

Mason Competitive Cyber

What gameplan?



The Announcement Slides



1. NCL Codes still available! Highly recommended for anyone trying to get their foot in the door with cyber stuff. DM Garrett Heckman for a code.
2. UMDCTF April 16-18 online. Unlimited size team. #umdctf2021
3. MasonCC elections! (Go vote and don't hack the election).

So, we did pretty good



Qualifying Round Final Standings

1. George Mason University
2. University of Maryland Baltimore County (Team 1)
3. Liberty University
4. University of Pittsburgh
5. Old Dominion University
6. Millersville University
7. Northern Virginia Community College
8. Capitol Technology University

Round 45

2021-02-27 16:44:35

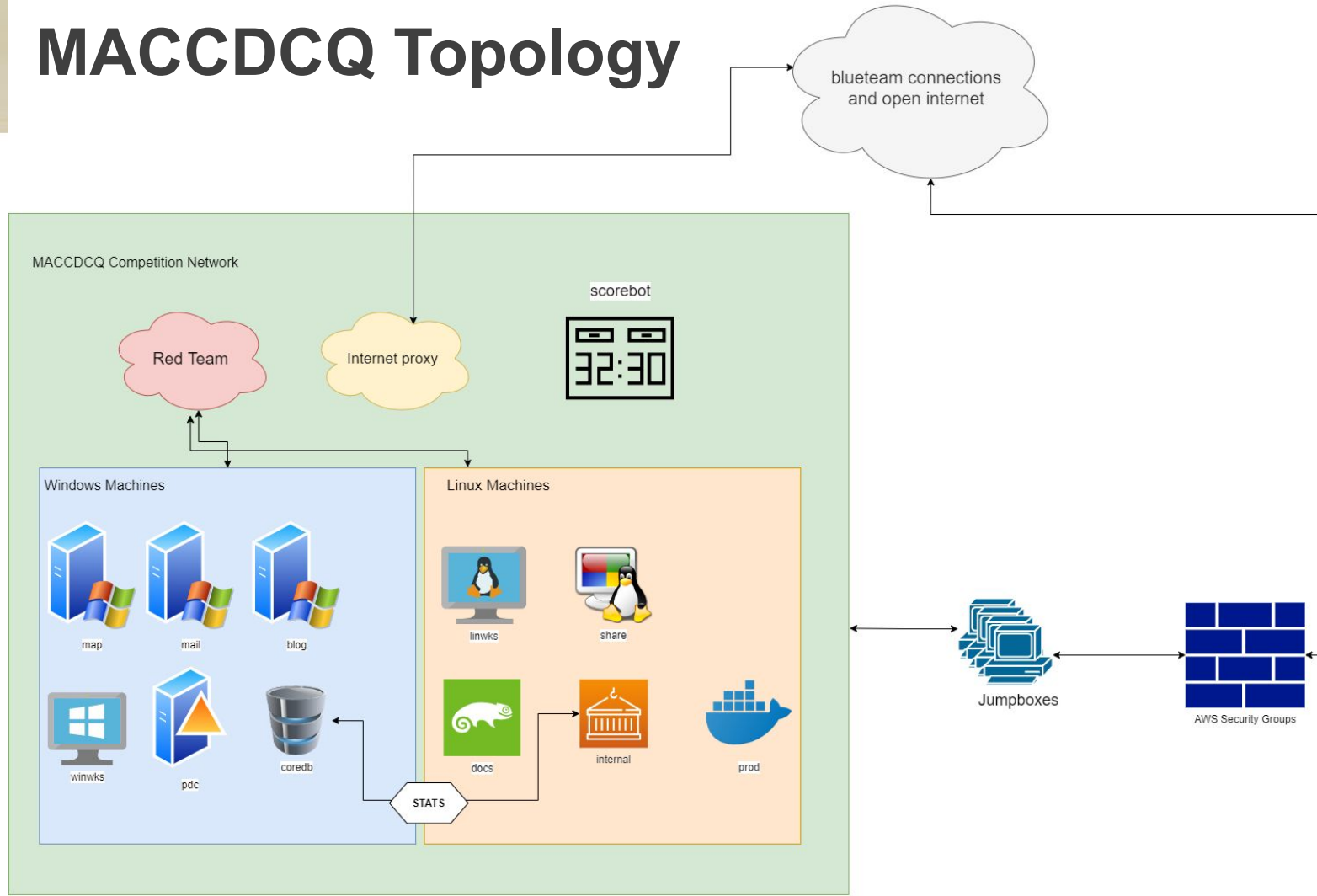
	team0	team1	team2	team3	team4	team5	team6	team7	team8	team9	team10	team11	team12	team13	team14	team15	team16	team17	team18	team19	team20	team21	team22	team23	team24	team25	team26
Current Score	175,500	114,290	90,270	56,630	112,750	96,920	137,540	108,310	103,010	64,620	111,370	109,580	129,030	119,590	116,480	91,950	74,830	89,370	98,670	129,880	94,350	123,720	109,720	96,680	100,720	119,440	174,700
Current Place	1🏆	10	23	27	11	19	3🏆	15	16	26	12	14	5	7	9	22	25	24	18	4	21	6	13	20	17	8	2🏆
Up/Down Ratio	30 / 0	13 / 17	15 / 15	9 / 21	14 / 16	11 / 19	22 / 8	11 / 19	4 / 26	2 / 28	12 / 18	14 / 16	11 / 19	9 / 21	11 / 19	10 / 20	25 / 5	10 / 20	17 / 13	20 / 10	8 / 22	14 / 16	8 / 22	15 / 15	9 / 21	14 / 16	29 / 1
PDC_SMB	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓
PDC_DNS	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
PDC_LDAP	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓
COREDB_POSTGRES	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓
COREDB_MYSQL	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✓
COREDB_SSH	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓
SHARE_NFS	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
SHARE_FTP	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓
SHARE_SSH	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✓	✗	✗	✓
LINWKS_SSH	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓
LINWKS_VNC	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
WINWKS_RDP	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓
WINWKS_SMB	✓	✓	✓	✗	✗	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✓	✗	✓	✓
MAIL_RDP	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✗	✓	✓	✗	✗	✓	✓
MAIL_SMB	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓	✓
MAP_HTTP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓
MAP_HTTPS	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓
MAP_SSH	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓
BLOG_HTTP	✓	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
BLOG_SMB	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✓	✓
INTERNAL_HTTP	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓
INTERNAL_SSH	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✓	✓	✗	✓
DOCS_HTTP	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗
DOCS_SSH	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
PROD_HTTP_CART	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓
PROD_HTTP_TICKET	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
PROD_HTTP_GIT	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
PROD_HTTP_FILE	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
PROD_DOCKER	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓
STATS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✗	✓

