

# The Darkside of Red-Teaming?

Common Traps & Pitfalls  
In Recent Red-Teaming

©2018 Netscylla

# Content

- Introduction
- OSINT
- SMTP
- HTTP(S)
- C2C
- Payloads
- Reporting
- Bonus Round / Extra Time



## Red-Side

**Andy Davies**

Old skool pentester from circa  
2000

Developer of some popular  
scripts & hardware

Professional experience in  
infosec consulting +15 yrs

Track day addict





## Blue-Side

### Jon Medvenics

Young-blood Blue team generalist

Malware, Network and Incident analysis. Is currently the Cyber Incident Response lead for the Houses of Parliament.

Get's jumpy at the mention of "Bears"

Spends too much time trying to understand the Red Team just to trip them up in engagements.

ENFP



VS



[http://rvb.wikia.com/wiki/File:Red\\_Team\\_Jersey.jpg](http://rvb.wikia.com/wiki/File:Red_Team_Jersey.jpg)

<http://gamebattles.majorleaguegaming.com/xboxone/halo-5-guardians/team/blue-team-na-ot-5>



©2018 Netscylla

# Testing from your own IP!

Who here has tested from their own IP or corporate range?



# Testing from your own IP!

Who here has tested from their own IP or corporate range?

Why this is bad.....



# Whois

Selection of 'Whois'  
Commands:

```
whois 4.2.2.1
whois -h whois.geektools.com
4.2.2.1
whois -a -T inetnum <org>
```

```
> whois -h whois.pwhois.org 4.2.2.1
IP: 4.2.2.1
Origin-AS: 3356
Prefix: 4.0.0.0/9
AS-Path: 3257 3356
AS-Org-Name: Level 3 Communications, LLC
Org-Name: Level 3 Communications, Inc.
Net-Name: LVLT-ORG-4-8
Cache-Date: 1240446962
Latitude: 39.913500
Longitude: -105.093000
City: BROOMFIELD
Region: COLORADO
Country: UNITED STATES
```

[https://commons.wikimedia.org/wiki/File:Pwhois\\_query.png](https://commons.wikimedia.org/wiki/File:Pwhois_query.png)





# Ever heard of a Firewall?



<https://pixabay.com/en/firewall-security-internet-web-29940/>

# Cloud Accounts?



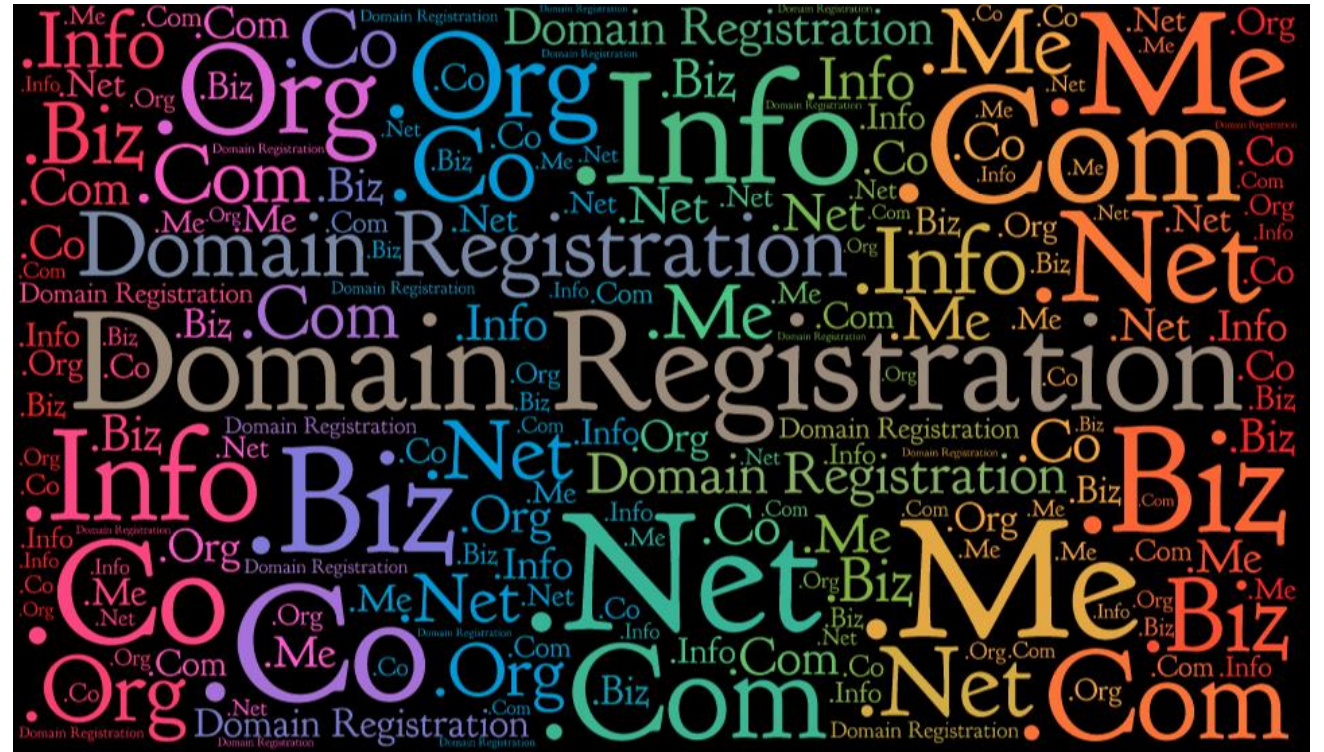
# Choosing a Domain!

Why should we be careful around choosing domains?

# Domains

Purchasing domains:

- Typo squatting
- Include organisation name in domain name?
- Generic domain, organisation name as subdomain?
- Expired domains.



[https://www.flickr.com/photos/india\\_7/15881201596](https://www.flickr.com/photos/india_7/15881201596)

# Domains – Legalities

- DCMA - digital copyright law
- RIPE/ARIN/IPNIC/AfriNIC/APNIC/LACNIC domain seizures if use similar name, or trademark infringement
- When you pay for domains/ISP through personal Credit Card – you details are stored and may be passed on to authorities



# Danger!



- [https://commons.wikimedia.org/wiki/File:Day\\_296\\_-\\_West\\_Midlands\\_Police\\_-\\_Two\\_Person\\_Enforcer\\_\(8112650465\).jpg](https://commons.wikimedia.org/wiki/File:Day_296_-_West_Midlands_Police_-_Two_Person_Enforcer_(8112650465).jpg)



# Setting up Mail in a Day?

Who here has had 1-day to set up a mail-server/  
phishing server for red-teaming?



