Scanner DCERPC Auxiliary Modules a11y.text Scanner DCERPC Auxiliary Modules endpoint_mapper a11y.text endpoint_mapper The endpoint_mapper module queries the EndPoint Mapper service of a remote system to determine what services are available. In the information gathering stage, this can provide some very valuable information. msf > use auxiliary/scanner/dcerpc/endpoint_mapper

msf auxiliary(endpoint_mapper) > show options

Module options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	135	yes	The target port
THREADS	1	yes	The number of concurrent threads In order to run the module, all we need to do is pass it a range of IP addresses, set the THREADS count, and let it go to work. msf auxiliary(endpoint_mapper) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(endpoint_mapper) > set THREADS 55

threads => 55

msf auxiliary(endpoint_mapper) > run

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

...snip...

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (dhcpcsvc) [DHCP Client LRPC Endpoint]

[*] 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (W32TIME_ALT) [WinHttp Auto-Proxy Service]

[*] 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 PIPE (\PIPE\W32TIME_ALT) \\XEN-2K3-BARE [WinHttp Auto-Proxy Service]

[*] 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC00000408.00000001)

[*] 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC00000408.00000001)

[*] 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC00000408.00000001)

[*] 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC00000408.00000001)

[*] Could not connect to the endpoint mapper service

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\PIPE\lsass) \\XEN-2K3-BARE

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (audit)

[*] Connecting to the endpoint mapper service...

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (securityevent)

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (protected_storage)

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\PIPE\protected_storage) \\XEN-2K3-BARE

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (dsrole)

[*] 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP (1025) 192.168.1.204

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 PIPE (\PIPE\lsass) \\XEN-2K3-BARE [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (audit) [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (securityevent) [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (protected_storage) [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 PIPE (\PIPE\protected_storage)

\\XEN-2K3-BARE [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (dsrole) [IPSec Policy agent endpoint]

[*] 12345678-1234-abcd-ef00-0123456789ab v1.0 TCP (1025) 192.168.1.204 [IPSec Policy agent endpoint]

[*] 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (wzcsvc)

[*] 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (OLE3B0AF7639CA847BCA879F781582D)

[*] 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 PIPE (\PIPE\atsvc) \\XEN-2K3-BARE

[*] 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (wzcsvc)

[*] 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (OLE3B0AF7639CA847BCA879F781582D)

[*] 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 PIPE (\PIPE\atsvc) \\XEN-2K3-BARE

[*] 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (wzcsvc)

[*] 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (OLE3B0AF7639CA847BCA879F781582D)

[*] 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 PIPE (\PIPE\atsvc) \\XEN-2K3-BARE

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (DNSResolver) [DHCP Client LRPC Endpoint]

[*] d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 TCP (49152) 192.168.1.202

[*] 4b112204-0e19-11d3-b42b-0000f81feb9f v1.0 LRPC (LRPC-71ea8d8164d4fa6391)

[*] 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMsgKRpc05FBE22)

[*] 12e65dd8-887f-41ef-91bf-8d816c42c2e7 v1.0 LRPC (WMsgKRpc05FBE22) [Secure Desktop LRPC interface]

[*] b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (OLE7A8F68570F354B65A0C8D44DCBE0)

[*] b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 PIPE (\pipe\trkwks) \\XEN-WIN7-BARE

[*] b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (trkwks)

[*] b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (RemoteDevicesLPC_API)

[*] b58aa02e-2884-4e97-8176-4ee06d794184 v1.0 LRPC (TSUMRPD_PRINT_DRV_LPC_API)

[*] 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC

(OLE7A8F68570F354B65A0C8D44DCBE0) [PcaSvc]

[*] 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 PIPE (\pipe\trkwks) \\XEN-WIN7-BARE [PcaSvc]

[*] 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC (trkwks) [PcaSvc]

[*] 0767a036-0d22-48aa-ba69-b619480f38cb v1.0 LRPC (RemoteDevicesLPC_API) [PcaSvc]

...snip...

[*] f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 LRPC (eventlog) [Event log TCPIP]

[*] f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 PIPE (\pipe\eventlog) \\XEN-WIN7-BARE [Event log TCPIP]

[*] f6beaff7-1e19-4fbb-9f8f-b89e2018337c v1.0 TCP (49153) 192.168.1.202 [Event log TCPIP]

[*] 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (eventlog) [NRP server endpoint]

[*] 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 PIPE (\pipe\eventlog) \\XEN-WIN7-BARE [NRP server endpoint]

[*] 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 TCP (49153) 192.168.1.202 [NRP server endpoint]

[*] 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (AudioClientRpc) [NRP server endpoint]

