Emulating the Adversary in Post-Exploitation

Jake Williams (@MalwareJake)
Rendition Infosec
www.rsec.us
@RenditionSec

RENDITION INFOSEC
Cybersecurity by any legal means

$whoami

- Founder and President of Rendition Infosec
- IANS Faculty
- Endorsed by the Shadow Brokers
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

- What are adversaries doing that we aren't?
- Never go full cyber!
- Techniques for adversary emulation
- Conclusion

What are adversaries doing that we aren’t?

AKA: How do we get executives to pay attention to our reports?

The Process

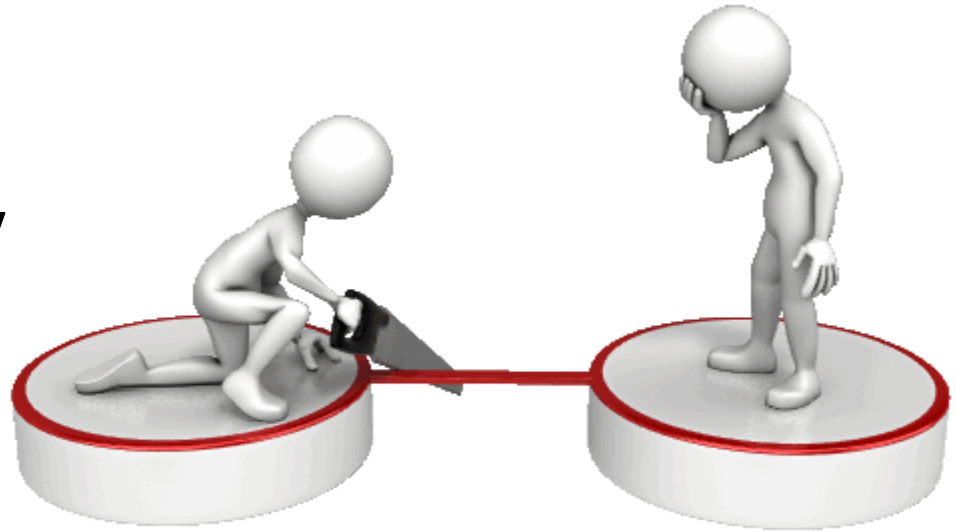
- We all know the standard pentest/red team process
  - Note: we are not arguing over definitions here, because:
    1. It's not relevant to the talk
    2. I don't care

On further inspection, this actually IS missing a step:
Arguing about the findings and severity…

The Disconnect

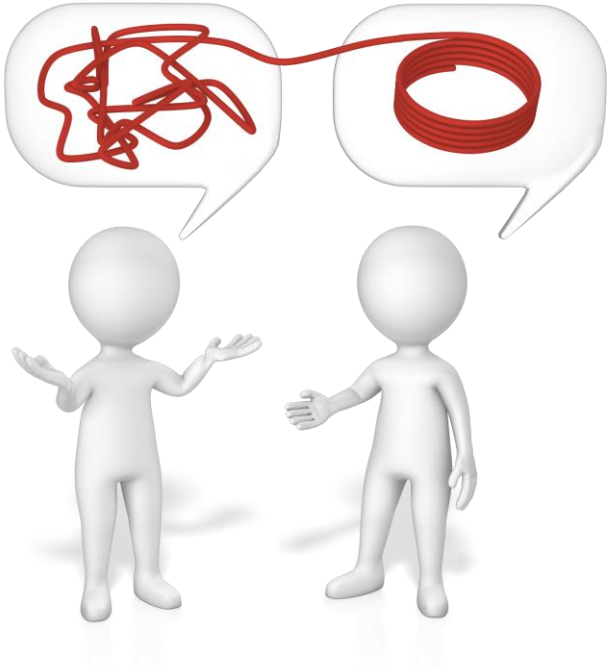
- After an incident, there's rarely a case where the exploitation vectors aren't remediated
  - Yet this occurs routinely after a penetration test

- Why the disconnect?
  - Hint: it's about WAY more than just liability



The Disconnect (2)

- As humans, we are inherently loss averse
  - We will spend more to avoid a loss than to gain the same



- Most humans are also better at understanding tangible things than their intangible counterparts
  - With an incident, there's a tangible loss
  - In an average pentest report, there's a technical summary of vulnerabilities, leaving decision makers to spot potential risks