# Testing from your own IP!

Who here has had 1-day to set up a mail-server/  
phishing server for red-teaming?

Why this is bad.....





# SMTP

- Dont forget to scrub your mail headers
- Remember to set an appropriate hostname
- use multi content, plain text and html
- catch all email, you might receive mail?



<https://pixabay.com/en/icon-e-mail-e-mail-mail-2898669/>

# SMTP – Hide your Origin, or go back to Slide 1

Postfix

```
define(`confRECEIVED_HEADER',`by $j ($v/$Z)$?r with $r$. id $i; $b')dnl
```



# SMTP – Hide your Origin; Go to Jail



# SMTP – SEM FRESH Blacklists

- Allow time for SEM FRESH blacklist to dissipate ( 5, 10, 15 30 days)
- Set up SPF/DKIM/DMARC
- Test against <https://spameatingmonkey.com> before delivery!



[https://i2-prod.walesonline.co.uk/incoming/article9796488.ec/e/ALTERNATES/s615b/MH2\\_7829.jpg](https://i2-prod.walesonline.co.uk/incoming/article9796488.ec/e/ALTERNATES/s615b/MH2_7829.jpg)

# Setting up a Phishing Site/Waterhole?

## Do you use automated tooling to build websites?



# HTTP(S)

- HTTrack
- Exploit Frameworks
  - Beef
  - Empire
- Domain Categorisation
- Site/C2C remember to implement SSL - its free with letsencrypt



<https://en.wikipedia.org/wiki/HTTPS>



# HTTrack

- It will insert a comment similar to the following in the **header and footer**:

```
<!-- Mirrored from www.example.com/ by HTTrack  
Website Copier/3.x [XR&CO'2013], Sat, 07 Apr  
2018 12:57:02 GMT -->
```

# Beef

The Defaults:

- Hook.js
- BEEFSESSION

Easily detected by any security gateway / proxy.





# Empire

- Powershell exploit framework
- Similar to Metasploit
- Lots of prebuilt modules
- Handy for leveraging Windows hosts
- Known default Endpoints:
  - /admin/news.php
  - /admin/get.php
  - /login/process.php



<https://www.powershellempire.com/>

# Domain Categories

## Old Skool

### Domain or IP

example.com

### Host

www.example.com

ftp.example.com

## Getting better

### Directory

example.com/directory1

### File Name

example.com/puppies.jpg

example.com/locky.php

## Getting too clever

### Query String

example.com/?sk=admin

example.com/?sk=fart



# Domain Categorisation

- Bluecoat/Symantec - <https://sitereview.bluecoat.com/sitereview.jsp>
- McAfee - <https://www.trustedsource.org>
- Palo Alto Wildfire - <https://urlfiltering.paloaltonetworks.com>
- Websense - <https://csi.forcepoint.com> & <https://www.websense.com/content/SiteLookup.aspx> (needs registration)
- Fortiguard - <http://www.fortiguard.com/iprep>
- IBM X-force - <https://exchange.xforce.ibmcloud.com>
- F-Secure SENSE - [https://www.f-secure.com/en/web/labs\\_global/submit-a-sample](https://www.f-secure.com/en/web/labs_global/submit-a-sample)
- Checkpoint - <https://www.checkpoint.com/urlcat/main.htm> (needs registration)
- Squid - [https://www.urlfilterdb.com/suggestentries/add\\_url.html](https://www.urlfilterdb.com/suggestentries/add_url.html)
- <https://community.opendns.com/domaintagging/>
- <https://www.brightcloud.com/tools/change-request-url-categorization.php>
- <https://archive.lightspeedsystems.com>
- <https://support.forcepoint.com/KBArticle?id=How-To-Submit-Uncategorized-Sites>

# Transport Encryption aka SSL

- No excuses!
- Promised clients/customers you'll handle their data securely
- GDPR 25th May 2018
- Free from following providers:
  - Letsencrypt
  - Comodo trial certificate (30 days)
  - ZeroSSL
  - Many more, but we are not going into this deep here!



# Blue Team and the use of CC and tracking

- The Blue Team may have links to local law enforcement?
  - Or through a third party?
- How did you pay for those domains and hosting?
- Government and law enforcement bodies can request banks and financial institutions to cough up CC ownership details
- This means LEO's will have your name and card holder address!

LEO = Law Enforcement Officer

# Using personal Credit Cards!



- [https://commons.wikimedia.org/wiki/File:Day\\_296\\_-\\_West\\_Midlands\\_Police\\_-\\_Two\\_Person\\_Enforcer\\_\(8112650465\).jpg](https://commons.wikimedia.org/wiki/File:Day_296_-_West_Midlands_Police_-_Two_Person_Enforcer_(8112650465).jpg)

# Command & Control



- [https://commons.wikimedia.org/wiki/File:Virus\\_malware\\_hazard\\_icon.svg](https://commons.wikimedia.org/wiki/File:Virus_malware_hazard_icon.svg)

# C2C – From the Outside

- Don't use your corporate IP address space
  - Attempt to use proxies/redirectors in the cloud
- Don't use hacking tools in default configurations
  - Empire, Metasploit
- Don't use default/known webshells
  - At least create some form of authentication/ authorization for the shell
  - We don't want a hackergroup pivoting in off our tools
- Remember to use SSL



# C2C – From the Inside

Important things to remember:

- Don't leave your hostname as Kali
- Don't immediately email the office email – to debug phishing? Or test mail out capability
- Download any popular hacking tools
  - Nmap, Crackmapexec, Responder, Metasploit, Empire, Powersploit, Bloodhound, Superscan, Caine and able, etc
- Don't immediately start brute forcing accounts.
- Don't steal the IP of a nearby worker, at start attacking the network!



