Scanner NetBIOS Auxiliary Modules a11y.text Scanner NetBIOS Auxiliary Modules nbname

a11y.text nbname The nbname auxiliary module scans a range of hosts and determines their hostnames via NetBIOS. msf > use auxiliary/scanner/netbios/nbname

msf auxiliary(nbname) > show options

Module options (auxiliary/scanner/netbios/nbname):


```
  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

  RPORT      137              yes       The target port (UDP)

  THREADS    10               yes       The number of concurrent threads To configure the module, we
```

set the RHOSTS and THREADS values then let it run. msf auxiliary(nbname) > set RHOSTS 192.168.1.200-210

RHOSTS => 192.168.1.200-210

msf auxiliary(nbname) > set THREADS 11

THREADS => 11

msf auxiliary(nbname) > run

[*] Sending NetBIOS status requests to 192.168.1.200->192.168.1.210 (11 hosts)

[*] 192.168.1.200 [METASPLOITABLE] OS:Unix Names:(METASPLOITABLE, WORKGROUP)

Addresses:(192.168.1.208) Mac:00:00:00:00:00:00

[*] 192.168.1.201 [XEN-XP-SPLOIT] OS:Windows Names:(XEN-XP-SPLOIT, WORKGROUP)

Addresses:(192.168.1.201) Mac:8a:e9:17:42:35:b0

[*] 192.168.1.203 [XEN-XP-FUZZBOX] OS:Windows Names:(XEN-XP-FUZZBOX, WORKGROUP)

Addresses:(192.168.1.203) Mac:3e:ff:3c:4c:89:67

[*] 192.168.1.205 [XEN-2K3-64] OS:Windows Names:(XEN-2K3-64, WORKGROUP,

__MSBROWSE__) Addresses:(192.168.1.205) Mac:3a:f1:47:f6:a3:ab

[*] 192.168.1.206 [XEN-2K3-EXPLOIT] OS:Windows Names:(XEN-2K3-EXPLOIT, WORKGROUP)

Addresses:(192.168.1.206) Mac:12:bf:af:84:1c:35

[*] Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(nbname) > nbname_probe a11y.text nbname_probe Note: The nbname_probe module

is no longer in the Metasploit framework. The nbname_probe auxiliary module uses sequential

NetBIOS probes to determine the NetBIOS names of the remote targets. msf > use

auxiliary/scanner/netbios/nbname_probe

msf auxiliary(nbname_probe) > show options

Module options (auxiliary/scanner/netbios/nbname_probe):

Name	Current Setting	Required	Description
CHOST		no	The local client address
RHOSTS		yes	The target address range or CIDR identifier
RPORT	137	yes	The target port
THREADS	1	yes	The number of concurrent threads The only configuration we need

for this module is to set our RHOSTS and THREADS values and let it run against our remote

targets. msf auxiliary(nbname_probe) > set RHOSTS 192.168.1.200-210

RHOSTS => 192.168.1.200-210

msf auxiliary(nbname_probe) > set THREADS 11

THREADS => 11

msf auxiliary(nbname_probe) > run

[*] 192.168.1.200 [METASPLOITABLE] OS:Unix Names:(METASPLOITABLE, WORKGROUP)

Addresses:(192.168.1.208) Mac:00:00:00:00:00:00

[*] Scanned 07 of 11 hosts (063% complete)

[*] 192.168.1.201 [XEN-XP-SPLOIT] OS:Windows Names:(XEN-XP-SPLOIT, WORKGROUP)

Addresses:(192.168.1.201) Mac:8a:e9:17:42:35:b0

[*] Scanned 08 of 11 hosts (072% complete)

[*] 192.168.1.203 [XEN-XP-FUZZBOX] OS:Windows Names:(XEN-XP-FUZZBOX, WORKGROUP)

Addresses:(192.168.1.203) Mac:3e:ff:3c:4c:89:67

[*] 192.168.1.205 [XEN-2K3-64] OS:Windows Names:(XEN-2K3-64, WORKGROUP,

__MSBROWSE__) Addresses:(192.168.1.205) Mac:3a:f1:47:f6:a3:ab

[*] Scanned 09 of 11 hosts (081% complete)

[*] Scanned 10 of 11 hosts (090% complete)

[*] 192.168.1.206 [XEN-2K3-EXPLOIT] OS:Windows Names:(XEN-2K3-EXPLOIT, WORKGROUP)

Addresses:(192.168.1.206) Mac:12:bf:af:84:1c:35

[*] Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(nbname_probe) > Next Scanner POP3 Auxiliary Modules Prev Scanner IMAP Auxiliary

Modules