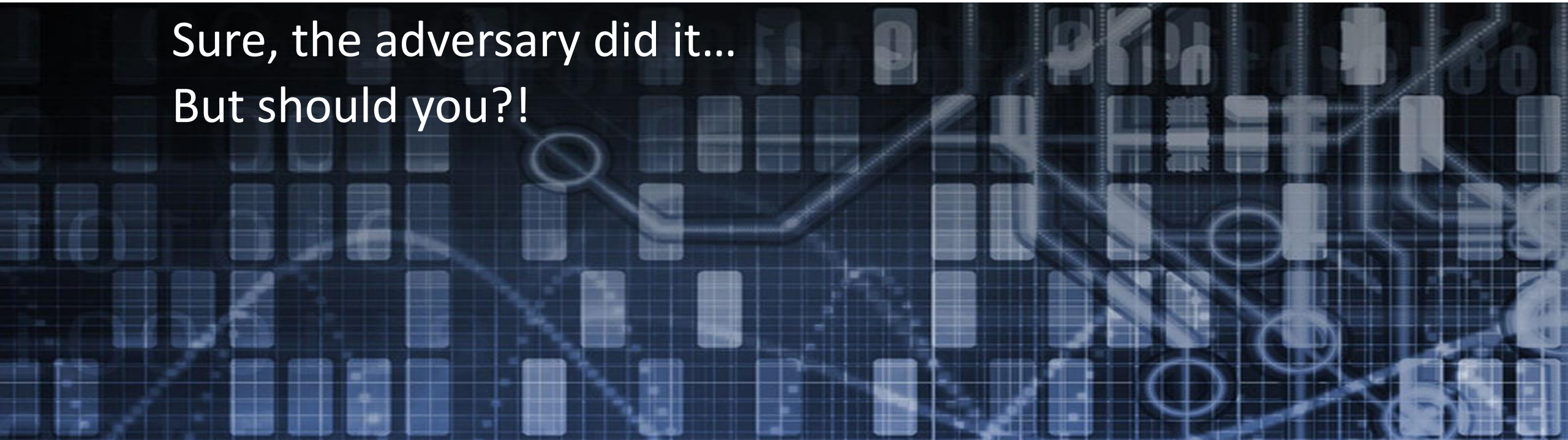
Stop Focusing On Domain Admin

- Stop focusing on domain admin in your penetration test reports
- That's it
- That's the whole slide

Stop Focusing On Domain Admin (2)

- Even saying “keys to the kingdom” doesn’t help create a concrete image for stakeholders
- Do better – explain the impact of what you’ve found
- This doesn’t have to be done for every vuln you discover, but create impact scenarios for the vulnerabilities you know need to be addressed

Never go full cyber!



Sure, the adversary did it…

But should you?!

Should We Completely Emulate The Adversary?

- Absolutely not – never go full cyber!
- Use common sense – just because an attacker is willing to take a risk with your client's infrastructure, should you?
  - Hint: of course not!
- Consider the impacts of reporting particularly sensitive data discovered in the course of the assessment

Choose Wisely

- Things to avoid in practice:
  - Locking out accounts (duh)
  - Anything that might destroy data or impact systems (duh)
  - Anything involving switching (STP is a fickle beast)
  - Actually exfiltrating sensitive, and especially regulated data
  - Exploiting storage devices and controllers
  - Performing post-exploitation activities on hypervisors

Techniques for adversary emulation

Top Post-exploitation Techniques

- In this section, we'll discuss the following post-exploitation techniques for demonstrating impact after the compromise:
  - Pivot to data the user already has access to
  - Hunt for the most sensitive documents
  - Target backups
  - Compromise source code
  - Plant web shells
  - Dump WiFi and VPN configurations

Pivot To User Accessible Data

- So you landed that first phishing email and have a shell
  - Should you immediately pivot?

- Consider examining what's in the user's mapped drives

```
PS C:\Users\IEUser> get-psdrive

Name           Used (GB)     Free (GB) Provider      Root
----           ---------     --------- --------      ----
Alias                                  Alias
C                  18.04         21.35 FileSystem    C:\
Cert                                   Certificate   \
D                                      FileSystem    D:\
E                                      FileSystem    E:\
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USE
HKLM                                   Registry      HKEY_LOCAL_MACHINE
S                  24.18         35.48 FileSystem    \\192.168.13.142\secrets
Variable                               Variable
WSMan                                  WSMan
Z                                      FileSystem    \\vmware-host\Shared Folders
```

```
C:\Users\IEUser>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           S:        \\192.168.13.142\secrets  Microsoft Windows Network
             Z:        \\vmware-host\Shared Folders
                                                  VMware Shared Folders
The command completed successfully.
```

