

Left of Boom: Three Basic Skills to Practice before a Cyber Incident

BE Rhodes

Roles: Industry/Military-Veteran/Academia

October 2021

Outline

WHOIS & Where to begin?

What do you see?

The Three Basic Skills

Logs: Everybody has them

Networks: Everybody uses them

Assets: Everybody forgets about them

Conclusion & Questions

WHOIS: Brad Rhodes

- WHOIS: Brad Rhodes
- TLDR:
 - ✓ Head of Cybersecurity at zvelo
 - ✓ COL, Cyber (17A), 76th Operational Response Command G6/CIO
 - ✓ Military Cyber Professionals Association, HammerCon Co-Lead
 - ✓ Speaker, Author, Professor, Coach
 - ✓ #toomany Pro-Certs, highlights: CISSP-ISSEP, CISM, CDPSE, PMP, CEH, GMON, GCIH, Cloud+, CySA+

Feel to view/listen/grab my previous presentation/articles here:

<https://github.com/cyberguy514>

Note: images used are Copyright/Trademark of the owning organization.

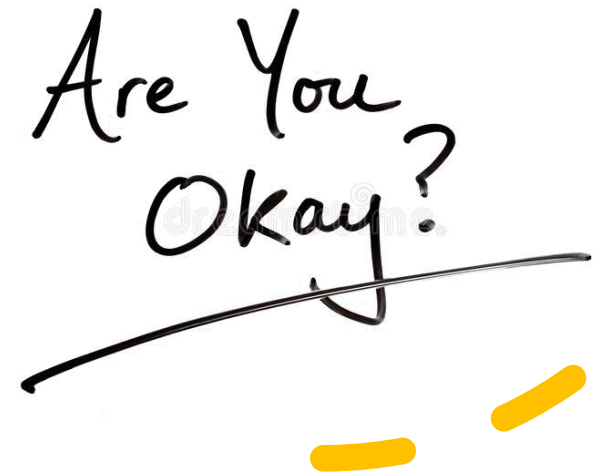
zvelo



Where to
begin?

- The last 18+ months have been nuts!
 - A global pandemic
 - Lockdowns & restrictions
 - Massive shift to work from home / remote work
 - Emboldened malicious cyber actors (MCA)
 - Medicine and vaccine scams
 - Misinformation on just about everything
 - US Presidential election
 - US Capitol attack
 - Afghanistan withdrawal

Are You
Okay?





A P T
ADVANCED PERSISTENT THREAT



What do you
see?

The Three Basic Skills



Logs [Logging & Analysis]

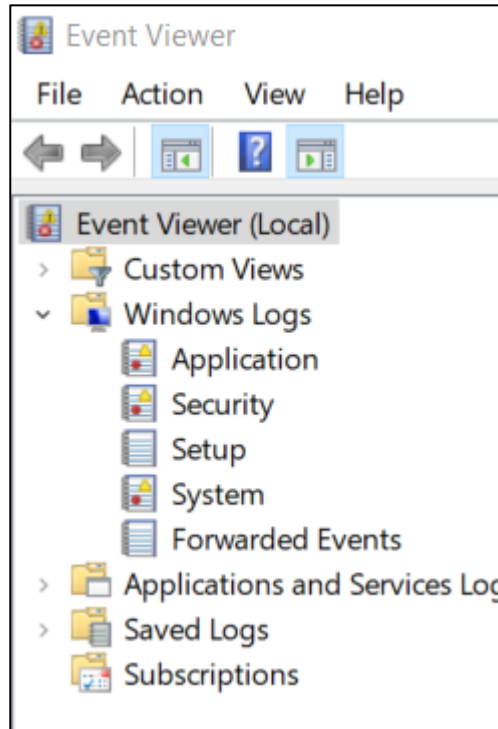


Networks [Traffic Analysis]

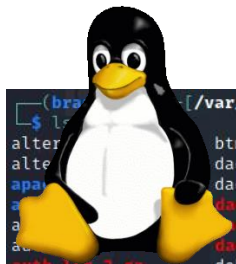
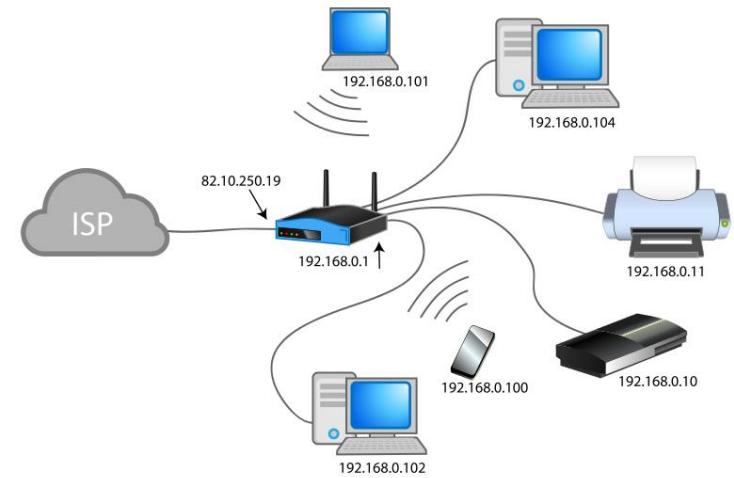