# Payloads

- PDF
- DOC(X)
- XSL(X)
- RTF
- URL
- PS1
- ZIP



# Payloads – Meta Data

- URLs – already covered domains
- EXEs/ZIPs and TAR/TGZ - can leak usernames, pathnames
- DOC/XSL - leak usernames, pathnames, additional files additional meta data
- Images may leak GPS co-ordinates, info about the device, ownership / copyright holder of the image



# Payloads – Meta Data - Tools

- Basic Hex editor: xxd or XIV
- <http://hachoir3.readthedocs.io/>
- <https://github.com/hiddenillusion/AnalyzePDF>
- <https://zeltser.com/peepdf-malicious-pdf-analysis>
- <http://blog.didierstevens.com/programs/pdf-tools/>
- <https://github.com/ElevenPaths/FOCA>

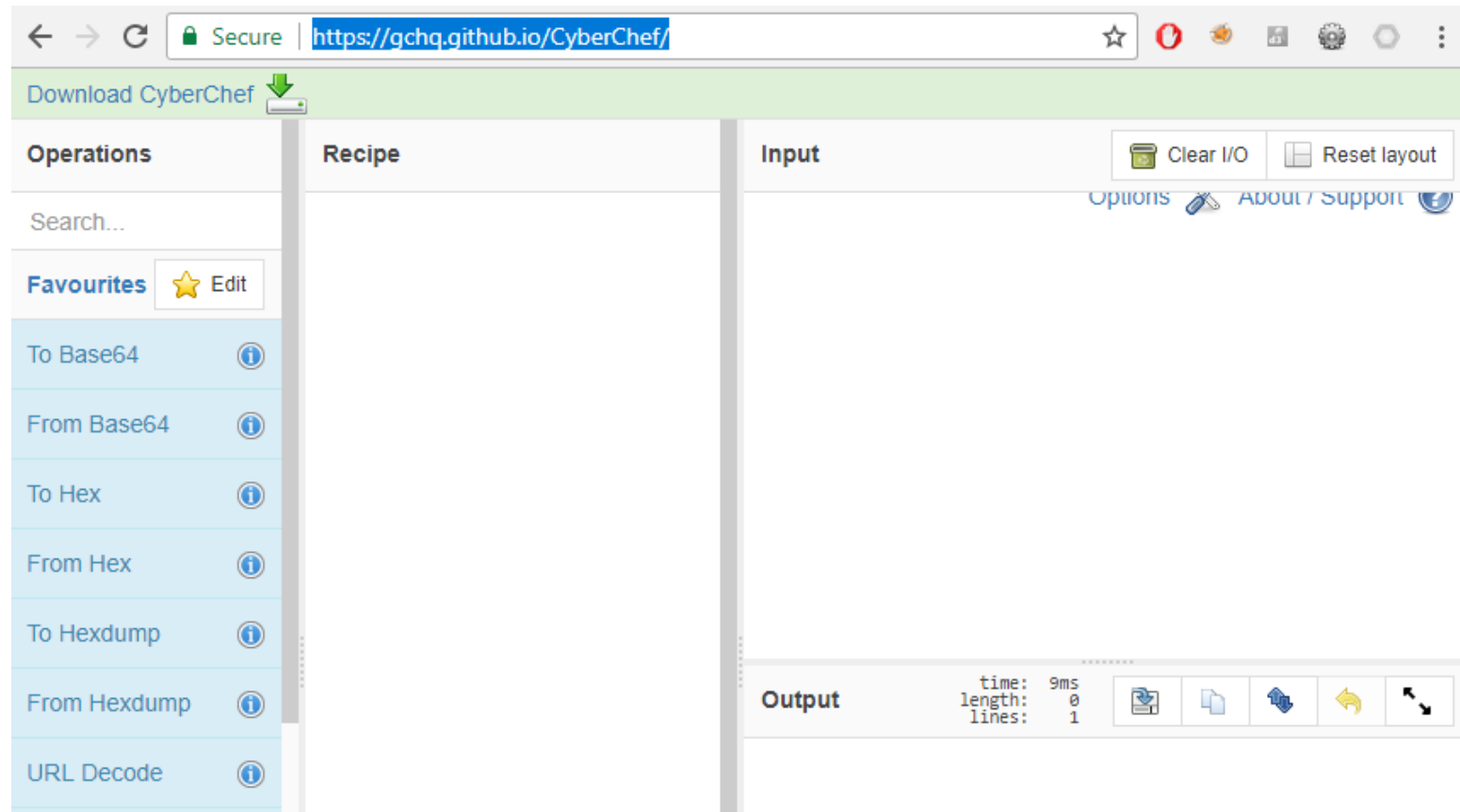


# Payloads – Reversing

- Many security gateways have AV or signature based detection for common attack modules.
- Also companies/blue teams with mature infrastructure, may have custom analysis platforms e.g. Cuckoo
- Automated Sandboxing and analysis, or even manual analysis may mean you get spotted quickly

