Scanner Discovery Auxiliary Modules a11y.text Scanner Discovery Auxiliary Modules arp_sweep a11y.text arp_sweep When your target systems are located on the same network as your attacking machine, you can enumerate systems by performing an ARP scan. Naturally, Metasploit has a module that can help you out. msf > use auxiliary/scanner/discovery/arp_sweep

msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
RHOSTS		yes	The target address range or CIDR identifier
SHOST		no	Source IP Address
SMAC		no	Source MAC Address
THREADS	1	yes	The number of concurrent threads
TIMEOUT	5	yes	The number of seconds to wait for new data Due to the manner in which ARP scanning is performed, you need to pass your MAC address and source IP address to the scanner in order for it to function properly. msf auxiliary(arp_sweep) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(arp_sweep) > set SHOST 192.168.1.101

SHOST => 192.168.1.101

msf auxiliary(arp_sweep) > set SMAC d6:46:a7:38:15:65

SMAC => d6:46:a7:38:15:65

msf auxiliary(arp_sweep) > set THREADS 55

THREADS => 55

msf auxiliary(arp_sweep) > run

[*] 192.168.1.201 appears to be up.

[*] 192.168.1.203 appears to be up.

[*] 192.168.1.205 appears to be up.

[*] 192.168.1.206 appears to be up.

[*] 192.168.1.250 appears to be up.

[*] Scanned 55 of 55 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(arp_sweep) > As you will see when running this module, ARP scanning is very fast. ipv6_neighbor a11y.text ipv6_neighbor The ipv6_neighbor auxiliary module probes the local network for IPv6 hosts that respond to Neighbor Solicitations with a link-local address. This module, like the arp_sweep one, will generally only work within the attacking machineâ€™s broadcast domain. msf > use auxiliary/scanner/discovery/ipv6_neighbor

msf auxiliary(ipv6_neighbor) > show options

Module options:

Name	Current Setting	Required	Description
INTERFACE		no	The name of the interface
PCAPFILE		no	The name of the PCAP capture file to process
RHOSTS		yes	The target address range or CIDR identifier
SHOST		yes	Source IP Address
SMAC		yes	Source MAC Address
THREADS	1	yes	The number of concurrent threads

TIMEOUT 500 yes The number of seconds to wait for new data In addition to setting our RHOSTS value, we also need to set our source MAC address(SMAC) and source host(SHOST) IP address. We then set our RHOSTS and THREADS values and let the scanner run. msf auxiliary(ipv6_neighbor) > set RHOSTS 192.168.1.2-254

RHOSTS => 192.168.1.200-254

msf auxiliary(ipv6_neighbor) > set SHOST 192.168.1.101

SHOST => 192.168.1.101

msf auxiliary(ipv6_neighbor) > set SMAC d6:46:a7:38:15:65

SMAC => d6:46:a7:38:15:65

msf auxiliary(ipv6_neighbor) > set THREADS 55

THREADS => 55

msf auxiliary(ipv6_neighbor) > run

[*] IPv4 Hosts Discovery

[*] 192.168.1.10 is alive.

[*] 192.168.1.11 is alive.

[*] 192.168.1.2 is alive.

[*] 192.168.1.69 is alive.

[*] 192.168.1.109 is alive.

[*] 192.168.1.150 is alive.

[*] 192.168.1.61 is alive.

[*] 192.168.1.201 is alive.

[*] 192.168.1.203 is alive.

[*] 192.168.1.205 is alive.

[*] 192.168.1.206 is alive.

[*] 192.168.1.99 is alive.

[*] 192.168.1.97 is alive.

[*] 192.168.1.250 is alive.

[*] IPv6 Neighbor Discovery

[*] 192.168.1.69 maps to IPv6 link local address fe80::5a55:caff:fe14:1e61

[*] 192.168.1.99 maps to IPv6 link local address fe80::5ab0:35ff:fe6a:4ecc

[*] 192.168.1.97 maps to IPv6 link local address fe80::7ec5:37ff:fef9:a96a

[*] Scanned 253 of 253 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(ipv6_neighbor) > Looking at the module output, you can see that this scanner serves the dual-purpose of showing what hosts are online similar to arp_sweep and then performs the IPv6 Neighbor Discovery. udp_probe a11y.text udp_probe The udp_probe module scans a given range of hosts for common UDP services. Note: This module is deprecated and may disappear at any time. msf > use auxiliary/scanner/discovery/udp_probe

