Module 11: Additional Scanning Tools

Scanning with Masscan

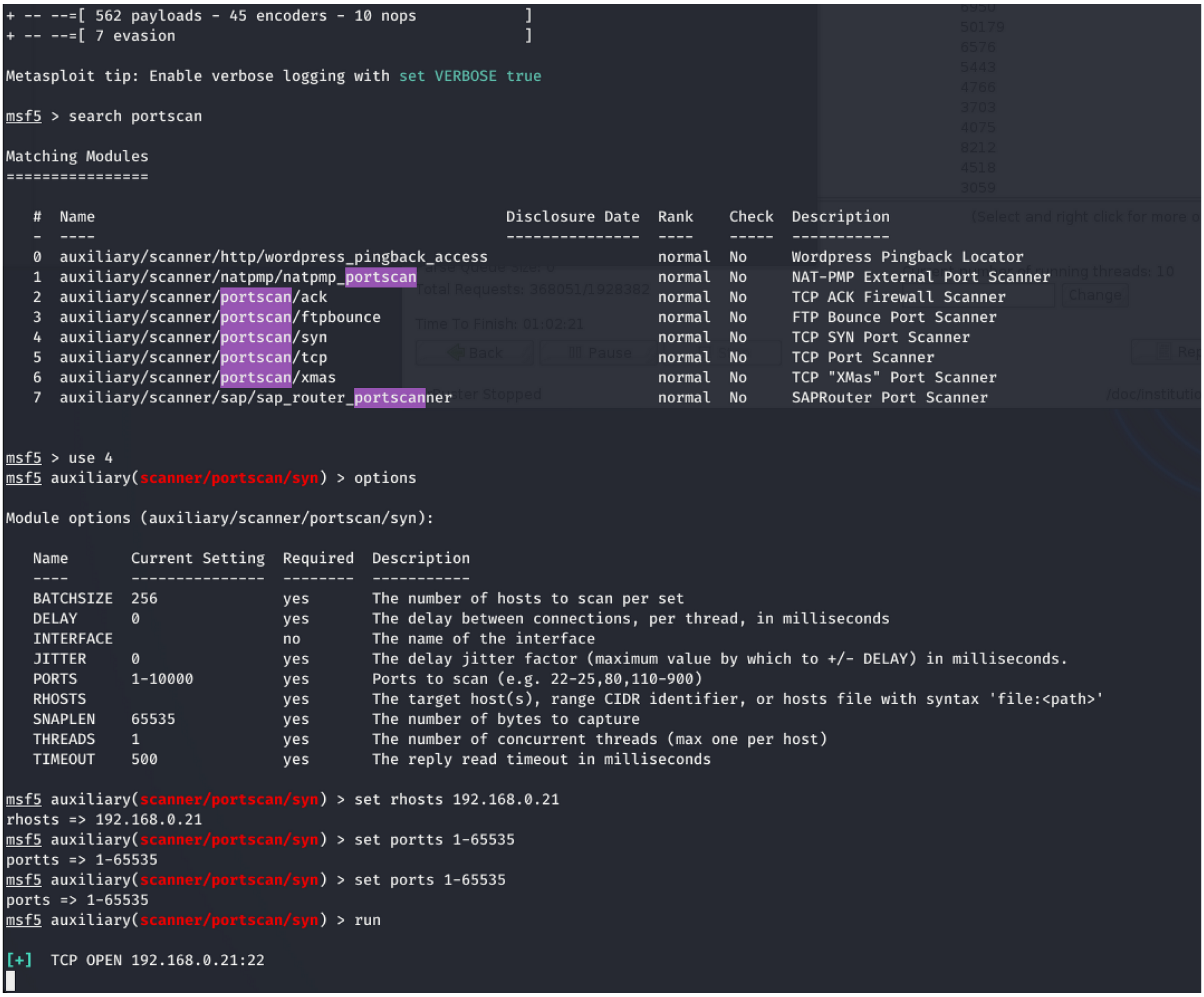
-Built to scan the entire internet very fast.

Don't Do this

This is pretty slow.