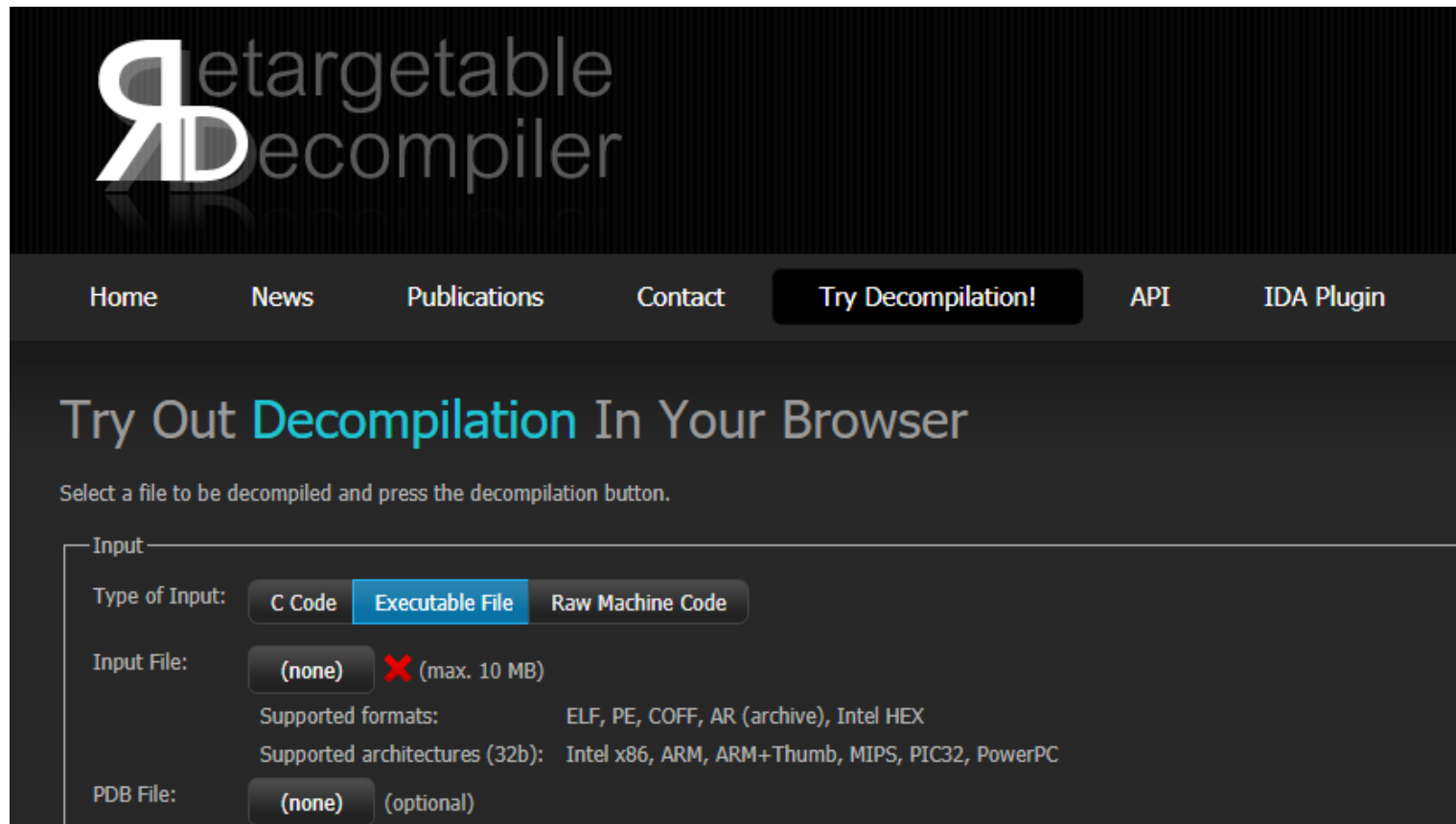
# Payloads – Reversing

- <https://gchq.github.io/CyberChef/>



# Payloads – Reversing

- <https://retdec.com/decompilation/>



The screenshot shows the RetDec web interface. At the top, the logo "retargetable decompiler" is displayed. Below the logo is a navigation bar with links: Home, News, Publications, Contact, Try Decompile! (highlighted), API, and IDA Plugin. The main heading is "Try Out Decompile In Your Browser". Below this, a instruction says "Select a file to be decompiled and press the decompilation button." The "Input" section contains three tabs: "C Code", "Executable File" (selected), and "Raw Machine Code". Under "Executable File", there is a file selection area showing "(none)" and a red "X" icon with the text "(max. 10 MB)". Below this, it lists "Supported formats: ELF, PE, COFF, AR (archive), Intel HEX" and "Supported architectures (32b): Intel x86, ARM, ARM+Thumb, MIPS, PIC32, PowerPC". At the bottom, there is a "PDB File:" section with a "(none)" button and the text "(optional)".



# Metasploit

- Powerful exploit framework
- Lots of prebuilt modules
- Handy for leveraging hosts
- OSINT & Recon Modules
- Most Attackers use this in the real world



<https://twitter.com/msfminute>



# Empire/MSF – Detection & Fingerprinting

## Monitoring

1. Endpoint (Carbon Black, Tanium, etc)
2. Powershell
  1. Script Block logging
  2. Module logging
  3. Transcript logging

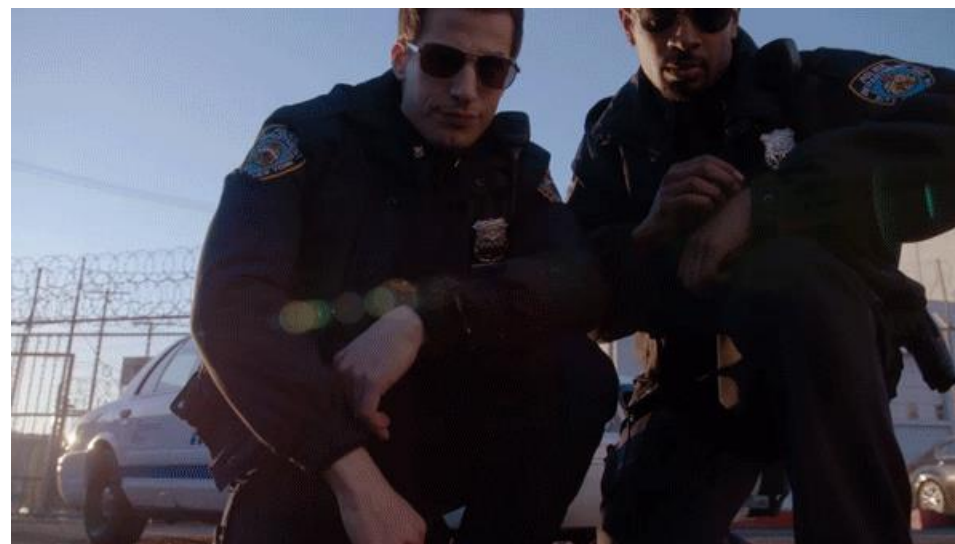
## Default strings

Listener = “powershell -noP -sta -w | enc”

Stager = “/b powershell -noP -sta -w | enc”

*Bonus Points for filtering by parent proc as WScript.*

*(It's scary how often this is forgotten)*



# Empire/MSF – Detection & Fingerprinting

## Antivirus & IDS/IPS

All Antivirus and IDS technology (should) have the capability to detect MSF:

```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e  
aQBmACgAWwBJAG4AdABQAHQAQcgBdADoAOgBTAGkAegBIACAALQ
```

```
$ecv = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer(  
(bwEq8ez kernel32.dll CreateThread), (t1P @([IntPtr], [UInt32], [IntPtr], [IntPtr], [UInt32],  
[IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero,0,$aoOMMDM,[IntPtr]::Zero,0,[IntPtr]::Zero)  
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((bwEq8ez kernel32.dll
```