Assets [Discovery & Management]

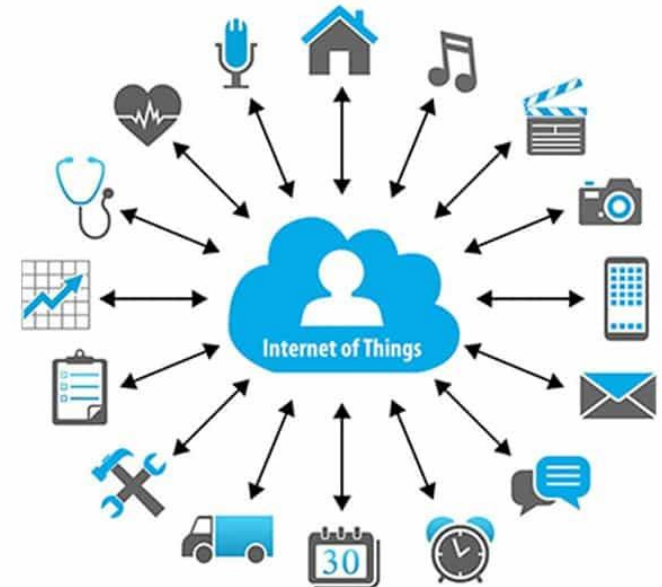
Logs: Where to find them



```
berhodes@brads-mbp log % ls
Bluetooth
CoreDuet
DiagnosticMessages
Tunnelblick
apache2
asl
com.apple.wifivelocity
com.apple.xpc.launchd
cups
daily.out
displaypolicy
displaypolicyd.stdout.log
dm
emond
fsck_apfs.log
fsck_apfs_error.log
fsck_hfs.log
install.log
mDNSResponder
monthly.out
powermanagement
ppp
shutdown_monitor.log
system.log
system.log.0.gz
system.log.1.gz
uucp
vnetlib
weekly.out
wifi-10-10-2021_10:41:52.931.log
wifi-10-10-2021_10:42:09.302.log
wifi-10-14-2021_08:28:10.298.log
wifi.log
wifi.log.0.bz2
wifi.log.1.bz2
wifi.log.10.bz2
wifi.log.2.bz2
wifi.log.3.bz2
wifi.log.4.bz2
wifi.log.5.bz2
wifi.log.6.bz2
wifi.log.7.bz2
wifi.log.8.bz2
wifi.log.9.bz2
```



```
(brads-mbp) [~/var/log]
$ ls
alter.log
alter.log.2.gz
alter.log.3.gz
alter.log.4.gz
auth.log
auth.log.2.gz
auth.log.3.gz
auth.log.4.gz
boot.log
bootstrap.log
btmtp
btmtp.1
daemon.log
daemon.log.1
daemon.log.2.gz
daemon.log.3.gz
daemon.log.4.gz
debug
debug.1
debug.2.gz
debug.3.gz
debug.4.gz
dpkg.log
dpkg.log.1
dpkg.log.2.gz
dpkg.log.3.gz
faillog
fontconfig.log
inetsim
installer
journal
kern.log
kern.log.1
kern.log.2.gz
kern.log.3.gz
kern.log.4.gz
kern.log.4.gz
lastlog
lightdm
macchanger.log.1.gz
macchanger.log.2.gz
macchanger.log.3.gz
macchanger.log.4.gz
messages
messages.1
messages.2.gz
messages.3.gz
messages.4.gz
mysql
nginx
nttpstats
openvpn
postgresql
private
runit
samba
stunnel4
syslog
syslog.1
syslog.2.gz
syslog.3.gz
syslog.4.gz
syslog.6.gz
syslog.7.gz
sysstat
user.log
user.log.1
user.log.2.gz
user.log.3.gz
user.log.4.gz
vmware-network.1.log
vmware-network.2.log
vmware-network.3.log
vmware-network.4.log
vmware-network.5.log
vmware-network.6.log
vmware-network.7.log
vmware-network.8.log
vmware-network.9.log
vmware-network.log
vmware-vmsvc-root.1.log
vmware-vmsvc-root.2.log
vmware-vmsvc-root.3.log
vmware-vmsvc-root.log
vmware-vmtoolsd-root.log
wtmp
Xorg.0.log
Xorg.0.log.old
Xorg.1.log
Xorg.1.log.old
```





Logs: Turning on logging or expanding logging

CONFIGURE:

1. **SYSTEM AUDIT POLICIES:** In order to capture what you want and need the following **Advanced Audit Policies** must be set. You may expand these to your specific needs, but here is a place to start.