Pivot To User Accessible Data

- Think about the user's recently accessed documents

```
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.ppt
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.pptx
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.py
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.ssv
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.tlp
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.txt
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.vmx
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.vsdx
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.webp
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.xls
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.xlsx
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\.zip
HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\recentdocs\Folder

C:\Users\jake>reg query "hkcu\software\microsoft\windows\currentversion\explorer\recentdocs"
```

Pivot To User Accessible Data

- Decoding Data

```
    107    REG_BINARY    320030003200300030003300300036002000 2D00200042005300690064006500730020004E004F005600410020002D0
020004D004100200044007500650020004400690006C006900670065006E006300650020002D00200043006F00700079002E007000700074007800000
0EC00320000000000000000000000323032303033036202D20425369646573204E4F5641202D204D41204475652044696C6967656E6365202D20436
F70792E707074782E6C6E6B00A40009000400EFBE0000000000000002E0000000000000000000000000000000000000000000000000000000320
030003200300030003300300036002000 2D00200042005300690064006500730020004E004F005600410020002D0020004D004100200044007500650
020004400690006C006900670065006E006300650020002D00200043006F00700079002E007000700074007800 2E006C006E006B00000048000000
    140    REG_BINARY    700072006500730065006E007400610074006900 6F006E00730000007400320000000000000000000000070726573656
E746174696F6E732E6C6E6B0054000900400EFBE0000000000000002E0000000000000000000000000000000000000000000000000000000000700
072006500730065006E007400610074006900 6F006E0073002E006C006E006B00000020000000
    2
26E6574
5002000
    47
4C00090
6100700
```

```
>>> fname
'2\x000\x002\x000\x000\x006\x000\x004\x00-\x00 \x00H\x00a\x00c\x00k\x00f\x00e\x00s\x00t\x00 \x00E\x00m\x00u\x00l\x00a\x0
0t\x00i\x00n\x00g\x00 \x00t\x00h\x00e\x00 \x00A\x00d\x00v\x00e\x00r\x00s\x00a\x00r\x00y\x00.\x00p\x00p\x00t\x00x\x00\x00
\x00Ú\x002\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0020200604- Hackfest Emulating the Adversary.pptx.lnk\x00\x98\x00\t\
x00\x04\x00ï¾\x00\x00\x00\x00\x00\x00\x00\x00.\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x002\x000\x002\x000\x000\x006\x000\x004\x00-\x00 \x00H\x00a\x00c\x00k\x00f\x00e\x
00s\x00t\x00 \x00E\x00m\x00u\x00l\x00a\x00t\x00i\x00n\x00g\x00 \x00t\x00h\x00e\x00 \x00A\x00d\x00v\x00e\x00r\x00s\x00a\x
00r\x00y\x00.\x00p\x00p\x00t\x00x\x00.\x00l\x00n\x00k\x00\x00\x00B\x00\x00\x00'
```

```
>>> fname = ''
>>> for i in range(0, len(x),2):
...   print(x[i:i+2] + " = " + chr(int(x[i:i+2], 16)))
...   fname +=  chr(int(x[i:i+2], 16))
...
```

Hunt For The Most Sensitive Documents

- Sometimes you're presented with hundreds (or even thousands) of documents
  - You can't (and shouldn't) exfiltrate them all
  - Saying "we were able to access these thousands of documents" doesn't communicate impact
  - Be real, in many cases the client forgot those files existed or has no idea what's in them
  - And you really don't have time to open lots of documents and performing analysis individually

Tika To The Rescue!

- While we can't natively read office documents, we can extract data from them using Tika
  - The worst part about Tika is that it requires Java
  - And it's HUGE (70MB+)

```
C:\Users\IEUser>type "Desktop\20200604- Hackfest Emulating the Adversary.pptx" |findstr /i exfil

C:\Users\IEUser>java -jar Downloads\tika-app-1.24.1.jar "Desktop\20200604- Hackfest Emulating the Adversary.pptx" |findstr /i exfil
Jun 03, 2020 5:38:20 PM org.apache.tika.config.InitializableProblemHandler$3 handleInitializableProblem
WARNING: J2KImageReader not loaded. JPEG2000 files will not be processed.
See https://pdfbox.apache.org/2.0/dependencies.html#jai-image-io
for optional dependencies.

Jun 03, 2020 5:38:20 PM org.apache.tika.config.InitializableProblemHandler$3 handleInitializableProblem
WARNING: org.xerial's sqlite-jdbc is not loaded.
Please provide the jar on your classpath to parse sqlite files.
See tika-parsers/pom.xml for the correct version.
<p>Actually exfiltrating sensitive, and especially regulated data</p>
<p>You canΓÇÖt (and shouldnΓÇÖt) exfiltrate them all</p>
```