# Empire/MSF – Detection & Fingerprinting

## Antivirus Continued

All antivirus and ids technology (should) have the capability to detect MSF:

Clamav

=====

test.bin.data: Win.Trojan.MSShellcode-7 FOUND

MSF/Sample Fingerprint

=====

MD5(..../reverse.bin.msff)=

92f42265acf057eab58a7ae8b35ededa

SHA1(..../reverse.bin.msff)=

fdbccfbd1fd4af350c2f12b15f3c814062c86189

windows/meterpreter/reverse\_tcp

windows/meterpreter/reverse\_tcp\_uuid

Clamav

=====

dridex.bin.data: Win.Trojan.MSShellcode-7  
FOUND

MSF/Sample Fingerprint

=====

MD5(dridex.bin.msff)=

836496b1035773f98d23a097b8bc4252

SHA1(dridex.bin.msff)=

9c118ba0b74a76ad6242855bd8470b97ef92f9  
76

windows/shell/reverse\_http

# Payloads – Reversing

What happens when the blue-team identifies you?



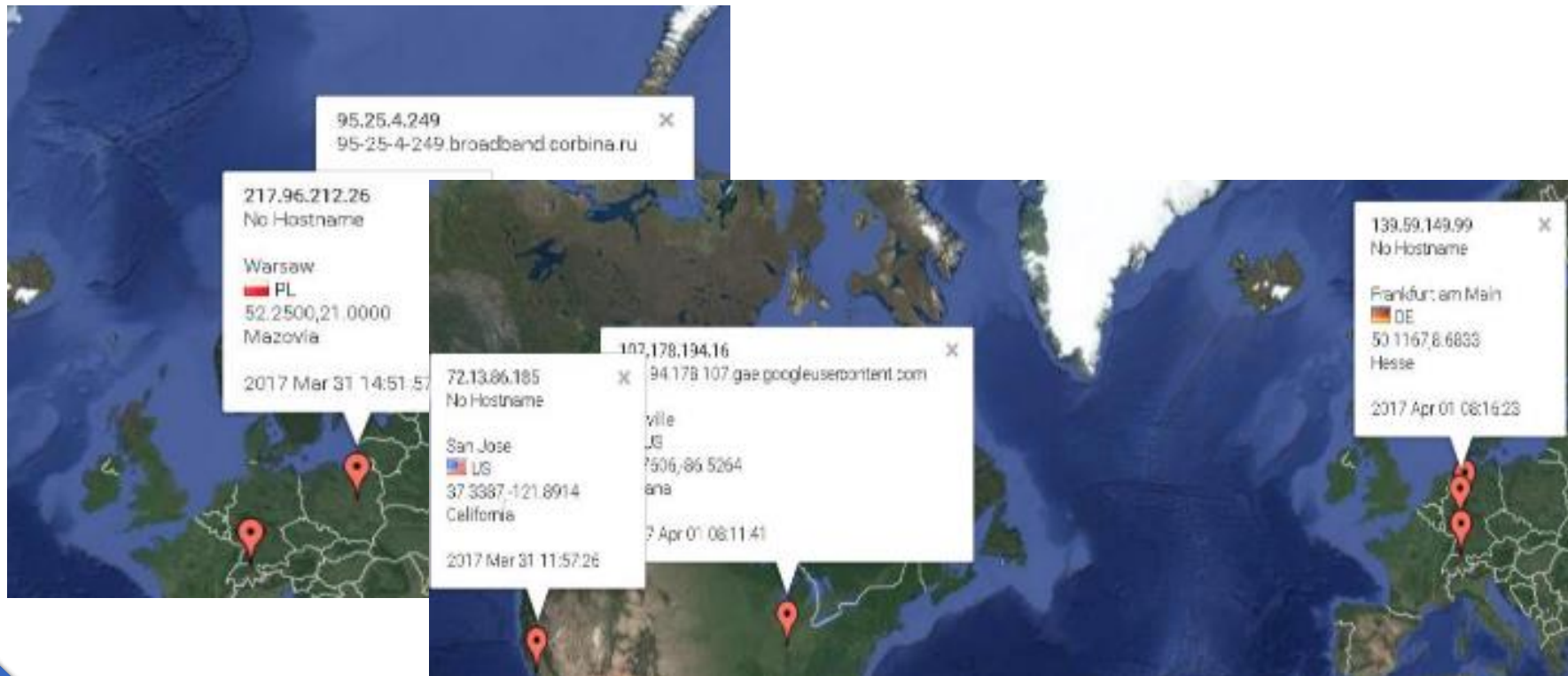
# Payloads – Reversing

We have two responses depending on what side you sit?

The Blue Team

# Payloads – Tracking

## VirusTotal will share your payloads!



# Payloads – Tracking

VirusTotal will share your payloads!

Other Privateers:

- 176.24.96.80
- 213.254.241.7
- 95.211.95.129 (Tor Exit Node)
- 193.226.177.0/24
- 66.102.0.0/20



# Payloads – Tracking

And Authorities may be notified and  
scrambled to your location?



# Leaked Payloads – The Interview



- [https://commons.wikimedia.org/wiki/File:Otakuthon\\_2014- The Men in black taking down a thug \(14850547629\).jpg](https://commons.wikimedia.org/wiki/File:Otakuthon_2014- The Men in black taking down a thug (14850547629).jpg)

# Payloads – Reversing

We have two responses depending on what side you sit?