[*] 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (Audiosrv) [NRP server endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (eventlog) [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 PIPE (\pipe\eventlog) \\XEN-WIN7-BARE [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 TCP (49153) 192.168.1.202 [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (AudioClientRpc) [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (Audiosrv) [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 v1.0 LRPC (dhcpcsvc) [DHCP Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (eventlog) [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 PIPE (\pipe\eventlog) \\XEN-WIN7-BARE [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 TCP (49153) 192.168.1.202 [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (AudioClientRpc) [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (Audiosrv) [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhcpcsvc) [DHCPv6 Client LRPC Endpoint]

[*] 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhcpcsvc6) [DHCPv6 Client LRPC Endpoint]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (eventlog) [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 PIPE (\pipe\eventlog) \\XEN-WIN7-BARE [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 TCP (49153) 192.168.1.202 [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (AudioClientRpc) [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (Audiosrv) [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (dhcpcsvc) [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (dhcpcsvc6) [Security Center]

[*] 06bba54a-be05-49f9-b0a0-30f790261023 v1.0 LRPC (OLE7F5D2071B7D4441897C08153F2A2) [Security Center]

[*] 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMsgKRpc045EC1)

[*] c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (LRPC-af541be9090579589d) [Impl friendly name]

[*] 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMsgKRpc0441F0)

[*] 76f226c3-ec14-4325-8a99-6a46348418af v1.0 PIPE (\PIPE\InitShutdown) \\XEN-WIN7-BARE

[*] 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WindowsShutdown)

[*] d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WMsgKRpc0441F0)

[*] d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 PIPE (\PIPE\InitShutdown) \\XEN-WIN7-BARE

[*] d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WindowsShutdown)

[*] Could not connect to the endpoint mapper service

[*] Scanned 06 of 55 hosts (010% complete)

...snip...

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

[*] Auxiliary module execution completed

msf auxiliary(endpoint_mapper) > hidden a11y.text hidden The dcerpc/hidden scanner connects to a given range of IP addresses and try to locate any RPC services that are not listed in the Endpoint Mapper and determine if anonymous access to the service is allowed. msf > use auxiliary/scanner/dcerpc/hidden

msf auxiliary(hidden) > show options

Module options:

Name	Current Setting	Required	Description

RHOSTS yes The target address range or CIDR identifier

THREADS 1 yes The number of concurrent threads As you can see, there are not many options to configure so we will just point it at some targets and let it run. msf auxiliary(hidden) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(hidden) > set THREADS 55

THREADS => 55

msf auxiliary(hidden) > run

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

...snip...

[*] Connecting to the endpoint mapper service...

[*] Connecting to the endpoint mapper service...

[*] Could not obtain the endpoint list: DCERPC FAULT => nca_s_fault_access_denied

[*] Could not contact the endpoint mapper on 192.168.1.203

[*] Could not obtain the endpoint list: DCERPC FAULT => nca_s_fault_access_denied

[*] Could not contact the endpoint mapper on 192.168.1.201

[*] Could not connect to the endpoint mapper service

[*] Could not contact the endpoint mapper on 192.168.1.250

[*] Looking for services on 192.168.1.204:1025...

[*] HIDDEN: UUID 12345778-1234-abcd-ef00-0123456789ab v0.0

[*] Looking for services on 192.168.1.202:49152...

[*] CONN BIND CALL ERROR=DCERPC FAULT => nca_s_fault_ndr

[*]

[*] HIDDEN: UUID c681d488-d850-11d0-8c52-00c04fd90f7e v1.0

[*]   CONN BIND CALL ERROR=DCERPC FAULT => nca_s_fault_ndr

[*]

[*] HIDDEN: UUID 11220835-5b26-4d94-ae86-c3e475a809de v1.0

[*]   CONN BIND ERROR=DCERPC FAULT => nca_s_fault_access_denied

[*]

[*] HIDDEN: UUID 5cbe92cb-f4be-45c9-9fc9-33e73e557b20 v1.0

[*]   CONN BIND ERROR=DCERPC FAULT => nca_s_fault_access_denied

[*]

[*] HIDDEN: UUID 3919286a-b10c-11d0-9ba8-00c04fd92ef5 v0.0

[*]   CONN BIND CALL DATA=0000000057000000

[*]

[*] HIDDEN: UUID 1cbcad78-df0b-4934-b558-87839ea501c9 v0.0

[*]   CONN BIND ERROR=DCERPC FAULT => nca_s_fault_access_denied

[*]

[*] HIDDEN: UUID c9378ff1-16f7-11d0-a0b2-00aa0061426a v1.0

[*]   CONN BIND ERROR=DCERPC FAULT => nca_s_fault_access_denied

[*]

[*] Remote Management Interface Error: The connection timed out (192.168.1.202:49152).

...snip...