[!] **

[!] * The module scanner/discovery/udp_probe is deprecated! *

[!] * It will be removed on or about 2016-11-23 *

[!] * Use auxiliary/scanner/discovery/udp_sweep instead *

[!] **

msf auxiliary(udp_probe) > show options

Module options (auxiliary/scanner/discovery/udp_probe):

Name	Current Setting	Required	Description
CHOST		no	The local client address

RHOSTS yes The target address range or CIDR identifier

THREADS 1 yes The number of concurrent threads There are very few required settings for this module so we just configure the RHOSTS and THREADS values and let it run. msf auxiliary(udp_probe) > set RHOSTS 192.168.1.2-254

RHOSTS => 192.168.1.2-254

msf auxiliary(udp_probe) > set THREADS 253

THREADS => 253

msf auxiliary(udp_probe) > run

[*] Discovered SNMP on 192.168.1.2:161 (GSM7224 L2 Managed Gigabit Switch)

[*] Discovered SNMP on 192.168.1.2:161 (GSM7224 L2 Managed Gigabit Switch)

[*] Discovered NetBIOS on 192.168.1.109:137 (SAMSUNG::U :SAMSUNG::U :00:15:99:3f:40:bd)

[*] Discovered NetBIOS on 192.168.1.150:137 (XEN-WIN7-PROD::U :WORKGROUP::G :XEN-WIN7-PROD::U :WORKGROUP::G :aa:e3:27:6e:3b:a5)

[*] Discovered SNMP on 192.168.1.109:161 (Samsung CLX-3160 Series; OS V1.01.01.16 02-25-2008;Engine 6.01.00;NIC V4.03.08(CLX-3160) 02-25-2008;S/N 8Y61B1GP400065Y.)

[*] Discovered NetBIOS on 192.168.1.206:137 (XEN-XP-PATCHED::U :XEN-XP-PATCHED::U :HOTZONE::G :HOTZONE::G :12:fa:1a:75:b8:a5)

[*] Discovered NetBIOS on 192.168.1.203:137 (XEN-XP-SPLOIT::U :WORKGROUP::G :XEN-XP-SPLOIT::U :WORKGROUP::G :3e:ff:3c:4c:89:67)

[*] Discovered NetBIOS on 192.168.1.201:137 (XEN-XP-SP2-BARE::U :HOTZONE::G :XEN-XP-SP2-BARE::U :HOTZONE::G :HOTZONE::U :__MSBROWSE__::G :c6:ce:4e:d9:c9:6e)

[*] Discovered SNMP on 192.168.1.109:161 (Samsung CLX-3160 Series; OS V1.01.01.16 02-25-2008;Engine 6.01.00;NIC V4.03.08(CLX-3160) 02-25-2008;S/N 8Y61B1GP400065Y.)

[*] Discovered NTP on 192.168.1.69:123 (NTP v4)

[*] Discovered NetBIOS on 192.168.1.250:137 (FREENAS::U :FREENAS::U :FREENAS::U

:__MSBROWSE__::G :WORKGROUP::U :WORKGROUP::G :WORKGROUP::G

:00:00:00:00:00:00)

[*] Discovered NTP on 192.168.1.203:123 (Microsoft NTP)

[*] Discovered MSSQL on 192.168.1.206:1434 (ServerName=XEN-XP-PATCHED

InstanceName=SQLEXPRESS IsClustered=No Version=9.00.4035.00 tcp=1050

np=\\XEN-XP-PATCHED\pipe\MSSQL$SQLEXPRESS\sql\query)

[*] Discovered NTP on 192.168.1.206:123 (Microsoft NTP)

[*] Discovered NTP on 192.168.1.201:123 (Microsoft NTP)

[*] Scanned 029 of 253 hosts (011% complete)

[*] Scanned 052 of 253 hosts (020% complete)

[*] Scanned 084 of 253 hosts (033% complete)

[*] Scanned 114 of 253 hosts (045% complete)

[*] Scanned 140 of 253 hosts (055% complete)

[*] Scanned 160 of 253 hosts (063% complete)

[*] Scanned 184 of 253 hosts (072% complete)

[*] Scanned 243 of 253 hosts (096% complete)