Syntax: masscan -p65535 192.168.0.21

Scanning with Metasploit



```
+ -- --=[ 562 payloads - 45 encoders - 10 nops          ]
+ -- --=[ 7 evasion                                      ]

Metasploit tip: Enable verbose logging with set VERBOSE true

msf5 > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/wordpress_pingback_access                   normal  No     Wordpress Pingback Locator
   1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/portscan/ack                                     normal  No     TCP ACK Firewall Scanner
   3  auxiliary/scanner/portscan/ftpbounce                               normal  No     FTP Bounce Port Scanner
   4  auxiliary/scanner/portscan/syn                                     normal  No     TCP SYN Port Scanner
   5  auxiliary/scanner/portscan/tcp                                     normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/xmas                                    normal  No     TCP "XMas" Port Scanner
   7  auxiliary/scanner/sap/sap_router_portscanner                       normal  No     SAPRouter Port Scanner


msf5 > use 4
msf5 auxiliary(scanner/portscan/syn) > options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf5 auxiliary(scanner/portscan/syn) > set rhosts 192.168.0.21
rhosts => 192.168.0.21
msf5 auxiliary(scanner/portscan/syn) > set portts 1-65535
portts => 1-65535
msf5 auxiliary(scanner/portscan/syn) > set ports 1-65535
ports => 1-65535
msf5 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.0.21:22
```

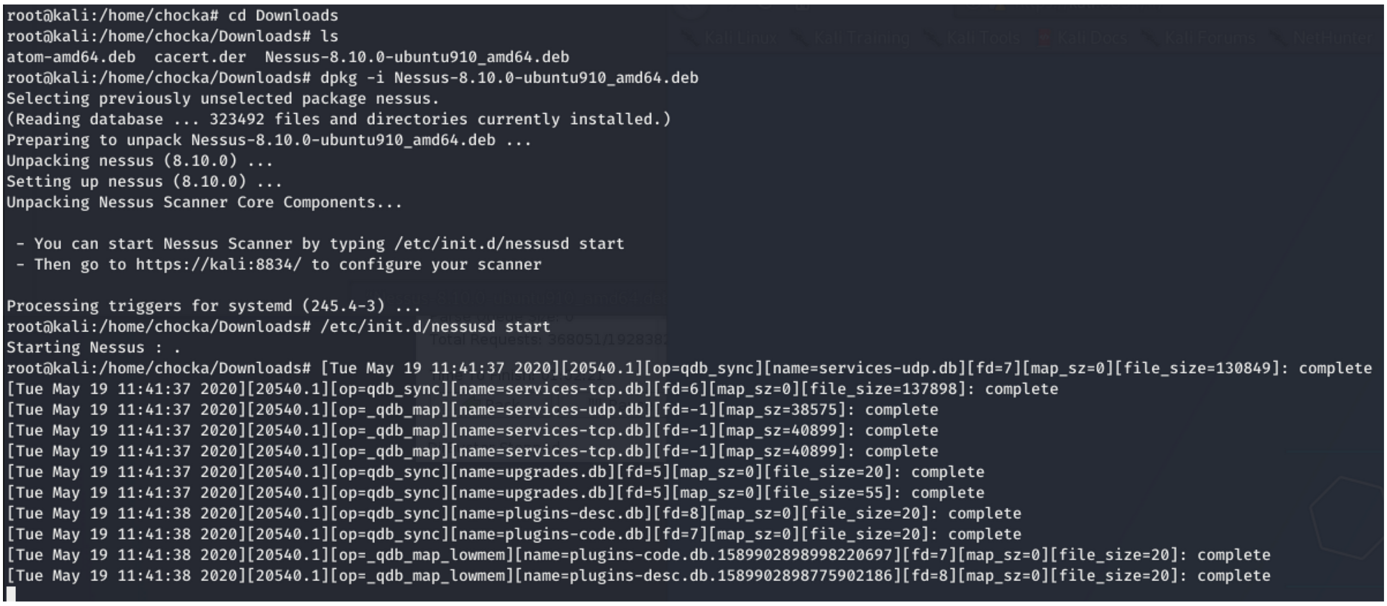
Nessus - Vulnerability scanner

To install:

https://www.tenable.com/downloads/nessus?loginAttempted=true

Debian/ubuntu 64bit

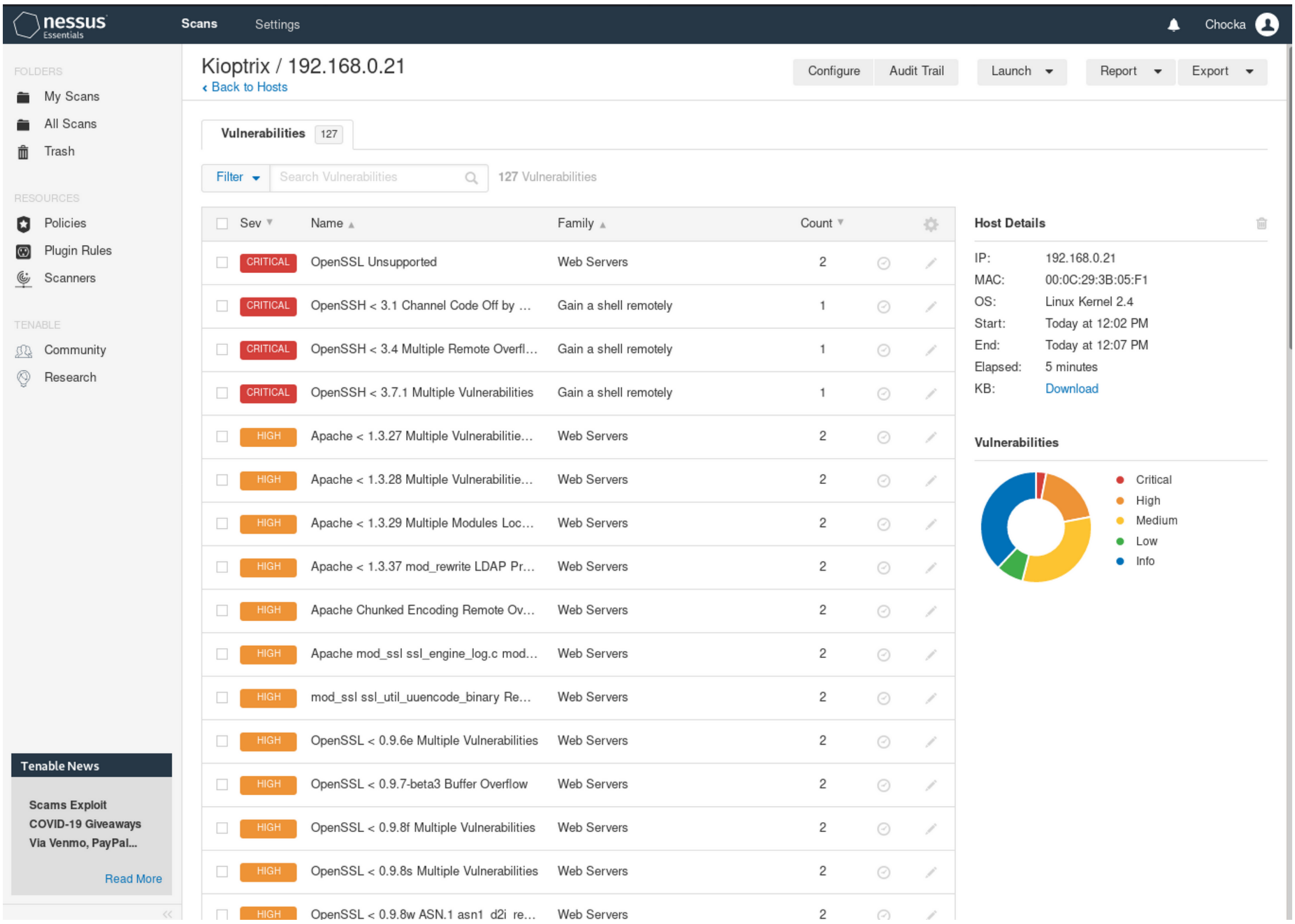
dpkg -i "Downloaded Nessus file"



```
root@kali:/home/chocka# cd Downloads
root@kali:/home/chocka/Downloads# ls
atom-amd64.deb  cacert.der  Nessus-8.10.0-ubuntu910_amd64.deb
root@kali:/home/chocka/Downloads# dpkg -i Nessus-8.10.0-ubuntu910_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 323492 files and directories currently installed.)
Preparing to unpack Nessus-8.10.0-ubuntu910_amd64.deb ...
Unpacking nessus (8.10.0) ...
Setting up nessus (8.10.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (245.4-3) ...
root@kali:/home/chocka/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:/home/chocka/Downloads# [Tue May 19 11:41:37 2020][20540.1][op=qdb_sync][name=services-udp.db][fd=7][map_sz=0][file_size=130849]: complete
[Tue May 19 11:41:37 2020][20540.1][op=qdb_sync][name=services-tcp.db][fd=6][map_sz=0][file_size=137898]: complete
[Tue May 19 11:41:37 2020][20540.1][op=_qdb_map][name=services-udp.db][fd=-1][map_sz=38575]: complete
[Tue May 19 11:41:37 2020][20540.1][op=_qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Tue May 19 11:41:37 2020][20540.1][op=_qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Tue May 19 11:41:37 2020][20540.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=20]: complete
[Tue May 19 11:41:37 2020][20540.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=55]: complete
[Tue May 19 11:41:38 2020][20540.1][op=qdb_sync][name=plugins-desc.db][fd=8][map_sz=0][file_size=20]: complete
[Tue May 19 11:41:38 2020][20540.1][op=qdb_sync][name=plugins-code.db][fd=7][map_sz=0][file_size=20]: complete
[Tue May 19 11:41:38 2020][20540.1][op=_qdb_map_lowmem][name=plugins-code.db.1589902898998220697][fd=7][map_sz=0][file_size=20]: complete
[Tue May 19 11:41:38 2020][20540.1][op=_qdb_map_lowmem][name=plugins-desc.db.1589902898775902186][fd=8][map_sz=0][file_size=20]: complete
```