Scoring Points in CCDC



- Keep your services running
- Keep the Red Team suppressed
- Deliver Injects complete them on time

MACCDCQ Topology



Defending a flat network



- Assume the Red Team is everywhere, always
- No insights on border traffic or capability to block at the gateway
- Also, no single point of failure for the Red Team to attack

CCDC 2020 vs 2021



Hostname	IP Addr	OS	Score Services
judge	192.168.X.209	Win 2019	No Scored Service - NO local/jumpbox RDP access
pdcc	192.168.X.10	Win 2012 R2	445, 88, 53, 389
coredb	192.168.X.11	Win 2012 R2	5432, 3306, 22
share	192.168.X.12	RHEL 8	2049, 111, 21, 22
linwks	192.168.X.21	Ubuntu 18	22, 5901
winwks	192.168.X.22	Win 2016	3389, 445
mail	192.168.X.23	Win 2016	3389, 445
map	192.168.X.35	Win 2012 R2	80, 443, 22
blog	192.168.X.36	Win 2012 R2	80, 445
internal	192.168.X.37	Amazon Linux 2	80, 22
docs	192.168.X.80	SUSE 15	80, 22
prod	192.168.X.88	Ubuntu 20.04	8080, 8888, 80, 8081, 2375

Service Checks		
Team	Service Name	Last Check Status
Team 8	ad-dns	Passed
Team 8	bind-dns	Passed
Team 8	ecom-http	Passed
Team 8	mail-pop3	Passed
Team 8	mail-smtp	Passed
Team 8	phantom-https	Passed
Team 8	splunk-http	Passed

Windows



Total of 6 Windows machines to defend

PDC : 445 (SMB), 53 (DNS), 389 (LDAP)

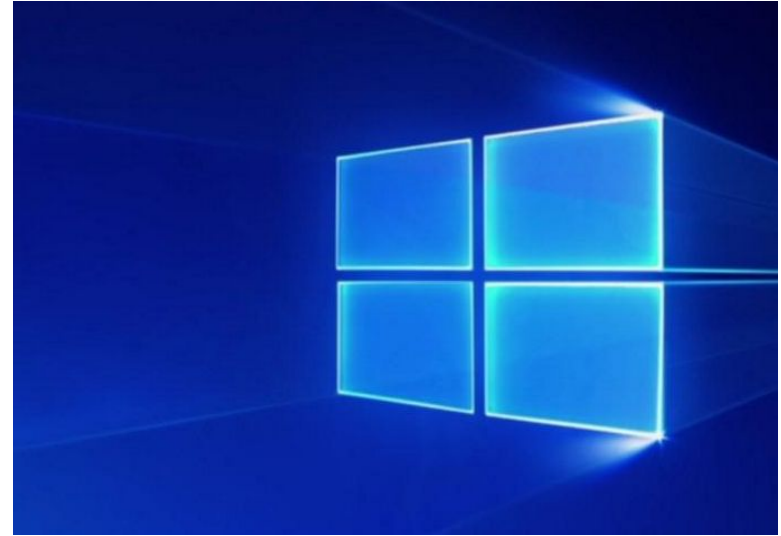
CoreDB: 5432 (Postgresql), 3306 (MySQL), 22 (SSH)

