NeXpose via MSFconsole a11y.text NeXpose via MSFconsole NeXpose Vulnerability Scanning in Metasploit a11y.text NeXpose Vulnerability Scanning in Metasploit The Metasploit/NeXpose integration is not limited to simply importing scan results files. You can run NeXpose scans directly from msfconsole by first making use of the nexpose plugin. msf > load nexpose

â–„â–„â–„ â–„â–„â–„ â–„â–„â–„â–„ â–„â–„â–„â–„
â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ
â–ˆâ–ˆâ–ˆâ€â–ˆ â–ˆâ–ˆâ–ˆ â–„â–ˆâ–ˆâ–ˆâ–ˆâ–„ â–ˆâ–ˆâ–ˆâ–„â–ˆâ–ˆâ–ˆâ–„
â–„â–ˆâ–ˆâ–ˆâ–ˆâ–ˆâ–„ â–„â–„â–„â–ˆâ–ˆâ–ˆâ–ˆâ–ˆâ–„â–„â–„ â–„â–„â–„â–ˆâ–ˆâ–ˆâ–ˆâ–ˆâ–„â–„â–„
â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–„â–„â–„â–„â–„â–„â–„â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–€ â–€â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–€
â–€â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–„â–„â–„â–„â–„â–„â–„ â–ˆâ–€ â–ˆâ–ˆâ–ˆâ–„â–„â–„â–„â–„â–„â–„â–ˆâ–ˆâ–ˆ
â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–„â–ˆâ–ˆâ–ˆâ–ˆâ–„ â–ˆâ–ˆâ–ˆâ–€â–€â–€â–€â–€â–€â–€ â–ˆâ–ˆâ–ˆâ–ˆâ–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ
â–ˆâ–ˆâ–ˆ â–€â–€â–€â–€â–€â–€â–€â–€â–€â–€â–€ â–„â–„â–„â–ˆâ–ˆâ–ˆâ–„â–„â–„ â–€â–€â–€â–€â–€â–€â–€â–€â–€â–€â–€
â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–„â–„â–„â–„â–„â–„â–„â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆ â–ˆâ–ˆâ–ˆâ–„â–„â–„â–„â–„â–„â–„â–ˆâ–ˆâ–ˆ
â–€â–€â–€ â–€â–€â–€ â–€â–€â–€â–€â–€â–€â–€â–€â–€ â–€â–€â–€ â–€â–€â–€ â–€â–€â–€ â–€â–€â–€ â–€â–€â–€ â–€â–€â–€â–€â–€â–€â–€â–€â–€

[*] Nexpose integration has been activated

[*] Successfully loaded plugin: nexpose msf > help

Nexpose Commands

==========

Command	Description

------- -----------

nexpose_activity Display any active scan jobs on the Nexpose instance

nexpose_command Execute a console command on the Nexpose instance

nexpose_connect Connect to a running Nexpose instance (user:pass@host[:port])

nexpose_disconnect Disconnect from an active Nexpose instance

nexpose_discover Launch a scan but only perform host and minimal service discovery

nexpose_dos Launch a scan that includes checks that can crash services and devices (caution)

nexpose_exhaustive Launch a scan covering all TCP ports and all authorized safe checks

nexpose_report_templates List all available report templates

nexpose_save Save credentials to a Nexpose instance

nexpose_scan Launch a Nexpose scan against a specific IP range and import the results

nexpose_site_devices List all discovered devices within a site

nexpose_site_import Import data from the specified site ID

nexpose_sites List all defined sites

nexpose_sysinfo Display detailed system information about the Nexpose instance

...snip... Before running a scan against a target, we first need to connect to our server running NeXpose by using the nexpose_connect command along with the credentials for the NeXpose instance. Note that you will have to append â€˜okâ€™ to the end of the connect string to acknowledge that the SSL connections are not verified. msf > nexpose_connect -h

[*] Usage:

[*] nexpose_connect username:password@host[:port] >ssl-confirm>

[*] -OR-

[*] nexpose_connect username password host port >ssl-confirm>

msf > nexpose_connect loneferret:something@127.0.0.1:3780 ok

[*] Connecting to Nexpose instance at 127.0.0.1:3780 with username loneferret... Now that we are connected to our server, we can run a vulnerability scan right from within Metasploit. msf > nexpose_scan -h