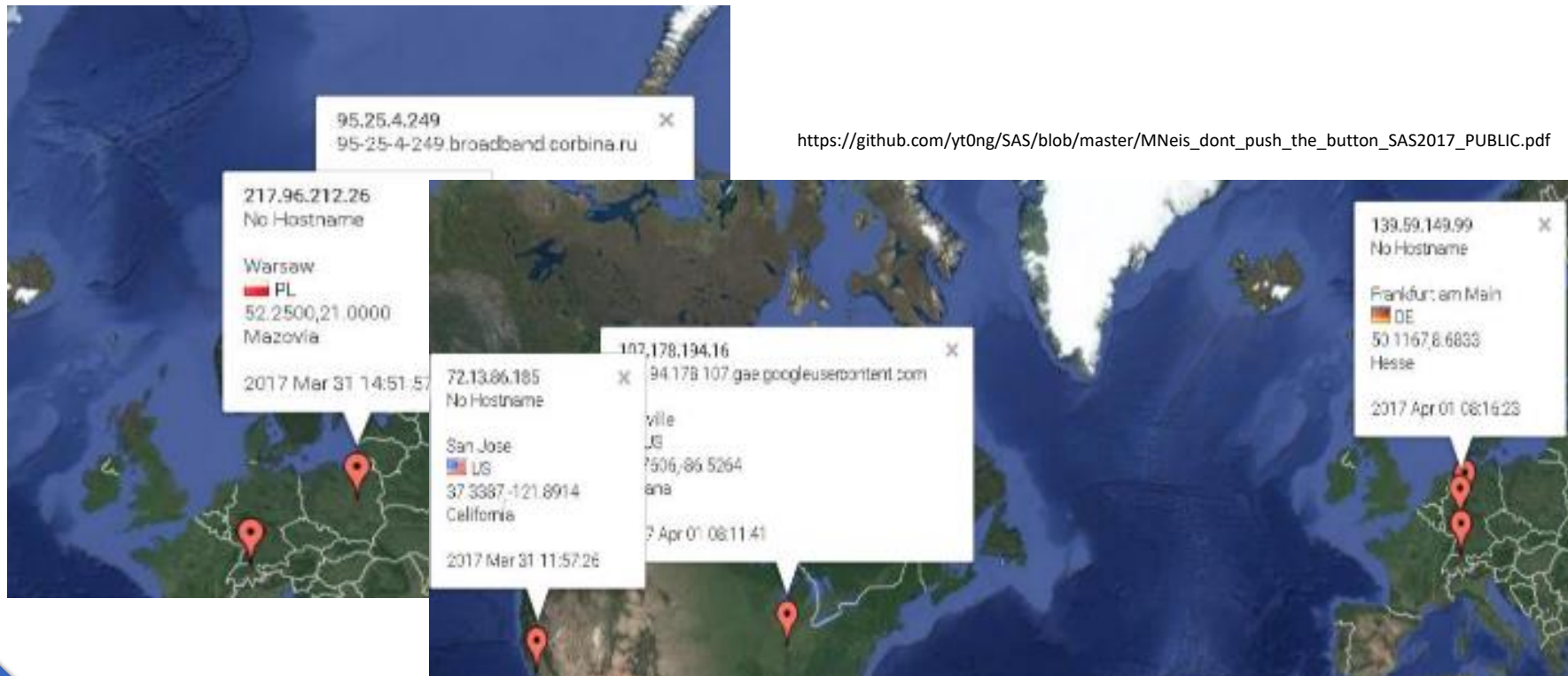
The Red Team

# Payloads – Reversing

How many of you have tested your payload  
in VirusTotal before the RedTeam

# Payloads – Tracking

Again... VirusTotal will share your payloads!



[https://github.com/yt0ng/SAS/blob/master/MNeis\\_dont\\_push\\_the\\_button\\_SAS2017\\_PUBLIC.pdf](https://github.com/yt0ng/SAS/blob/master/MNeis_dont_push_the_button_SAS2017_PUBLIC.pdf)

# Payloads – Tracking

Use you own private system firewalled off  
from rest of the world!