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

[*] Auxiliary module execution completed

msf auxiliary(hidden) > As you can see, despite the simple setup, we still gathered some additional information about one of our targets. management a11y.text management The dcerpc/management module scans a range of IP addresses and obtains information from the Remote Management interface of the DCERPC service. msf > use auxiliary/scanner/dcerpc/management

```
msf auxiliary(management) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    135              yes       The target port
   THREADS  1                yes       The number of concurrent threads There is minimal configuration
required for this module; we simply need to set our THREADS value and the range of hosts we want
scanned and run the module. msf auxiliary(management) > set RHOSTS 192.168.1.200-254
RHOSTS => 192.168.1.200-254
msf auxiliary(management) > set THREADS 55
THREADS => 55
msf auxiliary(management) > run

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_access_denied
[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_access_denied
[*] UUID e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_access_denied
[*] Remote Management Interface Error: The connection was refused by the remote host
(192.168.1.250:135).
[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*]   listening: 00000000
[*]   killed: 00000005
[*]   name: 000100000000000001000000000000d3060000
```

[*] UUID 0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.1

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 1d55b526-c137-46c5-ab79-638f2a68e869 v1.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID e60c73e6-88f9-11cf-9af1-0020af6e72f4 v2.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 99fcfec4-5260-101b-bbcb-00aa0021347a v0.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID b9e79e60-3d52-11ce-aaa1-00006901293f v0.2

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 412f241e-c12a-11ce-abff-0020af6e7a17 v0.2

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 00000136-0000-0000-c000-000000000046 v0.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID c6f3ee72-ce7e-11d1-b71e-00c04fc3111a v1.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 v0.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

[*] UUID 000001a0-0000-0000-c000-000000000046 v0.0

[*] Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr

[*] listening: 00000000

[*] killed: 00000005

[*] name: 000100000000000001000000000000d3060000

...snip...

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

[*] Auxiliary module execution completed

msf auxiliary(management) > tcp_dcerpc_auditor a11y.text tcp_dcerpc_auditor The dcerpc/tcp_dcerpc_auditor module scans a range of IP addresses to determine what DCERPC services are available over a TCP port. msf > use auxiliary/scanner/dcerpc/tcp_dcerpc_auditor

msf auxiliary(tcp_dcerpc_auditor) > show options

Module options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	135	yes	The target port
THREADS	1	yes	The number of concurrent threads To run this scanner, we just need to set our RHOSTS and THREADS values and let it run. msf auxiliary(tcp_dcerpc_auditor) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(tcp_dcerpc_auditor) > set THREADS 55

THREADS => 55

msf auxiliary(tcp_dcerpc_auditor) > run

The connection was refused by the remote host (192.168.1.250:135).

The host (192.168.1.210:135) was unreachable.

...snip...

The host (192.168.1.200:135) was unreachable.

[*] Scanned 38 of 55 hosts (069% complete)

...snip...

The host (192.168.1.246:135) was unreachable.

192.168.1.203 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135 ACCESS GRANTED 000000000000000000000000000000000000000000000005000000

192.168.1.201 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135 ACCESS GRANTED 000000000000000000000000000000000000000000000005000000

192.168.1.204 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135 ACCESS GRANTED 000000000000000000000000000000000000000000076070000

192.168.1.202 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a 0.0 OPEN VIA 135 ACCESS GRANTED 000000000000000000000000000000000000000000005000000

192.168.1.204 - UUID afa8bd80-7d8a-11c9-bef4-08002b102989 1.0 OPEN VIA 135 ACCESS GRANTED

000002000b0000000b00000004000200080002000c000200100002001400020018000200 1c000200

200002002400020028000200 2c0002000883afe11f5dc91191a408002b14a0fa0300000084650a0b0f

9ecf11a3cf00805f68cb1b0100010026b5551d37c1c546ab79638f2a68e86901000000e6730ce6f988c

f119af10020af6e72f402000000c4fefc9960521b10bbcb00aa0021347a00000000609ee7b9523dce11

aaa100006901293f000002001e242f412ac1ce11abff0020af6e7a17000002003601000000000000c0

000000000000460000000072eef3c67eced111b71e00c04fc3111a01000000b84a9f4d1c7dcf11861e

0020af6e7c5700000000a001000000000000c000000000000046000000000000000000

192.168.1.204 - UUID e1af8308-5d1f-11c9-91a4-08002b14a0fa 3.0 OPEN VIA 135 ACCESS GRANTED d8060000

[*] Scanned 52 of 55 hosts (094% complete)

[*] Scanned 54 of 55 hosts (098% complete)

The connection timed out (192.168.1.205:135).

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

[*] Auxiliary module execution completed

msf auxiliary(tcp_dcerpc_auditor) > As you can see, this quick scan has turned up some available

services on a number of our hosts which could warrant further investigation. Next Scanner Discovery Auxiliary Modules Prev Admin VMware Auxiliary Modules