Working with NeXpose a11y.text Working with NeXpose Using NeXpose Results Within the Metasploit Framework a11y.text Using NeXpose Results Within the Metasploit Framework With the acquisition of Metasploit by Rapid7 back in 2009, there is now excellent compatibility between Metasploit and the NeXpose Vulnerability Scanner. Rapid7 has a community edition of their scanner that is available at http://www.rapid7.com/vulnerability-scanner.jsp . After we have installed and updated NeXpose, we run a full credentialed scan against our vulnerable Linux machine. NeXpose Security Console | Metasploit unleashed We create a new report in NeXpose and save the scan results in NeXpose Simple XML format that we can later import into Metasploit. Next, we fire up msfconsole, create a new workspace, and use the db_import command to auto-detect and import our scan results file. msf > db_import /root/Nexpose/report.xml

[*] Importing 'NeXpose Simple XML' data

[*] Importing host 172.16.194.172

[*] Successfully imported /root/Nexpose/report.xml 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 tcp portmapper open

172.16.194.172 111 udp 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 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 Apache 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 We now have NeXposeâ€™s report at ourÂ disposal directly from the msfconsole . As discussed in a previousÂ modules, using the database backend commands, we can search this information using a few simple key strokes. One that was not covered however was the vulns command. We can issue this command and see what vulnerabilities were found by our NeXpose scan. With no options given vulns will simply display

every vulnerability found suchÂ as service names, associated ports, CVEs (if any) etc. msf > vulns

[*] Time: 2012-06-20 02:09:50 UTC Vuln: host=172.16.194.172 name=NEXPOSE-vnc-password-password refs=NEXPOSE-vnc-password-password

[*] Time: 2012-06-20 02:09:50 UTC Vuln: host=172.16.194.172 name=NEXPOSE-backdoor-vnc-0001 refs=NEXPOSE-backdoor-vnc-0001

[*] Time: 2012-06-20 02:09:49 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/,NEXPOSE-cifs-nt-0001

...snip...

[*] Time: 2012-06-20 02:09:52 UTC Vuln: host=172.16.194.172 name=NEXPOSE-openssl-debian-weak-keys refs=CVE-2008-0166,BID-29179,SECUNIA-30136,SECUNIA-30220,SECUNIA-30221,SECUNIA-30231,SECUNIA-30239,SECUNIA-30249,URL-http://metasploit.com/users/hdm/tools/debian-openssl/,URL-http://wiki.debian.org/SSLkeys,URL-http://www.debian.org/security/2008/dsa-1571,URL-http://www.debian.org/security/2008/dsa-1576,URL-http://www.debian.org/security/key-rollover/,URL-http://www.ubuntu.com/usn/usn-612-1,URL-http://www.ubuntu.com/usn/usn-612-2,URL-http://www.ubuntu.com/usn/usn-612-3,URL-http://www.ubuntu.com/usn/usn-612-4,URL-http://www.ubuntu.com/usn/usn-612-5,URL-http://www.ubuntu.com/usn/usn-612-6,URL-http://www.ubuntu.com/usn/usn-612-7,URL-http://www.ubuntu.com/usn/usn-612-8,NEXPOSE-openssl-debian-weak-keys

[*] Time: 2012-06-20 02:09:52 UTC Vuln: host=172.16.194.172 name=NEXPOSE-ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack refs=CVE-2008-3259,BID-30339,SECUNIA-31179,NEXPOSE-ssh-openssh-x11uselocalhost-x11-forwarding-session-hijack Much like the hosts and services commands, we have a few options available to produce a more specific output when searching vulnerabilities stored in our imported

report. Letâ€™s take a look at those. msf > vulns -h

Print all vulnerabilities in the database

Usage: vulns [addr range]

-h,--help Show this help information

-p,--port >portspec> List vulns matching this port spec

-s >svc names> List vulns matching these service names

-S,--search Search string to filter by

-i,--info Display Vuln Info

Examples:

vulns -p 1-65536 # only vulns with associated services

vulns -p 1-65536 -s http # identified as http on any port Lets target a specific service we know to be running on Metasploitable and see what information was collected by our vulnerability scan. Weâ€™ll display vulnerabilities found for the â€˜mysqlâ€™ service. Using the following options: -p to specify the port number, -s service name and finally -i the vulnerability information. msf > vulns -p 3306 -s mysql -i

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-dispatch_command-multiple-format-string refs=CVE-2009-2446,BID-35609,OSVDB-55734,SECUNIA-35767,SECUNIA-38517,NEXPOSE-mysql-dispatch_command-multiple-format-string info=mysql-dispatch_command-multiple-format-string

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-32707-send-error-bof refs=URL-http://bugs.mysql.com/bug.php?id=32707,NEXPOSE-mysql-bug-32707-send-error-bof info=mysql-bug-32707-send-error-bof

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-37428-user-defind-function-remote-codex refs=URL-http://bugs.mysql.com/bug.php?id=37428,NEXPOSE-mysql-bug-37428-user-defind-function-remote-codex info=mysql-bug-37428-user-defind-function-remote-codex

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-default-account-root-nopassword refs=CVE-2002-1809,BID-5503,NEXPOSE-mysql-default-account-root-nopassword info=mysql-default-account-root-nopassword

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-yassl-certdecodergetname-multiple-bofs refs=CVE-2009-4484,BID-37640,BID-37943,BID-37974,OSVDB-61956,SECUNIA-37493,SECUNIA-38344,SECUNIA-38364,SECUNIA-38517,SECUNIA-38573,URL-http://bugs.mysql.com/bug.php?id=50227,URL-http://dev.mysql.com/doc/refman/5.0/en/news-5-0-90.html,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-43.html,NEXPOSE-mysql-yassl-certdecodergetname-multiple-bofs info=mysql-yassl-certdecodergetname-multiple-bofs