List out the System audit policy

- **Command:** AuditPol /get /category:*

Category/Subcategory	Setting
Account Logon	
• Credential Validation	Success and Failure
• Kerberos Authentication Service	No Auditing (WA)
• Kerberos Service Ticket Oper	No Auditing (WA)
• Other Account Logon Events	Success and Failure
Account Management	
• Application Group Management	Success and Failure
• Computer Account Management	Success and Failure
• Distribution Group Management	Success and Failure
• Other Acct Management Events	Success and Failure
• Security Group Management	Success and Failure
• User Account Management	Success and Failure
Detailed Tracking	
• DPAPI Activity	No Auditing
• Plug and Play (10/2016)	Success
• Process Creation	Success and Failure
• Process Termination	No Auditing (WA)
• RPC Events	Success and Failure
• Audit Token Right Adj (10/2016)	Success (N)
DS Access	
• Detailed Directory Service Repl	No Auditing
• Directory Service Access	No Auditing (WA)
• Directory Service Changes	Success and Failure
• Directory Service Replication	No Auditing (WA)
Logon/Logoff	
• Account Lockout	Success (WA)
• Group Membership (10/2016)	Success
• IPsec Extended Mode	No Auditing
• IPsec Main Mode	No Auditing
• IPsec Quick Mode	No Auditing
• Logoff	Success
• Logon	Success and Failure
• Network Policy Server	Success and Failure
• Other Logon/Logoff Events	Success and Failure
• Special Logon	Success and Failure
• User / Device Claims	No Auditing

CONFIGURE:

SYSTEM AUDIT POLICIES: Continued

To set an item:

- Auditpol /set /category:"Account Management" /success:enable /failure:enable

To set a subcategory individually:

- Auditpol /set /subcategory:"Directory Service Access" /success:disable /failure:disable

Category/Subcategory	Setting
Object Access	
• Application Generated	Success and Failure
• Certification Services	Success and Failure
• Central Policy Staging (8/2012)	No Auditing
• Detailed File Share	Success
• File Share	Success and Failure
• File System	Success
• Filtering Platform Connection	Success (N) (WA)
• Filtering Platform Packet Drop	No Auditing (WA)
• Handle Manipulation	No Auditing (N)(WA)
• Kernel Object	No Auditing (WA)
• Other Object Access Events	No Auditing (WA)
• Removable Storage	Success and Failure
• Registry	Success
• SAM	Success
Policy Change	
• Audit Policy Change	Success and Failure
• Authentication Policy Change	Success and Failure
• Authorization Policy Change	Success and Failure
• Filtering Platform Policy Change	Success (Win FW)
• MPSSVC Rule-Level Policy Change	No Auditing
• Other Policy Change Events	No Auditing (WA)
Privilege Use	
• Non Sensitive Privilege Use	No Auditing
• Other Privilege Use Events	No Auditing
• Sensitive Privilege Use	Success and Failure
System	
• IPsec Driver	Success (WA)
• Other System Events	Failure (WA)
• Security State Change	Success and Failure
• Security System Extension	Success and Failure
• System Integrity	Success and Failure
<i>Global Object Access Auditing – ignore</i>	

Priorities / Severities

0	emerg	system is unusable
1	alert	action must be taken immediately
2	crit	critical conditions
3	err	error conditions
4	warning	warning conditions
5	notice	normal, but significant, cond
6	info	informational message
7	debug	debug-level message



from:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

to:

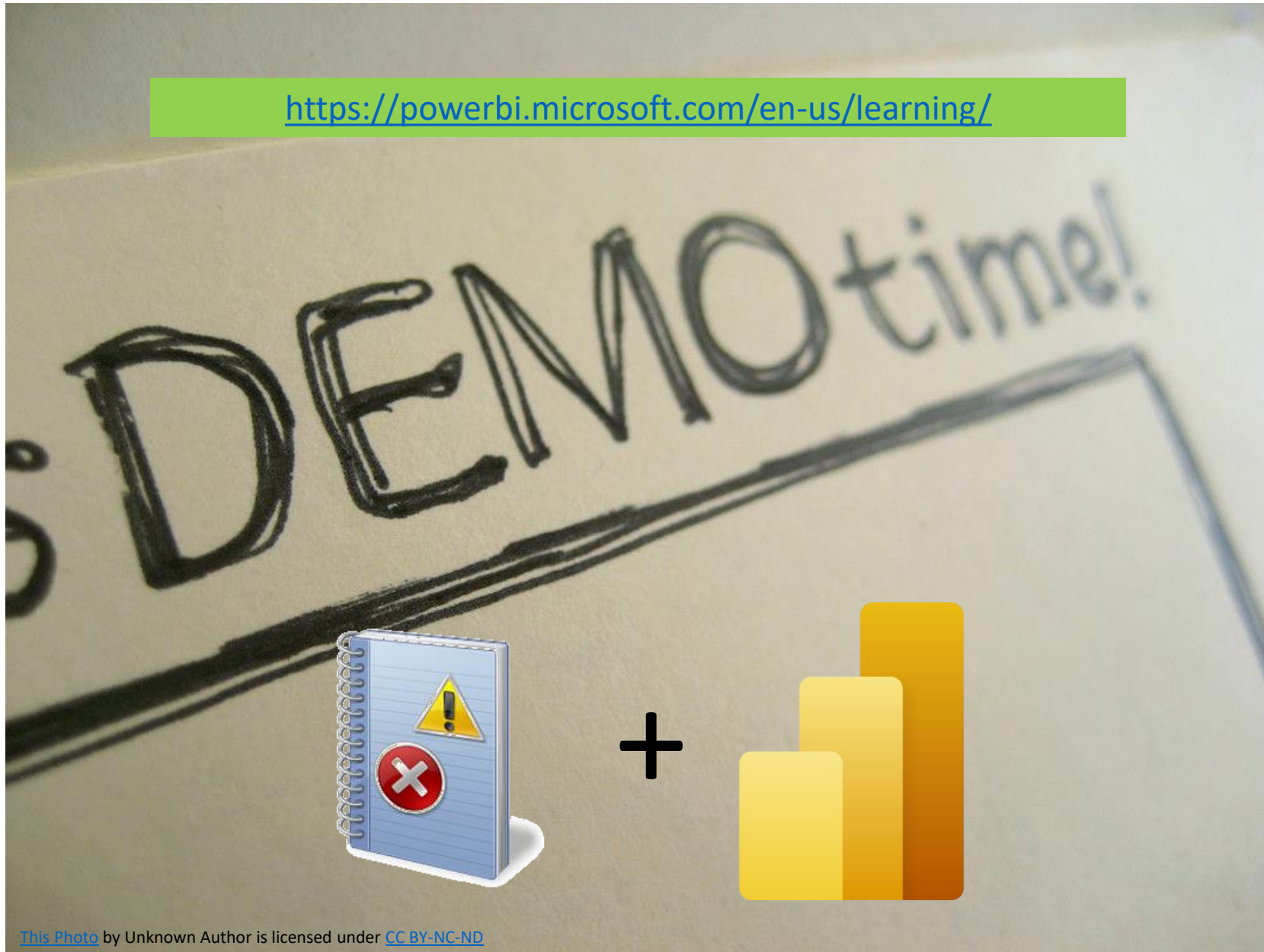
```
*.debug;mail.none;authpriv.none;cron.none /var/log/messages
```

<https://www.malwarearchaeology.com/cheat-sheets>

```
# Some "catch-all" log files.
#
*==debug;\
    auth,authpriv.none;\
    mail.none                -/var/log/debug
*==info;*==notice;*==warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail.none                 -/var/log/messages
```


Logs: Windows log analysis – the easy way

<https://powerbi.microsoft.com/en-us/learning/>



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

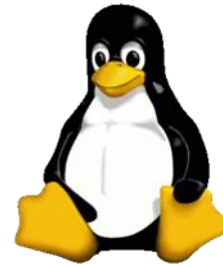
Networks: Where to observe networks



```
C:\Users\bradr>netstat -ant
```

Active Connections

Proto	Local Address	Foreign Address	State	Offload State
TCP	192.168.86.47:1024	162.159.136.234:443	ESTABLISHED	InHost
TCP	192.168.86.47:1025	52.245.128.79:443	ESTABLISHED	InHost
TCP	192.168.86.47:1026	143.204.25.78:443	ESTABLISHED	InHost
TCP	192.168.86.47:1028	40.83.247.108:443	ESTABLISHED	InHost
TCP	192.168.86.47:1030	100.25.227.114:443	ESTABLISHED	InHost
TCP	192.168.86.47:1031	40.66.31.98:443	ESTABLISHED	InHost