Usage: nexpose_scan [options] >Target IP Ranges>

OPTIONS:

-E Exclude hosts in the specified range from the scan

-I Only scan systems with an address within the specified range

-P Leave the scan data on the server when it completes (this counts against the maximum licensed IPs)

-c Specify credentials to use against these targets (format is type:user:pass

-d Scan hosts based on the contents of the existing database

-h This help menu

-n The maximum number of IPs to scan at a time (default is 32)

-s The directory to store the raw XML files from the Nexpose instance (optional)

-t The scan template to use (default:pentest-audit options:full-audit,exhaustive-audit,discovery,aggressive-discovery,dos-audit)

-v Display diagnostic information about the scanning process Weâ€™ll provide our scanner with the credentials for the â€˜sshâ€™ services, and use the â€˜full-auditâ€™Â scan template. Our scan results should be very similar to one we previously imported. msf > msf > nexpose_scan -c ssh:msfadmin:msfadmin -t full-audit 172.16.194.172

[*] Scanning 1 addresses with template aggressive-discovery in sets of 32

[*] Completed the scan of 1 addresses

msf > msf > hosts

Hosts

=====

address mac name os_name os_flavor os_sp purpose info comments

------- --- ---- ------- --------- ----- ------- ---- --------

172.16.194.172 METASPLOITABLE Ubuntu Linux device Again, we run services and vulns and we can see that the results are of the same quality as those we imported via the XML file. msf > services

Services

========

host port proto name state info

---- ---- ----- ---- ----- ----

172.16.194.172 21 tcp ftp open vsFTPd 2.3.4

172.16.194.172 22 tcp ssh open OpenSSH 4.7p1

172.16.194.172 23 tcp telnet open

172.16.194.172 25 tcp smtp open Postfix

172.16.194.172 53 tcp dns-tcp open BIND 9.4.2

172.16.194.172 53 udp dns open BIND 9.4.2

172.16.194.172 80 tcp http open Apache 2.2.8

172.16.194.172 111 udp portmapper open

172.16.194.172 111 tcp portmapper open

172.16.194.172 137 udp cifs name service open

172.16.194.172 139 tcp cifs open Samba 3.0.20-Debian

172.16.194.172 445   tcp   cifs   open   Samba 3.0.20-Debian

172.16.194.172 512   tcp   remote execution   open

172.16.194.172 513   tcp   remote login   open

172.16.194.172 514   tcp   remote shell   open

172.16.194.172 1524   tcp   ingreslock (ingres) open

172.16.194.172 2049   tcp   nfs   open

172.16.194.172 2049   udp   nfs   open

172.16.194.172 3306   tcp   mysql   open   MySQL 5.0.51a

172.16.194.172 5432   tcp   postgres   open

172.16.194.172 5900   tcp   vnc   open

172.16.194.172 6000   tcp   xwindows   open

172.16.194.172 8180   tcp   http   open   Tomcat

172.16.194.172 41407 udp   status   open

172.16.194.172 44841 tcp   mountd   open

172.16.194.172 47207 tcp   nfs lockd   open

172.16.194.172 48972 udp   nfs lockd   open

172.16.194.172 51255 tcp   status   open

172.16.194.172 58769 udp   mountd   open msf > vulns

[*] Time: 2012-06-20 16:34:21 UTC Vuln: host=172.16.194.172 name=NEXPOSE-cifs-nt-0001

refs=CVE-1999-0519,URL-http://www.hsc.fr/ressources/presentations/null_sessions/

[*] Time: 2012-06-20 16:34:21 UTC Vuln: host=172.16.194.172

name=NEXPOSE-generic-ip-source-routing-enabled

refs=BID-646,CVE-1999-0510,CVE-1999-0909,MSB-MS99-038,URL-http://packetstormsecurity.nl/a

dvisories/nai/nai.99-09-20.windows_ip_source_routing

[*] Time: 2012-06-20 16:34:21 UTC Vuln: host=172.16.194.172

name=NEXPOSE-unix-hosts-equiv-allows-access refs=

[*] Time: 2012-06-20 16:34:21 UTC Vuln: host=172.16.194.172

name=NEXPOSE-cifs-share-world-writeable refs=CVE-1999-0520

...snip...