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-yassl-multiple-bof refs=CVE-2008-0226,CVE-2008-0227,BID-27140,BID-31681,SECUNIA-28324,SECUNIA-28419,SECUNIA-28597,SECUNIA-29443,SECUNIA-32222,URL-http://bugs.mysql.com/bug.php?id=33814,NEXPOSE-mysql-yassl-multiple-bof info=mysql-yassl-multiple-bof

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-directory-traversal-and-arbitrary-table-access refs=CVE-2010-1848,URL-http://bugs.mysql.com/bug.php?id=53371,URL-http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html,NEXPOSE-mysql-directory-traversal-and-arbitrary-table-access info=mysql-directory-traversal-and-arbitrary-table-access

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-vio_verify_callback-zero-depth-x-509-certificate refs=CVE-2009-4028,URL-http://bugs.mysql.com/bug.php?id=47320,URL-http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html,NEXPOSE-mysql-vio_verify_callback-zero-depth-x-509-certificate info=mysql-vio_verify_callback-zero-depth-x-509-certificate
[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-29801-remote-federated-engine-crash refs=URL-http://bugs.mysql.com/bug.php?id=29801,NEXPOSE-mysql-bug-29801-remote-federated-engine-crash info=mysql-bug-29801-remote-federated-engine-crash
[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-38296-nested-boolean-query-exhaustion-dos refs=URL-http://bugs.mysql.com/bug.php?id=38296,NEXPOSE-mysql-bug-38296-nested-boolean-query-exhaustion-dos info=mysql-bug-38296-nested-boolean-query-exhaustion-dos
[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-com_field_list-command-bof refs=CVE-2010-1850,URL-http://bugs.mysql.com/bug.php?id=53237,URL-http://dev.mysql.com/doc/refman/5.0/en/news-5-0-91.html,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html,NEXPOSE-mysql-com_field_list-command-bof info=mysql-com_field_list-command-bof
[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-datadir-isam-table-privilege-escalation refs=CVE-2008-2079,BID-29106,BID-31681,SECUNIA-30134,SECUNIA-31066,SECUNIA-31226,SECUNIA-31687,SECUNIA-32222,SECUNIA-36701,URL-http://bugs.mysql.com/32091,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-23.html,URL-http://dev.mysql.com/doc/refman/6.0/en/news-6-0-4.html,NEXPOSE-mysql-datadir-isam-table-privilege-escalation info=mysql-datadir-isam-table-privilege-escalation

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-my_net_skip_rest-packet-length-dos refs=CVE-2010-1849,URL-http://bugs.mysql.com/bug.php?id=50974,URL-http://bugs.mysql.com/bug.php?id=53371,URL-http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html,NEXPOSE-mysql-my_net_skip_rest-packet-length-dos info=mysql-my_net_skip_rest-packet-length-dos

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-myisam-table-privilege-check-bypass refs=CVE-2008-4097,CVE-2008-4098,SECUNIA-32759,SECUNIA-38517,URL-http://bugs.mysql.com/bug.php?id=32167,URL-http://lists.mysql.com/commits/50036,URL-http://lists.mysql.com/commits/50773,NEXPOSE-mysql-myisam-table-privilege-check-bypass info=mysql-myisam-table-privilege-check-bypass

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-29908-alter-view-priv-esc refs=URL-http://bugs.mysql.com/bug.php?id=29908,NEXPOSE-mysql-bug-29908-alter-view-priv-esc info=mysql-bug-29908-alter-view-priv-esc

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-bug-44798-stored-procedures-server-crash refs=URL-http://bugs.mysql.com/bug.php?id=44798,NEXPOSE-mysql-bug-44798-stored-procedures-server-crash info=mysql-bug-44798-stored-procedures-server-crash

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-empty-bit-string-dos refs=CVE-2008-3963,SECUNIA-31769,SECUNIA-32759,SECUNIA-34907,URL-http://bugs.mysql.com/bug.php?id=35658,NEXPOSE-mysql-empty-bit-string-dos info=mysql-empty-bit-string-dos

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172 name=NEXPOSE-mysql-innodb-dos refs=CVE-2007-5925,BID-26353,SECUNIA-27568,SECUNIA-27649,SECUNIA-27823,SECUNIA-28025,SECUNIA-28040,SECUNIA-28099,SECUNIA-28108,SECUNIA-28128,SECUNIA-28838,URL-ht

tp://bugs.mysql.com/bug.php?id=32125,NEXPOSE-mysql-innodb-dos info=mysql-innodb-dos

[*] Time: 2012-06-20 02:09:51 UTC Vuln: host=172.16.194.172

name=NEXPOSE-mysql-html-output-script-insertion

refs=CVE-2008-4456,BID-31486,SECUNIA-32072,SECUNIA-34907,SECUNIA-38517,URL-http://bu

gs.mysql.com/bug.php?id=27884,URL-http://www.henlich.de/it-security/mysql-command-line-client-

html-injection-vulnerability,NEXPOSE-mysql-html-output-script-insertion

info=mysql-html-output-script-insertion

[*] Time: 2012-06-20 02:09:50 UTC Vuln: host=172.16.194.172

name=NEXPOSE-database-open-access

refs=URL-https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.

pdf,NEXPOSE-database-open-access info=database-open-access Next NeXpose via MSFconsole

Prev WMAP Web Scanner