[*] Scanned 250 of 253 hosts (098% complete)

[*] Scanned 253 of 253 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(udp_probe) > As you can see in the above output, our quick little scan discovered many services running on a wide variety of platforms. udp_sweep a11y.text udp_sweep The udp_sweep module scans across a given range of hosts to detect commonly available UDP services. msf > use auxiliary/scanner/discovery/udp_sweep

msf auxiliary(udp_sweep) > show options

Module options (auxiliary/scanner/discovery/udp_sweep):

Name Current Setting Required Description

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

BATCHSIZE 256 yes The number of hosts to probe in each set

RHOSTS yes The target address range or CIDR identifier

THREADS 10 yes The number of concurrent threads To configure this module, we just need to set the RHOSTS and THREADS values and run it. msf auxiliary(udp_sweep) > set RHOSTS 192.168.1.2-254

RHOSTS => 192.168.1.2-254

msf auxiliary(udp_sweep) > set THREADS 253

THREADS => 253

msf auxiliary(udp_sweep) > run

[*] Sending 10 probes to 192.168.1.2->192.168.1.254 (253 hosts)

[*] Discovered NetBIOS on 192.168.1.109:137 (SAMSUNG::U :SAMSUNG::U :00:15:99:3f:40:bd)

[*] Discovered NetBIOS on 192.168.1.150:137 (XEN-WIN7-PROD::U :WORKGROUP::G :XEN-WIN7-PROD::U :WORKGROUP::G :aa:e3:27:6e:3b:a5)

[*] Discovered NetBIOS on 192.168.1.203:137 (XEN-XP-SPLOIT::U :WORKGROUP::G :XEN-XP-SPLOIT::U :WORKGROUP::G :3e:ff:3c:4c:89:67)

[*] Discovered NetBIOS on 192.168.1.201:137 (XEN-XP-SP2-BARE::U :HOTZONE::G :XEN-XP-SP2-BARE::U :HOTZONE::G :HOTZONE::U :__MSBROWSE__::G :c6:ce:4e:d9:c9:6e)

[*] Discovered NetBIOS on 192.168.1.206:137 (XEN-XP-PATCHED::U :XEN-XP-PATCHED::U :HOTZONE::G :HOTZONE::G :12:fa:1a:75:b8:a5)

[*] Discovered NetBIOS on 192.168.1.250:137 (FREENAS::U :FREENAS::U :FREENAS::U :__MSBROWSE__::G :WORKGROUP::U :WORKGROUP::G :WORKGROUP::G :00:00:00:00:00:00)

[*] Discovered SNMP on 192.168.1.2:161 (GSM7224 L2 Managed Gigabit Switch)

[*] Discovered SNMP on 192.168.1.109:161 (Samsung CLX-3160 Series; OS V1.01.01.16 02-25-2008;Engine 6.01.00;NIC V4.03.08(CLX-3160) 02-25-2008;S/N 8Y61B1GP400065Y.)

[*] Discovered NTP on 192.168.1.69:123 (NTP v4)

[*] Discovered NTP on 192.168.1.99:123 (NTP v4)

[*] Discovered NTP on 192.168.1.201:123 (Microsoft NTP)

[*] Discovered NTP on 192.168.1.203:123 (Microsoft NTP)

[*] Discovered NTP on 192.168.1.206:123 (Microsoft NTP)

[*] Discovered MSSQL on 192.168.1.206:1434 (ServerName=XEN-XP-PATCHED InstanceName=SQLEXPRESS IsClustered=No Version=9.00.4035.00 tcp=1050 np=\\XEN-XP-PATCHED\pipe\MSSQL$SQLEXPRESS\sql\query)

[*] Discovered SNMP on 192.168.1.2:161 (GSM7224 L2 Managed Gigabit Switch)

[*] Discovered SNMP on 192.168.1.109:161 (Samsung CLX-3160 Series; OS V1.01.01.16 02-25-2008;Engine 6.01.00;NIC V4.03.08(CLX-3160) 02-25-2008;S/N 8Y61B1GP400065Y.)

[*] Scanned 253 of 253 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(udp_sweep) > With minimal effort, we have once again identified a wide range of services running on many different platforms within our network. Next Scanner FTP Auxiliary Modules Prev Scanner DCERPC Auxiliary Modules