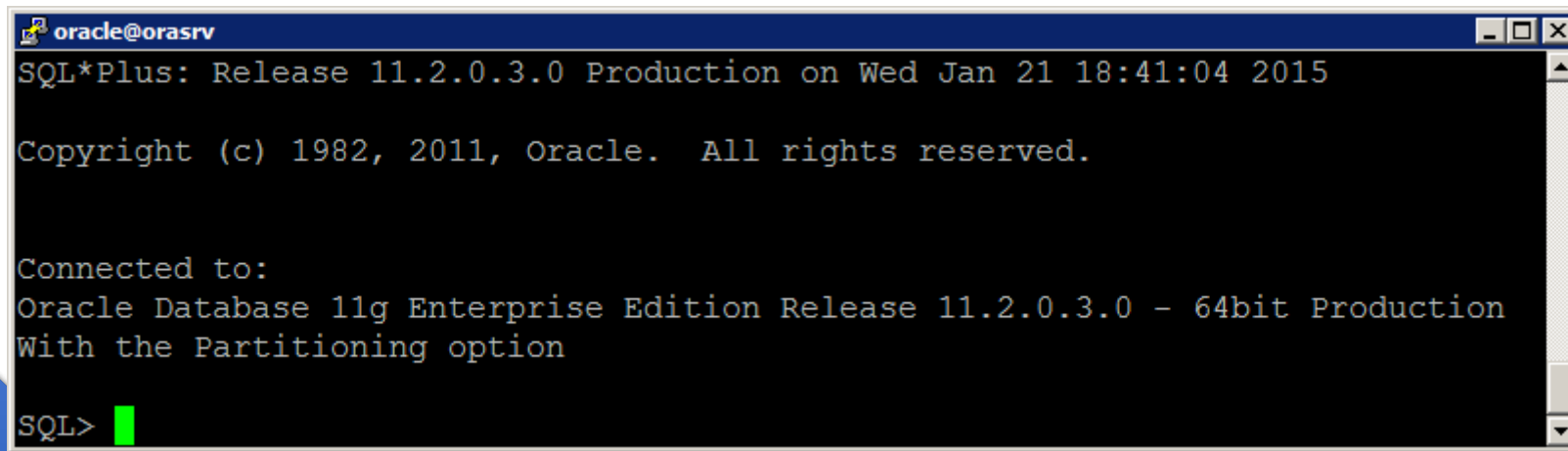
Or use

<https://nodistribute.com/>

# Know your shells

```
Microsoft Windows [Version 10.0.17133.1]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

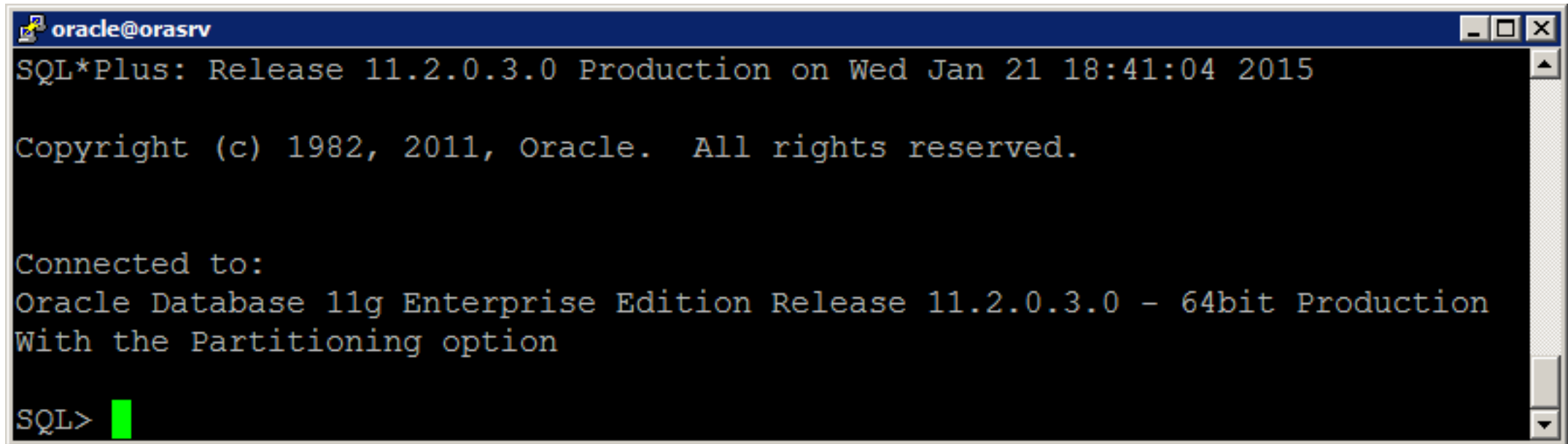
```
andy@Andys-Laptop:~$
```

A screenshot of a terminal window titled 'oracle@orasrv'. The window shows the output of the SQL\*Plus startup sequence. The text displayed is: 'SQL\*Plus: Release 11.2.0.3.0 Production on Wed Jan 21 18:41:04 2015', 'Copyright (c) 1982, 2011, Oracle. All rights reserved.', 'Connected to:', 'Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production', 'With the Partitioning option', and 'SQL>' followed by a green cursor bar. The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

```
oracle@orasrv  
SQL*Plus: Release 11.2.0.3.0 Production on Wed Jan 21 18:41:04 2015  
  
Copyright (c) 1982, 2011, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production  
With the Partitioning option  
  
SQL> █
```

# Don't type **whoami** or **dir** here

- This is a database client – not a command prompt / shell!

A screenshot of a terminal window titled 'oracle@orasrv'. The window displays the SQL\*Plus startup sequence, including the release information (11.2.0.3.0 Production), copyright notice, and connection details to an Oracle Database 11g Enterprise Edition. The prompt 'SQL>' is visible at the bottom with a green cursor.

```
oracle@orasrv
SQL*Plus: Release 11.2.0.3.0 Production on Wed Jan 21 18:41:04 2015

Copyright (c) 1982, 2011, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning option

SQL>
```



# Reporting



<https://www.flickr.com/photos/orleepasion/9048154451>



©2018 Netscylla



# Reporting

Obvious reasons why reporting is important....

- did you record suitable evidence
- is it date-time stamped!
- may get challenged on timeline / collaborate blue team logs
- stuff may get patched during engagement, cant go back
- Be prepared for 2-4 weeks reporting unless your making brilliant notes as you go along.
- **Not your standard pentest report!** Next Slide...



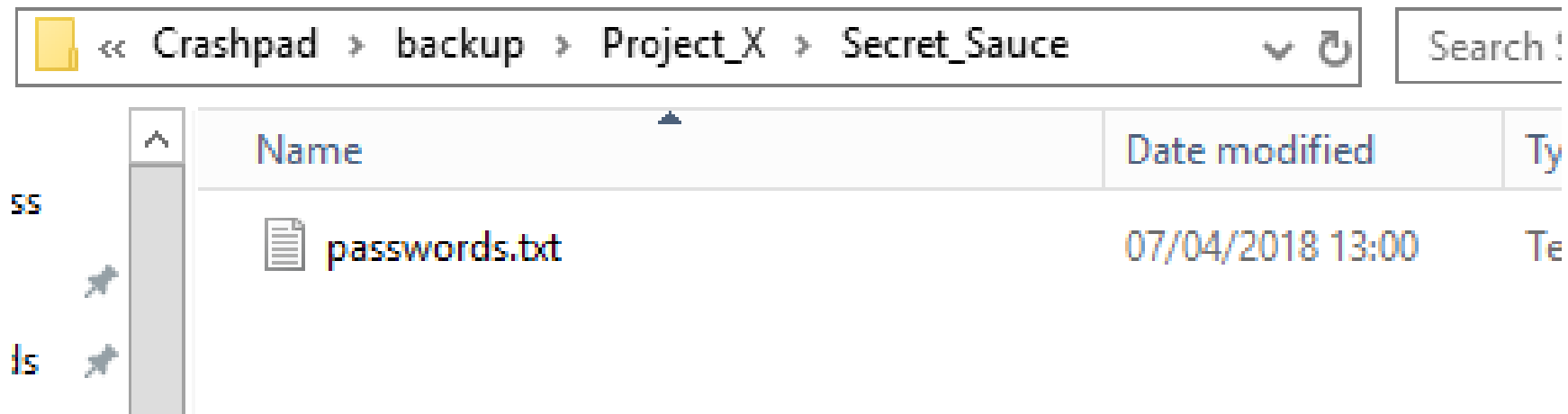
# Reporting

- People, Processes, Technology
- Tactical and Strategical recommendations
- Level of Skill employed: Scr1p7 K1dd13 -> 1ee7 Hax0r / Admin
- Lockheed Martin Cyber Kill Chain™
- Diamond Model – Use full for modelling your kill chains

<http://www.activeresponse.org/the-diamond-model/>

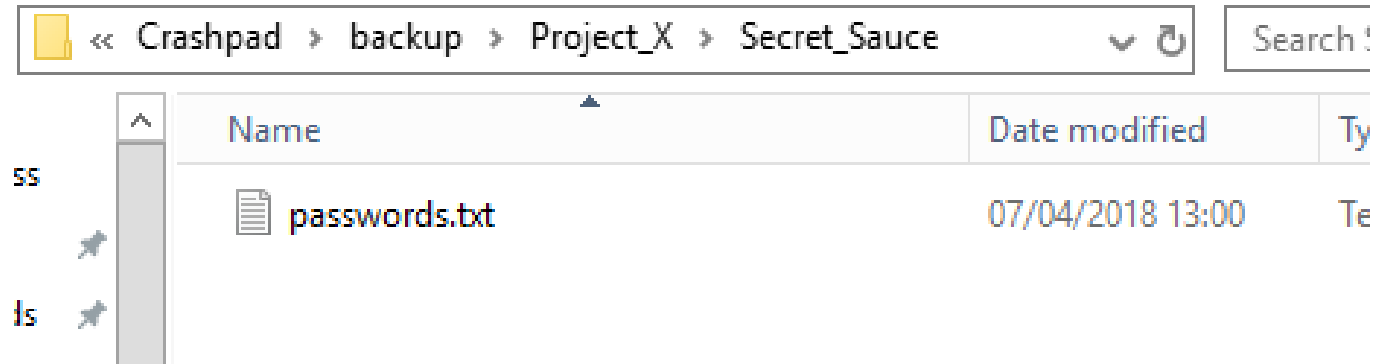
# Reporting

Obvious reasons why reporting is important....



# Reporting

Obvious reasons why reporting is important....



What network folder did you find this file in???

You can bet it won't be there when it comes to retesting.

**FULL PATHS – ALWAYS DOCUMENT FULL PATHS!!!**

# Reporting – Console Cheat sheet

## Windows CMD