Use Tika To Find Your “Keys To The Kingdom”

- To demonstrate maximum impact, we ask what specific data would hurt the business the most if it were targeted
- Once we get Tika into the environment, we can use it to parse text from documents
  - If in scope, the extracted text can be zipped and exfiltrated en-masse

- This prevents the client from wondering “does this matter”

Target Backups

- Targeting backup servers is a great way to find sensitive data
- We've found backups on open iSCSI endpoints
  - Made me laugh extra hard when this happened to Hacking Team
- When you find a backup, don't make it about the data you have
  - Instead, report that you can run the server you have the backup of
  - For some reason, the idea of attackers duplicating their infrastructure really eats at stakeholders

Compromise Source Code

- If you can compromise a developer or a source code repository, you can do (at least) two things:
  - Exfil source code (this IS a serious business impact for most orgs)
  - Add a backdoor to the source code

- Rendition has demonstrated changing source code on multiple occasions - https://www.youtube.com/watch?v=Rc-eEArQV4Q

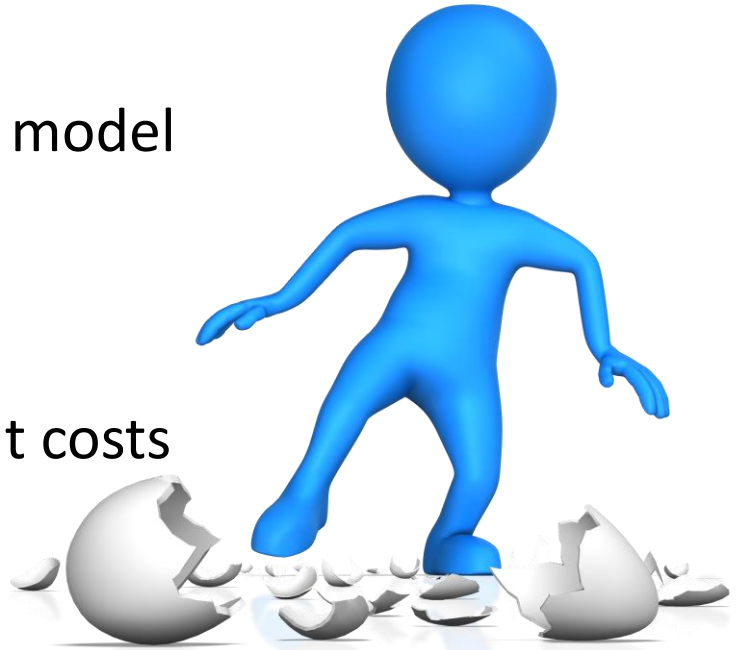
- Don't forget to look in source code for passwords and API keys

Plant Web Shells

- In most environments, web shells are difficult to detect
- Post-breach, the effort to hunt for web shells (beyond a cursory examination) is a significant expense if the organization doesn't know what "good" looks like in their code base
  - Hint: few do
- Stakeholders detest uncertainty – highlight how web shells were planted as long term backdoors but were undetected

Plant Web Shells (2)

- Even in cases where a refined build and deploy system exists, redeploying an entire web application infrastructure is not easy
  - Or cheap
  - Usually the shops that can do this effectively use a DevOps model
- Even when infrastructure can be rebuilt, it's not easy
  - Work with infosec stakeholders to obtain information about costs of previous outages in web application infrastructure
  - This helps highlight the impact



Plant Web Shells (3)

- In most cases where you'd have access to plant a web shell, you also have access to change existing files
- It's easy to demonstrate a modification that logs plaintext usernames and passwords to a text file (don't ACTUALLY do this)
- In an e-commerce application, the same modification can be used to store credit card numbers or exfiltrate session IDs

Dump WiFi and VPN Configurations

- Hunting VPN configurations is fun, but dumping Wifi configurations makes things personal

- Most workers have connected their laptops to home Wifi
  - Demonstrating that you can dump their Wifi configurations (including passwords) for their home networks is something that gets attention

```
C:\Users\jake>netsh wlan export profile

Interface profile "eternallyblue_5G_2" is saved in file ".\Wi-Fi-eternallyblue_5G_2.xml" successfully.

Interface profile "eternallyblue_guest_5G" is saved in file ".\Wi-Fi-eternallyblue_guest_5G.xml" successfully.
```

Closing Thoughts

Conclusion

Emulating an adversary in post-exploitation helps stakeholders understand impact

Unlike traditional adversary emulation, this doesn't require substantial CTI resources

Choose your actions carefully in order to avoid negatively impacting security

@MalwareJake

@RenditionSec

www.rsec.us