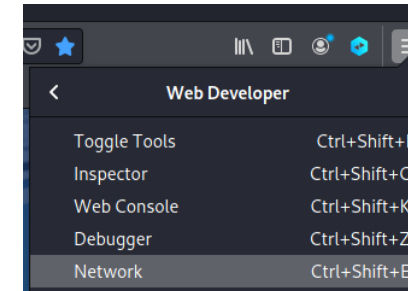
```
$ sudo netstat -antp
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	192.168.221.136:37628	35.201.96.133:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:55292	104.96.221.65:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:47424	173.223.192.244:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:55362	104.96.221.58:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:46280	35.155.1.44:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:45170	104.16.18.94:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:55210	104.104.91.27:80	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:34938	65.8.233.2:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:48742	65.8.233.40:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:40746	104.16.149.64:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:57030	23.56.9.127:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:50292	34.208.48.90:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:47762	104.96.237.38:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:51322	151.101.184.157:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:37378	35.201.96.133:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:59610	104.18.252.222:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:51424	104.96.221.67:443	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:55208	142.250.72.35:80	ESTABLISHED	2334/x-www-browser
tcp	0	0	192.168.221.136:34802	143.204.25.146:80	ESTABLISHED	2334/x-www-browser

Resource Monitor

TCP Connections					
Image	PID	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	2044	192.168.86.47	5145	40.66.25.130	443
chrome.exe	2044	192.168.86.47	1234	40.66.31.98	443
chrome.exe	2044	192.168.86.47	1031	40.66.31.98	443
CoreSync.exe	17724	192.168.86.47	13307	18.235.195.121	443
CoreSync.exe	17724	192.168.86.47	1030	100.25.227.114	443
Discord.exe	13012	192.168.86.47	1056	162.159.137.232	443
Discord.exe	13500	192.168.86.47	1024	162.159.136.234	443



Status	Method	Domain	File
301	GET	thehackernews.com	/
200	GET	thehackernews.com	/
	GET	thehackernews.com	roboto.css