```
prompt $D$$T$$P$G
```

Becomes

```
[Date] [Time] [Drive & Path]>
```

## Bash shell

```
export PS1='[\u@\h \W] \D{%F %T}\n\$_ '
```

# Reporting – Console Cheat sheet

## Metasploit

- Change PROMPT

```
msf> setg PROMPT %T msf
PROMPT => %T msf
2015-06-12 00:11:54 +0100 msf> save
Saved configuration to: /home/<user>/.msf4/config
2015-06-12 00:11:57 +0100 msf>
```

- Log to specific file

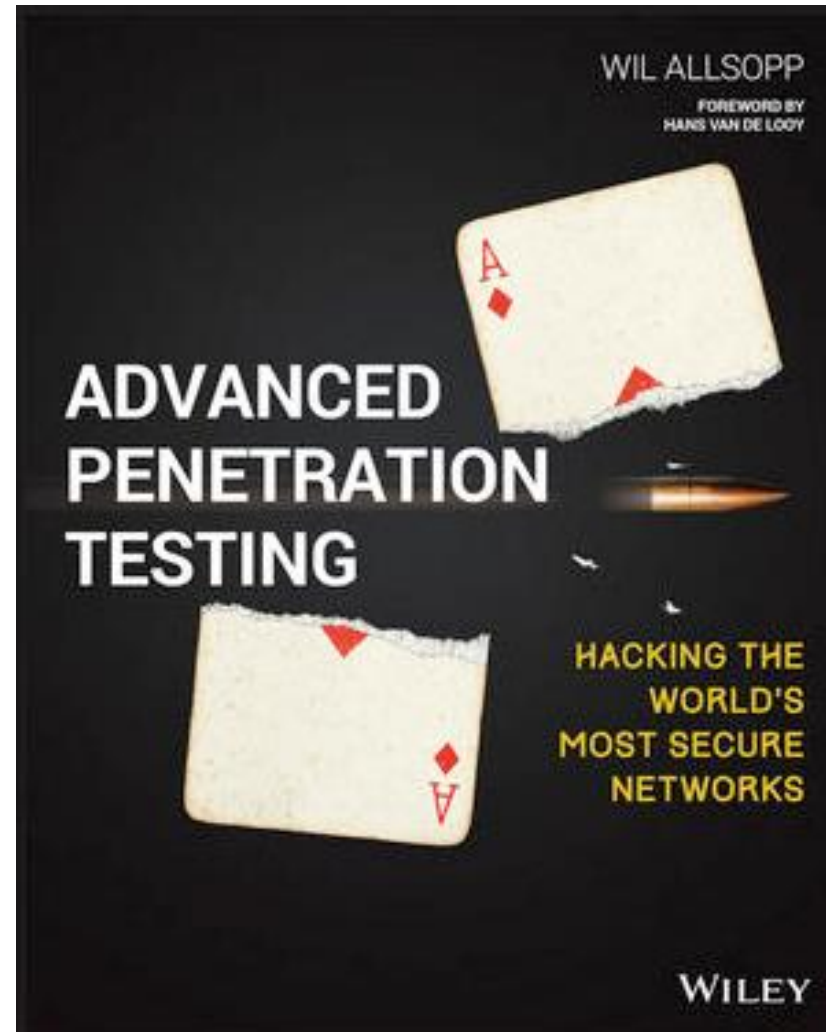
```
Msf> spool /root/msf_console.log
```



Lastly

So you want a quick tip on red teaming...

# Most Plays Come From This...





# Extra Time – Some Bad Mistakes



[https://cdn.pixabay.com/photo/2017/08/13/05/08/deadline-stopwatch-2636259\\_960\\_720.jpg](https://cdn.pixabay.com/photo/2017/08/13/05/08/deadline-stopwatch-2636259_960_720.jpg)

# Extra Time – Not Safe for Work

- nsa mac address
- pineapple mac addresses
- set hostname to pineapple/kali/pwned
- hack the blue team workstation of the staff member changing passwords, reset passwords after hes logged out, or moved to another server
- add your laptop/hackbox as a domain controller on the network, let it sync, unplug and walk away....
- insert filter dll, and reboot dc, watch passwords get sent in clear text to a http server you control
- Start brute-forcing all user accounts
- unlock all locked accounts, to mask the fact you just DoSed/locked 5000+ user accounts
- change everyone's (not entire company - just blue team ad group) desktop wallpaper to french/italian black cockrel
- change CEOs townhall/meeting/AGM speech thanking the red-team



# FIN



<https://health.mil/~media/Images/MHS/Photos/acoustics.ashx?h=428&la=en&mw=720&w=720>



©2018 Netscylla