Tenable News

Scams Exploit COVID-19 Giveaways Via Venmo, PayPal...

Read More

Kioptrix / 192.168.0.21

‹ Back to Hosts

Vulnerabilities 127

127 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	OpenSSL Unsupported	Web Servers	2
CRITICAL	OpenSSH < 3.1 Channel Code Off by ...	Gain a shell remotely	1
CRITICAL	OpenSSH < 3.4 Multiple Remote Overfl...	Gain a shell remotely	1
CRITICAL	OpenSSH < 3.7.1 Multiple Vulnerabilities	Gain a shell remotely	1
HIGH	Apache < 1.3.27 Multiple Vulnerabilitie...	Web Servers	2
HIGH	Apache < 1.3.28 Multiple Vulnerabilitie...	Web Servers	2
HIGH	Apache < 1.3.29 Multiple Modules Loc...	Web Servers	2
HIGH	Apache < 1.3.37 mod_rewrite LDAP Pr...	Web Servers	2
HIGH	Apache Chunked Encoding Remote Ov...	Web Servers	2
HIGH	Apache mod_ssl ssl_engine_log.c mod...	Web Servers	2
HIGH	mod_ssl ssl_util_uuencode_binary Re...	Web Servers	2
HIGH	OpenSSL < 0.9.6e Multiple Vulnerabilities	Web Servers	2
HIGH	OpenSSL < 0.9.7-beta3 Buffer Overflow	Web Servers	2
HIGH	OpenSSL < 0.9.8f Multiple Vulnerabilities	Web Servers	2
HIGH	OpenSSL < 0.9.8s Multiple Vulnerabilities	Web Servers	2
HIGH	OpenSSL < 0.9.8w ASN.1 asn1_d2i_re...	Web Servers	2

Host Details

IP: 192.168.0.21
MAC: 00:0C:29:3B:05:F1
OS: Linux Kernel 2.4
Start: Today at 12:02 PM
End: Today at 12:07 PM
Elapsed: 5 minutes
KB: Download

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

- You can download and convert (Excel File) this nessus scan results to give to clients.