

Scanning your (large) network with Nmap

Brandon Enright, bmenrigh@ucsd.edu

Presentation at: http://noh.ucsd.edu/~bmenrigh/nmap_ddcsw.pdf

Code available at: http://noh.ucsd.edu/~bmenrigh/nmap_ddcsw.tar.gz



Nmap isn't just another fast port scanner anymore.

Nmap has two features that are exceptionally good at finding compromised hosts:

- Service Versioning (-sV)
 - Connects to each open port and sends a series of probes
 - Responses are matched against a huge list of regular expressions
- Script Scanning (-sC)
 - Runs a series of scripts against the host, open ports, or external services to provide information
 - Much like what you can get out of Nessus, Hydra, Metasploit, etc



So what can this scanning find?

- Open ports (typically not terribly interesting)
- Running services (semi-interesting)

- Backdoors, shells, open consoles, etc
- FTP servers, Pubstros, etc
- Malware listeners
- Open proxies

- Lots more

There are barriers to scanning

The simple one-host scan:

```
$ nmap -v -p- -T5 target.school.edu
```

doesn't scale well when you want to scan a few /16s

The simple /16 network scan:

```
$ nmap -v -p- -T5 x.y.0.0/16
```

also doesn't work because it would take months to finish

Problems getting Nmap to scale

- Memory usage of large hostgroups
- Occasional bugs in Nmap
- Each hostgroup only as fast as slowest host
- Global Congestion Control needs work

My scaling solution: fastnmap.pl

- Simple
- Written in perl
- Handles running many Nmap instances in parallel
- Measures past performance to calculate needed parallelism
- Reports progress
- Prevents memory exhaustion
- Is a deadline-based scan scheduler

fastnmap.pl screenshot

```
Terminal - bmenrigh@asplode:~
File Edit View Terminal Go Help
Average thread-work-factor: 5.95 mIST
Currently using 51 threads, will finish at Thu May 28 14:04:59 2009 UTC
Target off of goal by -247.36 minutes
Network rate: TX 40413 pps (2.24 MBps); RX 775 pps (0.05 MBps)
-----
Scan started at Thu May 21 18:12:21 2009 UTC
Goal end time at Thu May 28 18:12:21 2009 UTC
6700 IPs done (3.66%) in 21611 seconds with 52.06 average threads
Average thread-work-factor: 5.96 mIST
Currently using 51 threads, will finish at Thu May 28 14:05:39 2009 UTC
Target off of goal by -246.69 minutes
Network rate: TX 40429 pps (2.24 MBps); RX 778 pps (0.05 MBps)
-----
Scan started at Thu May 21 18:12:21 2009 UTC
Goal end time at Thu May 28 18:12:21 2009 UTC
6800 IPs done (3.72%) in 21902 seconds with 52.05 average threads
Average thread-work-factor: 5.97 mIST
Currently using 51 threads, will finish at Thu May 28 13:51:30 2009 UTC
Target off of goal by -260.83 minutes
Network rate: TX 40459 pps (2.24 MBps); RX 780 pps (0.05 MBps)
-----
0*flexmap 1- npwn 1 2 npwn 2
[asplode] Load: 5.32 5.89 5.73 2009-05-22 0:19:31
```



Now that you can scan 3+ /16s how do you analyze the data? npwn.pl

- Output is simple
- Supports exclude lists
- Handles Normal and XML Nmap output
- Easily extensible (by changing the code)
- Easily scales to any network size

npwn.pl screenshot 1

```
Terminal - bmenrigh@asplode:~
File Edit View Terminal Go Help
bmenrigh@asplode ~/npwn $ ./displayfullnpwn_xml
{98}:
-----
{1} [SMTP] -- SMTP server on 25 is Microsoft ESMTP 6.0.3790.3959
{1} [HTTP] -- Web server on 80 is Microsoft IIS webserver 6.0
{1} [HTTP] -- Web server on 120 is Microsoft IIS httpd
{1} [HTTP] -- Web server on 4640 is Microsoft IIS webserver 6.0
{1} [HTTP] -- Web server on 6859 is Microsoft IIS webserver 6.0
{4} [SMB_OTHERPASS] -- SMB user/pass "rsvpevent" / "rsvpevent" caused Password
was correct, but user's account is disabled
{4} [SMB_OTHERPASS] -- SMB user/pass "sqlserv" / "sqlserv" caused Password was
correct, but user's account is disabled
{5} [SMB_SAMR] -- Was able to enumerate 237 users with SAMR
{8} [SMB_WEAKPASS] -- SMB user "emlibraryuser" has password "emlibraryuser"
{8} [SMB_WEAKPASS] -- SMB user "nizamova" has password "nizamova"
{8} [SMB_WEAKPASS] -- SMB user "nretonel" has password "<blank>"
{8} [SMB_WEAKPASS] -- SMB user "nt authority_network" has password "<blank>"
{8} [SMB_WEAKPASS] -- SMB user "rjones" has password
{8} [SMB_WEAKPASS] -- SMB user "rtomas" has password "<blank>"
{8} [SMB_WEAKPASS] -- SMB user "tfsreports" has password "tfsreports"
{8} [SMB_WEAKPASS] -- SMB user "tfsservice" has password "tfsservice"
{8} [SMB_WEAKPASS] -- SMB user "tfssetup" has password "tfssetup"
0- flexmap 1*npwn 1 2 npwn 2
[asplode] Load: 4.55 5.01 5.15 2009-05-22 0:43:52
```