	GET	cdn.doubleverify.com	dvbs_src.js?ctx=607671&cmp=24935727&
200	GET	thehackernews.com	rocket-loader.min.js
200	GET	thehackernews.com	thn.png
200	GET	thehackernews.com	favicon.ico
200	GET	cdnjs.cloudflare.com	jquery.min.js
	GET	www.google-analytics.com	analytics.js

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

Networks: How to capture network traffic



Data Collection - Architecture



Placement of the tap/sensor is key!

Monitoring computer NIC must be in promiscuous mode!

Don't forget that a Full Packet Capture will generate a TON of data!!

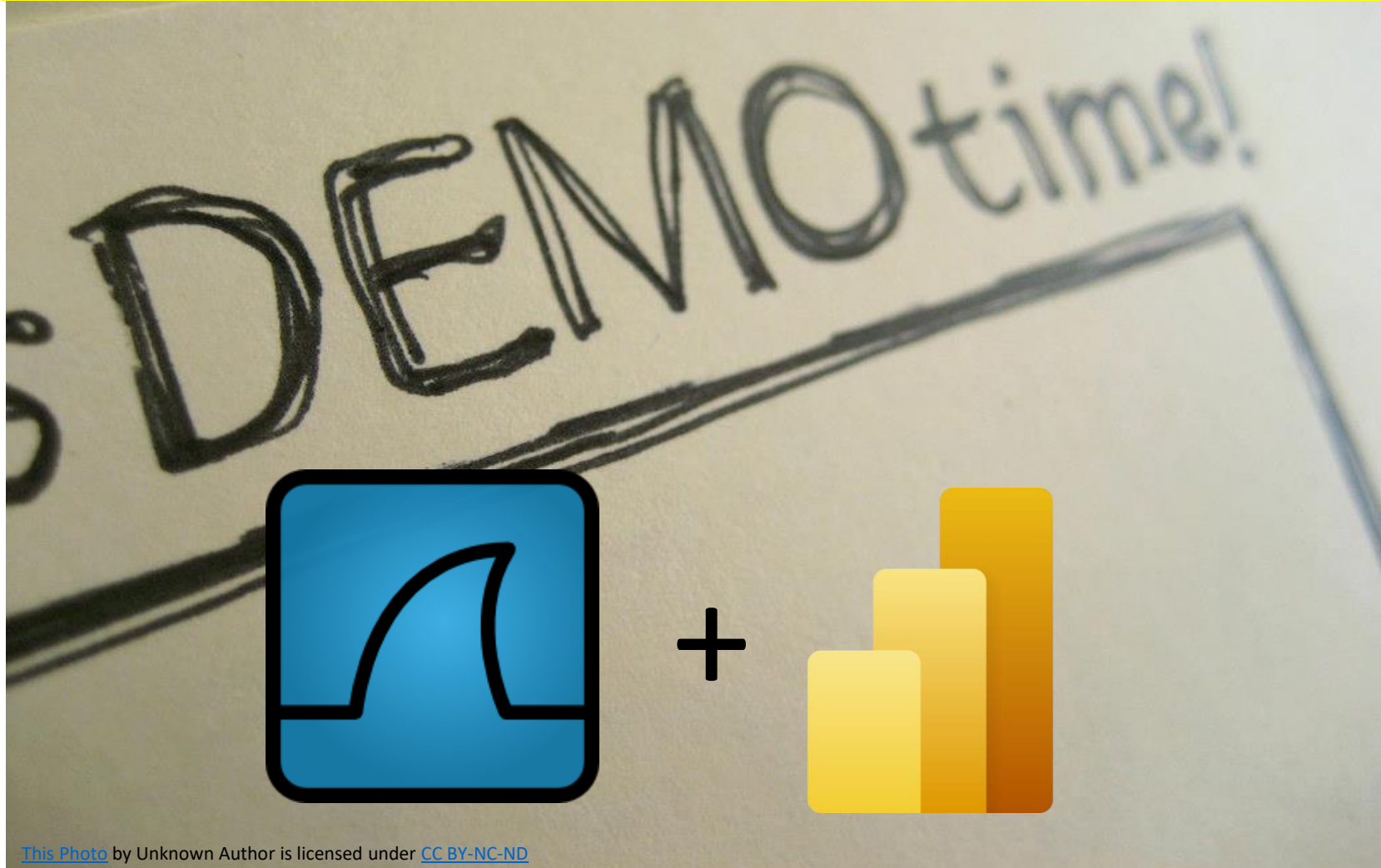
	capture_5-22-2020_42min.pcap	Wireshark capture ...	9,303,566 KB
	homenet_5-22-2020_42min.csv	Microsoft Excel Co...	2,774,413 KB

Networks: Analyzing network traffic

<https://www.wireshark.org/#learnWS>

Deep Dive into Wireshark Class:

<https://www.youtube.com/playlist?list=PLBNtagSCmDWyUcCsdq7m5ljKYDyTNG9R1>



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

Assets: Defined (hint, not just hardware)



Data



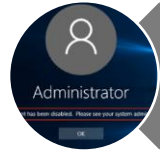
Endpoints



Networking (Gear)



