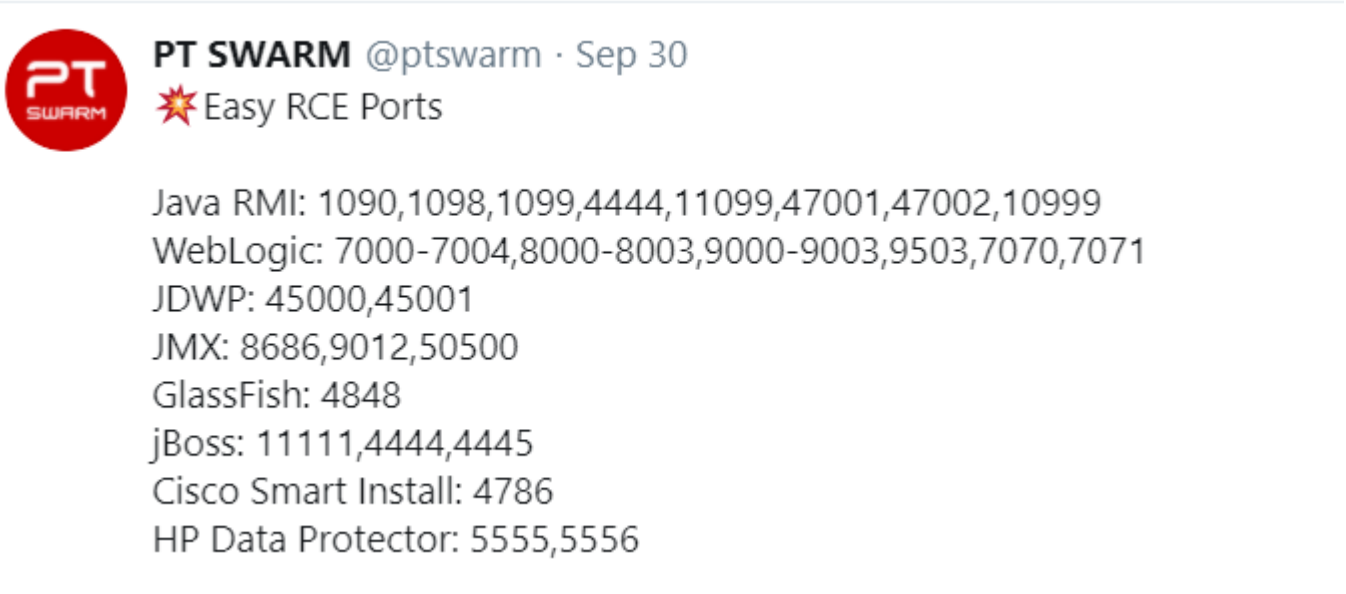
- Shell scripts
  - Nmap commands
- Cron jobs
  - Send nmap scan reports to email

Tales from the trenches

NMAP tricks I found helpful

- -Pn: Scan without piniging
- -p-: Scan all ports
- -sU: UDP

Check these out next time you are on a network



PT SWARM @ptswarm · Sep 30

💥 Easy RCE Ports

Java RMI: 1090,1098,1099,4444,11099,47001,47002,10999
WebLogic: 7000-7004,8000-8003,9000-9003,9503,7070,7071
JDWP: 45000,45001
JMX: 8686,9012,50500
GlassFish: 4848
jBoss: 11111,4444,4445
Cisco Smart Install: 4786
HP Data Protector: 5555,5556

Wrap Up

- NMAP is a double-edged sword
- It is noisy
  - Go stealth
- It is even much when used with other tools - Metasploit, ncat
- We just scratched the surface of what it can do
- Beware of false positives

Useful Resources

- Nmap.org
- https://www.youtube.com/watch?v=ltEFbi_I2KY
- https://www.stationx.net/nmap-cheat-sheet/
- https://www.youtube.com/watch?v=7XMIFTRiAGA
- https://www.lua.org/manual/5.1/

Thank You