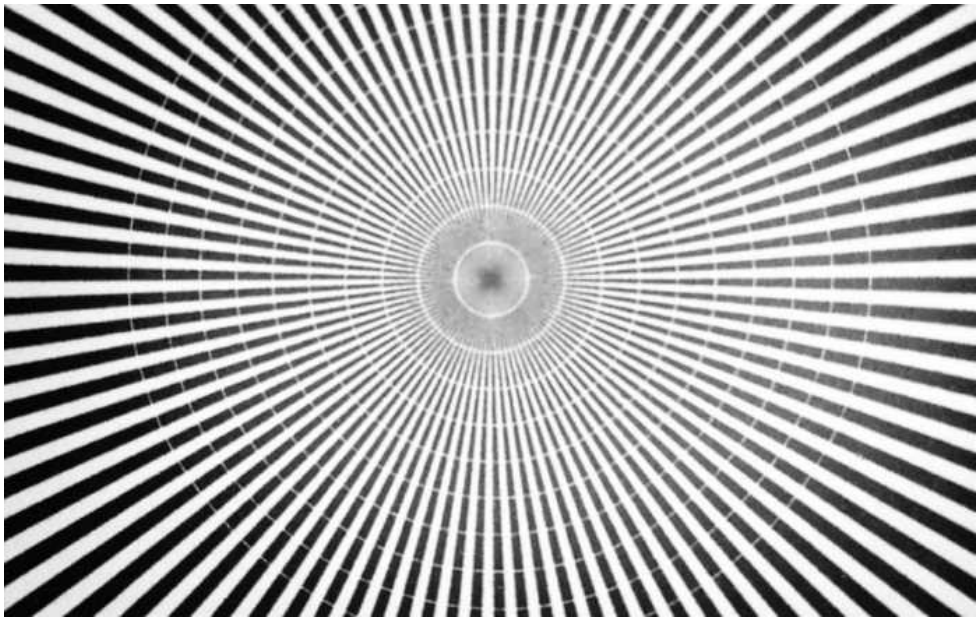
Directory Exploitation Tools

Windows Local Privilege Escalation PowerUp

November 23, 2015 282 0



This Week

Create a Fake AP and Sniff Data mitmAP

August 18, 2017

Windows Local Privilege Escalation PowerUp

Windows Local Privilege Escalation PowerUp is a powershell tool to assist with local privilege escalation on Windows systems. It contains several methods to identify and abuse vulnerable services, as well as DLL hijacking opportunities, vulnerable registry settings, and escalation opportunities.

The privesc/powerup/allchecks module implements a variety of checks for common Windows misconfigurations useful for privilege escalation. It will check:

- if you are an admin in a medium integrity process (exploitable with bypassuac)
- for any unquoted service path issues
- for any services with misconfigured ACLs (exploitable with service_*)
- any improper permissions on service executables (exploitable with service_exe_*)
- for any leftover unattend.xml files
- if the AlwaysInstallElevated registry key is set
- if any Autologon credentials are left in the registry

Recover files encrypted by the WannaCry ransomware wanakiwi

August 2, 2017

Advanced Stealthy Dropper Dr0p1t Framework

August 2, 2017

Bruteforcing From Nmap Output BruteSpray

August 1, 2017

Powerful WiFi Social Trap RogueSploit

March 5, 2017

Collaborative Penetration Test & Vulnerability Management Platform Faraday

February 6, 2017

Reverse Engineering Framework radare2

February 6, 2017

Automating Phishing Activities PhishLulz

December 24, 2016

Web Based Wireless Vulnerability Assessment Solution AtEar

December 22, 2016

Automated ettercap TCP/IP Hijacking Tool Morpheus

December 22, 2016

- for any encrypted web.config strings and application pool passwords
- for any %PATH% .DLL hijacking opportunities (exploitable with write_dllhijacker)

Service Enumeration:

```
Get-ServiceUnquoted          -   returns servic
Get-ServiceEXEPerms          -   returns servic
Get-ServicePerms             -   returns servic
```

Service Abuse:

```
Invoke-ServiceUserAdd        -   modifies a mod
Write-UserAddServiceBinary   -   writes out a p
Write-CMDServiceBinary       -   writes out a p
Write-ServiceEXE             -   replaces a ser
Write-ServiceEXECMD          -   replaces a ser
Restore-ServiceEXE           -   restores a rep
```

Section

DLL Hijacking:

```
Invoke-FindDLLHijack          -   finds DLL hija
Invoke-FindPathHijack         -   finds service
```

Registry Checks:

```
Get-RegAlwaysInstallElevated  -   checks if the
Get-RegAutoLogon              -   checks for Au
```

Misc. Checks:

```
Get-UnattendedInstallFiles  -   finds remaining
Get-Webconfig               -   checks for any
Get-ApplicationHost         -   checks for encr
Invoke-CheckLocalAdmin      -   checks if the u
```

Helpers:

```
Invoke-AllChecks        -   runs all current es
Write-UserAddMSI        -   write out a MSI ins
Invoke-ServiceStart     -   starts a given serv
Invoke-ServiceStop      -   stops a given servi
Invoke-ServiceEnable    -   enables a given ser
Invoke-ServiceDisable   -   disables a given se
Get-ServiceDetails      -   returns detailed ir
```

SOURCE Source & Download

TAGS Exploitation Exploitation Tools PowerShell Vulnerability Windows

Previous article

Nasty Android Malware Allows Adware to Install Without User Permission

Next article

Anonymous Has Shutdown 28,000+ ISIS' Twitter Accounts Since OpParis Began

RELATED ARTICLES MORE FROM AUTHOR

Exploitation Tools

Python Keylogger Radium

Exploitation Tools

Customized Payload Generator ARCANUS

Exploitation Tools

Command Line Attack Driven Penetration Testing Tool Ranger

Exploitation Tools

CTF Framework and Exploit Development Library binjitsu

Exploitation Tools

Powershell Penetration Testing Framework Pentestly

Exploitation Tools

Shell Exploit Generation Shellsploit

LEAVE A REPLY

Comment:

Name:*

Email:*

Website:

Post Comment

UAE INFORMATION SECURITY

UAE Information Security is one of the best resource for Information Security Research, Penetration Testing Professional , Security Analyst and Security Engineer. UAE Information Security is now one of most trusted online community for security professionals like you.

Contact us: info@uaeinfosec.com