npwn.pl screenshot 2

```
Terminal - bmenrigh@asplode:~
File Edit View Terminal Go Help
132.239.246.51 {3}:
-----
{3} [SOHOSSHD] -- Port 22 running Dropbear sshd.

132.239.27.67 (dale.ucsd.edu) {13}:
-----
{6} [IRCD] -- IRC server on 6667 is IRCnet-based ircd

132.239.8.87 (oec-server7.ucsd.edu) {37}:
-----
{9} [FTPSECURE] -- FTP service on 21 is pretending to be security service

132.239.85.60 (vmrflifesize.ucsd.edu) {5}:
-----
{3} [ASCIILINE] -- ASCII line art on 1167 found

132.239.9.99 (lec3.ucsd.edu) {14}:
-----
{6} [IRCD] -- IRC server on 6667 is ngircd
{6} [IRCD] -- IRC server on 6669 is ngircd

132.239.95.195 (applepie.ucsd.edu) {8}:
0- flexmap 1*npwn 1 2 npwn 2
[asplode] Load: 5.76 5.00 5.08 2009-05-22 0:47:13
```



npwn.pl screenshot 3

```
Terminal - bmenrigh@asplode:~
File Edit View Terminal Go Help
{1} [SMTP] -- SMTP server on 25 is Sendmail 8.14.3/8.14.3/IH
{1} [HTTP] -- Web server on 80 is Apache httpd 1.3.41 ((Unix) mod_jk/1.2.1)
{1} [POP3] -- POP3 server on 110 is Qpopper pop3d 4.0.9 (possible unencrypted a
{1} [IMAP] -- IMAP server on 143 is UW imapd 2004.357 (possible unencrypted aut
{1} [SMTP] -- SMTP server on 587 is Sendmail 8.14.3/8.14.3/IH
{1} [HTTP] -- Web server on 898 is Sun Solaris Management Console (Runs Tomcat
{1} [HTTP] -- Web server on 1705 is Apache httpd 1.3.41 ((Unix) mod_jk/1.2.1)
{1} [HTTP] -- Web server on 5988 is Sun Solaris Management Console (Runs Tomcat
{2} [FTP] -- FTP server on 21
{2} [SUNRPC] -- Sun RPC on 111
{2} [SUNRPC] -- Sun RPC on 4045
{2} [SUNRPC] -- Sun RPC on 32771
{2} [SUNRPC] -- Sun RPC on 32781
{2} [SUNRPC] -- Sun RPC on 32782
{3} [MULTI_RADMIN] -- Machine running multiple remote administration packages
{5} [FTPF] -- FTP server on 9990 found in fingerprint
{5} [FTPF] -- FTP server on 9992 found in fingerprint
{5} [SSLV2] -- Service on 993 supports SSLv2
{7} [POP3WEAKAUTHNOSSL] -- POP3 server on 110 supports plaintext authentication
{7} [IMAPWEAKAUTHNOSSL] -- IMAP server on 143 supports plaintext authentication
{8} [SSLV2 40BIT] -- Service on 993 supports 40-bit SSLv2
lines 7-27/28 99%
0- flexmap 1*npwn 1 2 npwn 2
[asplode] Load: 6.01 5.40 5.22 2009-05-22 0:50:26
```



Just like Nmap, npwn.pl can give you information overload but Npwn supports excludes

- By individual host
- By specific problem
- By network
- Exclude format is simple

npwn.pl example exclude file

```
Terminal - bmenrigh@asplode:~
File Edit View Terminal Go Help
group @campus 132.239.0.0/16 137.110.0.0/16 128.54.0.0/17
@campus WSD SSDP STCP NOPASSWD OLDTCPPIP HTTP_PROXY SQUID SOHOHTTPD FTP SMTP HTTP
MYSQL MSSQL MULTI_ADMIN NNTP IPHONE OLD_MSFTP OLD_MSSMTP SYNERGY LOGMEIN OPENX
11 MANYPORTS SOCKS_MULTI_SSHPORTS IMAP POP3 WAP TELNET SUNRPC MULTI_SQLDB MULTI_
SSHD SMB_LSA SMB_SAMR SMB_OTHERPASS MS08-067_LIKELY MAYBEWAP SMB_GUEST NSFTP PRI
NTER_HTTP_PRINTER_FTP_PRINTER_CUPS_PRINTER_TELNET_JETDIRECT POP3WEAKAUTH POP3WEA
KAUTHNOSSL IMAPWEAKAUTH IMAPWEAKAUTHNOSSL SMB_WEAKPASS SSLV2 SSLV2_40BIT
128.54.128.0/17 WSD SSDP HTTP IPHONE OLDTCPPIP SOCKS TELNET MS08-067_LIKELY SMB_L
SA SMB_SAMR FTP SQUID WAP MAYBEWAP SMB_OTHERPASS PRINTER_CUPS
137.110.222.0/24 BADPORT
132.239.119.242 L33TSPEAK
group @iwdc 132.239.2.20 132.239.2.24 132.239.2.57 132.239.2.58 132.239.2.59 132
.239.2.60
@iwdc IRCD
132.239.1.230 OPENHTTPPROXY
awknowledged.npwn lines 1-14/153 21%
0- flexmap 1*npwn 1 2 npwn 2
[asplode] Load: 5.39 5.52 5.31 2009-05-22 0:54:54
```



Putting it all together

Nmap has had many additions and improvements done recently and is quickly becoming a good vulnerability and application scanner to augment the port scanning ability.

Nmap can be hard to use to scale to large networks but with `fastnmap.pl` and `npwn.pl` the process of scanning and analysis is mostly automated.

You should be scanning your network for compromised hosts.

Questions?