[*] Time: 2012-06-20 16:34:22 UTC Vuln: host=172.16.194.172

name=NEXPOSE-vnc-password-password refs=

[*] Time: 2012-06-20 16:34:22 UTC Vuln: host=172.16.194.172

name=NEXPOSE-apache-tomcat-default-password

refs=BID-38084,CVE-2009-3843,CVE-2010-0557

[*] Time: 2012-06-20 16:34:22 UTC Vuln: host=172.16.194.172

name=NEXPOSE-apache-tomcat-example-leaks refs=

[*] Time: 2012-06-20 16:34:22 UTC Vuln: host=172.16.194.172

name=NEXPOSE-apache-tomcat-default-install-page refs=

[*] Time: 2012-06-20 16:34:22 UTC Vuln: host=172.16.194.172 name=NEXPOSE-nfs-mountd-0002 refs= Expanding on our NeXpose Scanning Methods a11y.text Expanding on our NeXpose Scanning Methods Other types of scans can be conducted against a target, or targets, by using the nexpose_discover , nexpose_dos and nexpose_exhaustive commands. The first performs a minimal service discovery scan, as the other will add denial of service checking. Caution should be used when running the nexpose_dos , as it may very well crash your target. The nexpose_exhaustive scan will cover all TCP ports and all authorized safe checks. msf > nexpose_discover -h

Usage: nexpose_scan [options] >Target IP Ranges>

OPTIONS:

-E Exclude hosts in the specified range from the scan

-I Only scan systems with an address within the specified range

-P Leave the scan data on the server when it completes (this counts against the maximum licensed IPs)

-c Specify credentials to use against these targets (format is type:user:pass

-d Scan hosts based on the contents of the existing database

-h This help menu

-n The maximum number of IPs to scan at a time (default is 32)

-s The directory to store the raw XML files from the Nexpose instance (optional)

-t The scan template to use (default:pentest-audit options:full-audit,exhaustive-audit,discovery,aggressive-discovery,dos-audit)

-v Display diagnostic information about the scanning process msf > nexpose_dos -h

Usage: nexpose_scan [options] >Target IP Ranges>

OPTIONS:

-E Exclude hosts in the specified range from the scan

-I Only scan systems with an address within the specified range

-P Leave the scan data on the server when it completes (this counts against the maximum licensed IPs)

-c Specify credentials to use against these targets (format is type:user:pass

-d Scan hosts based on the contents of the existing database

-h This help menu

-n The maximum number of IPs to scan at a time (default is 32)

-s The directory to store the raw XML files from the Nexpose instance (optional)

-t The scan template to use (default:pentest-audit options:full-audit,exhaustive-audit,discovery,aggressive-discovery,dos-audit)

-v Display diagnostic information about the scanning process msf > nexpose_exhaustive -h Usage: nexpose_scan [options] >Target IP Ranges>

OPTIONS:

-E Exclude hosts in the specified range from the scan

-I Only scan systems with an address within the specified range

-P Leave the scan data on the server when it completes (this counts against the maximum licensed IPs)

-c Specify credentials to use against these targets (format is type:user:pass

-d Scan hosts based on the contents of the existing database

-h This help menu

-n The maximum number of IPs to scan at a time (default is 32)

-s The directory to store the raw XML files from the Nexpose instance (optional)

-t The scan template to use (default:pentest-audit options:full-audit,exhaustive-audit,discovery,aggressive-discovery,dos-audit)

-v Display diagnostic information about the scanning process NeXpose and Metasploit integration has improved greatly over time. Running scans directly from the console using all of NeXposeâ€™s features is a great addition to the Framework. Also we now have the possibility to correlate our findings against Metasploitâ€™s different modules. This feature is offered using the Community Edition which is discussed in a later module. Nexpose Plugin loaded via msfconsole | Metasploit Unleashed Next Working with Nessus Prev Working with NeXpose