Code / Repos



Admin Accounts



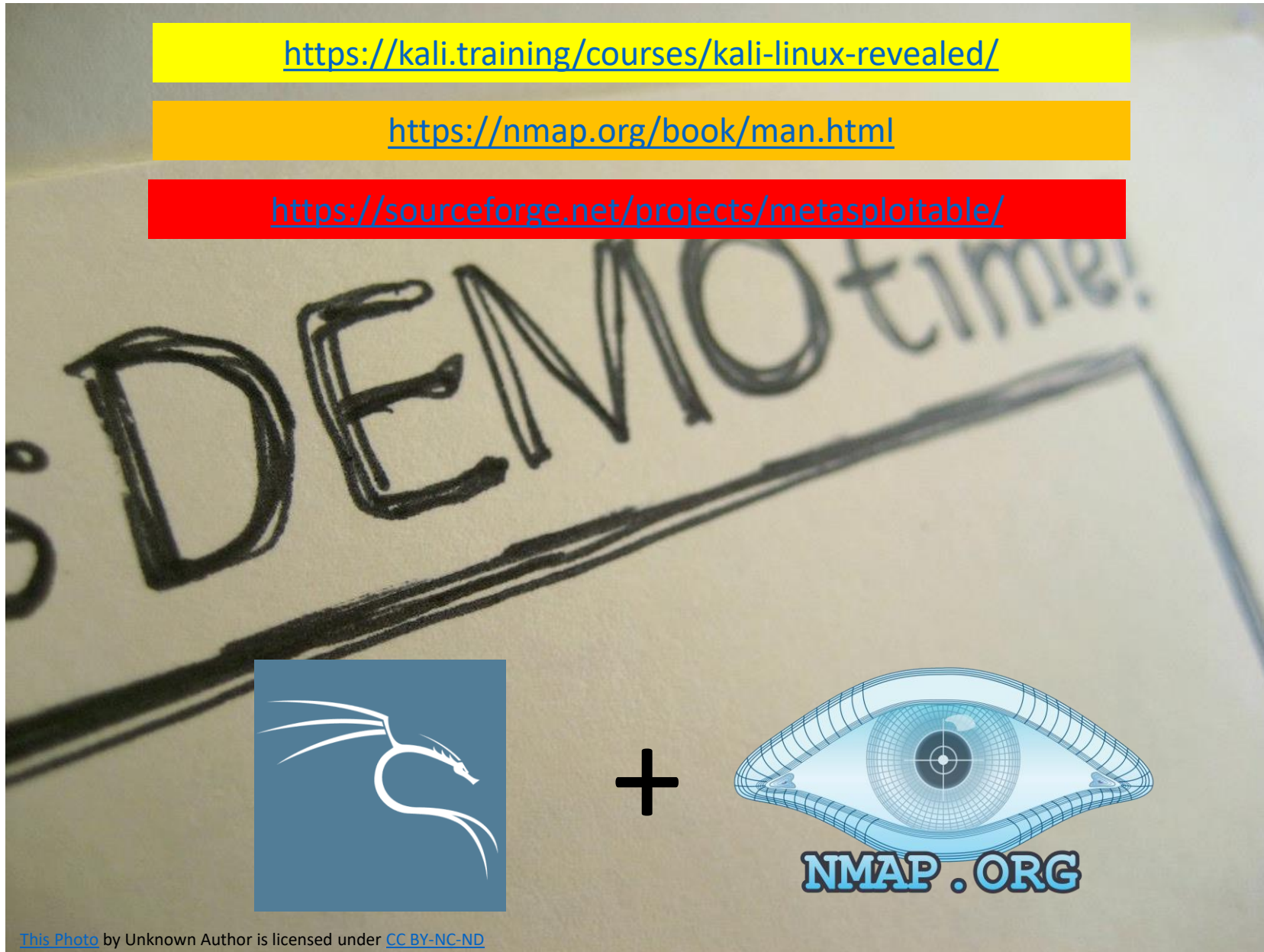
Exposed (Internet-Facing)

Assets: Internal assets

<https://kali.training/courses/kali-linux-revealed/>

<https://nmap.org/book/man.html>

<https://sourceforge.net/projects/metasploitable/>



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

Assets: External assets

<https://www.shodan.io/>



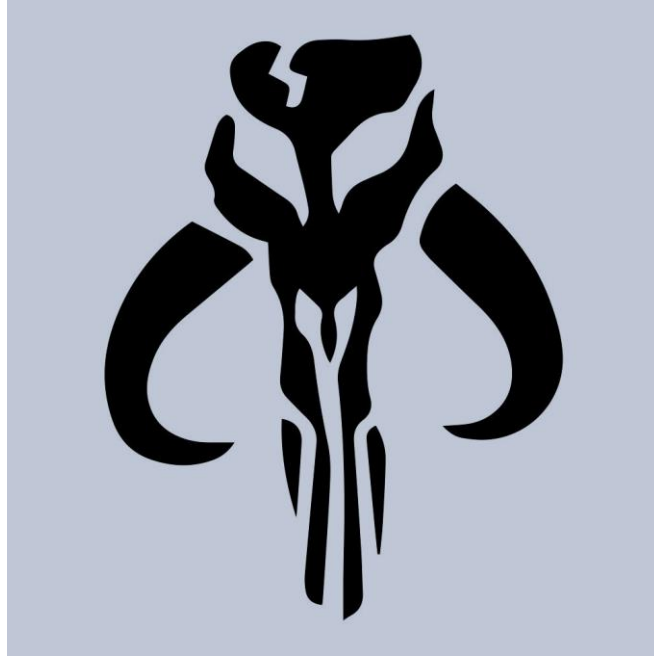
[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

Public Service Announcement: Intent

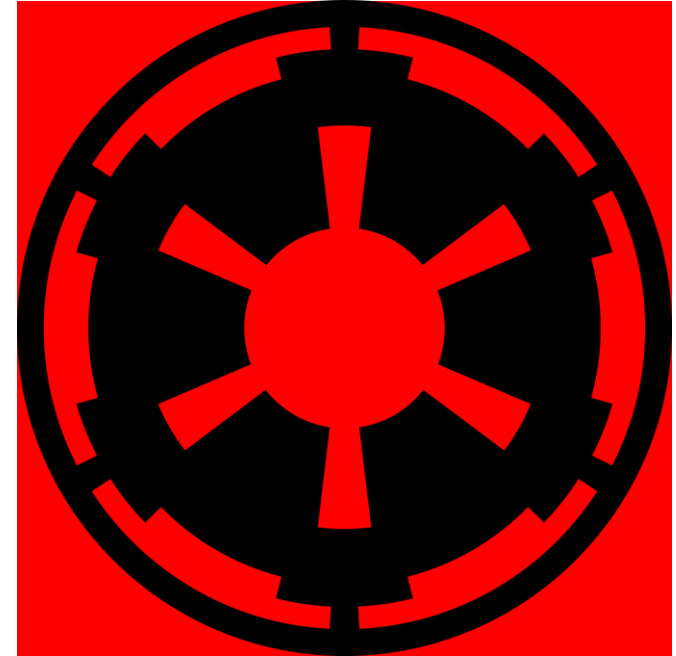
Blue Space (Good)



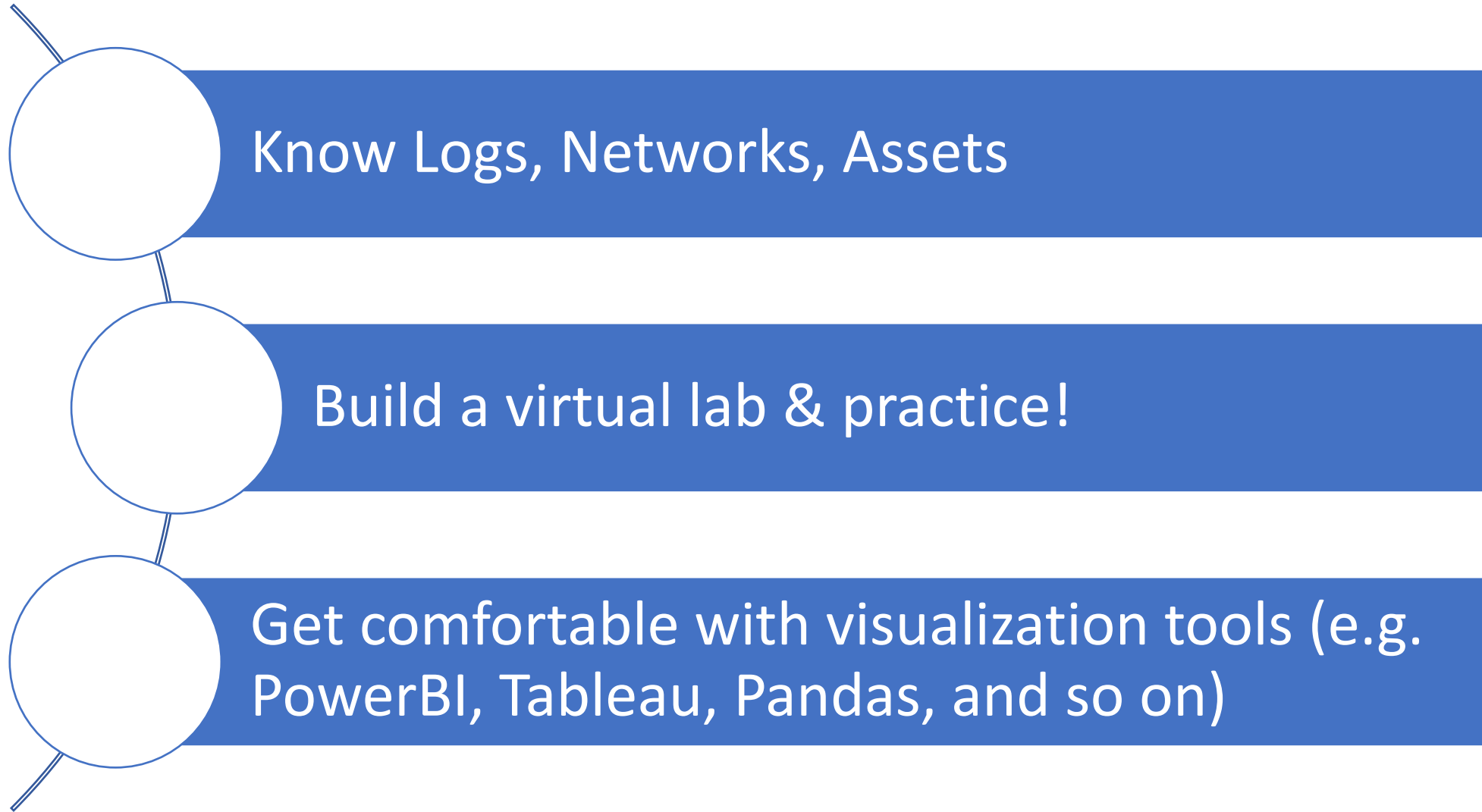
Gray Space (Internet)



Red Space (Bad)



Conclusions



Thank you, VetSecCon!

For the honor and privilege of this speaking opportunity!

Questions?



Presentation(s) on GitHub:
<https://github.com/cyberguy514/presentations>

Contact Details:

Civilian: brhodes@zvelo.com

Military: brad.e.rhodes.mil@army.mil

MCPA: brad.rhodes@milcyber.org

LinkedIn: <https://www.linkedin.com/in/brad-rhodes-1951ba7/>

Twitter: [@cyber514](https://twitter.com/cyber514)