WinWks: 3389 (RDP), 445 (SMB)

Mail: 3389 (RDP), 445 (SMB)

Map: 80 (HTTP), 443 (HTTPS), 22 (SSH)

Blog: 80 (HTTP), 445 (SMB)



Windows - By the numbers



Red Team had around **14** attacker shells at once

- That is 14 more than what you want !!!

We killed over **100** attacker shells throughout the 6 machines

- Yes, we counted...

Discovered around **16** different malicious IPs (usually reflectors)

- IP blocking was not allowed though :(

Eventually, we made it impossible for Red Team to get back in

- But they won't stop!

Useful Windows Hunting Commands

Netstat -NATB - Identify processes that are making outbound connection (We should know all the connections going outbound)

Tasklist - view current running process

net user / net localgroup - Look at users and groups on the system

Reviewing windows event log to perform forensics. Not good enough to know that our machine is infected, but **how** it was infected.

TCP	192.168.1.4:51868	52.177.165.30:443	ESTABLISHED	5492
TCP	192.168.1.4:51884	18.211.133.65:443	ESTABLISHED	14576
TCP	192.168.1.4:51894	18.211.133.65:443	ESTABLISHED	14576
TCP	192.168.1.4:51896	18.211.133.65:443	ESTABLISHED	14576
TCP	192.168.1.4:51899	18.211.133.65:443	ESTABLISHED	14576
TCP	192.168.1.4:51904	18.211.133.65:443	ESTABLISHED	14576
TCP	192.168.1.4:52103	52.89.88.19:443	ESTABLISHED	11728
TCP	192.168.1.4:53320	104.154.127.121:4070	ESTABLISHED	10660
TCP	192.168.1.4:53327	35.186.224.47:443	ESTABLISHED	10660

System Idle Process	0 Services	0	8 K
System	4 Services	0	132 K
Registry	120 Services	0	58,000 K
smss.exe	476 Services	0	1,068 K
csrss.exe	684 Services	0	4,428 K
wininit.exe	792 Services	0	5,584 K
csrss.exe	800 Console	1	5,552 K
services.exe	864 Services	0	10,104 K
lsass.exe	884 Services	0	20,760 K
svchost.exe	1004 Services	0	3,028 K
svchost.exe	88 Services	0	33,392 K
WUDFHost.exe	424 Services	0	4,804 K
fontdrvhost.exe	516 Services	0	2,568 K
svchost.exe	1068 Services	0	16,908 K
svchost.exe	1120 Services	0	7,316 K
winlogon.exe	1192 Console	1	9,648 K

Windows Payloads



14
/ 70

14 engines detected this file

ce91a028a80ba99f83073b106c0fb04a112c1bca8a8aebf33f4c535f1521f7

304.50 KB
Size

2021-02-27 19:59:00 UTC
a moment ago

64bits assembly peexe

Community Score

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
AhriLab-V3	Malware/Win64.RL.Trojan.R360751	SecureAge APEX	Malicious
ClamAV	Win.Trojan.CobaltStrike-9044898-1	Cybereason	Malicious.3625ed
Cynet	Malicious (score: 100)	Elastic	Malicious (high Confidence)
ESET-NOD32	A Variant Of Win64/RiskWare.CobaltStrike...	FireEye	Generic.mg.b7ef3c5aad68a
Kaspersky	HEUR:Trojan.Win32.Cobalt.vho	Malwarebytes	RiskWare.GameHack.CSGO
Microsoft	Backdoor:Win32/CobaltStrike.lldha	Sangfor Engine Zero	Trojan.Win32.Save.a
Sophos	MLPE-A + ATK/Cobalt-A	ZoneAlarm by Check Point	HEUR:Trojan.Win32.Cobalt.vho

12
/ 70

12 engines detected this file

e25382d1a7b8a7e3a37c1f75b0664339d22c8a67ad2cdf4612dfdddbeb61c60d

484.17 KB
Size

2021-02-27 18:45:30 UTC
a moment ago

64bits assembly invalid-signature overlay peexe signed

Community Score

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Antiy-AVL	RiskWare/Win64.Artifact	Avast	Win64/Malware-gen
AVG	Win64/Malware-gen	ClamAV	Win.Trojan.CobaltStrike-9044898-1
eGambit	PE.Heur.InvalidSig	Elastic	Malicious (high Confidence)
ESET-NOD32	A Variant Of Win64/RiskWare.CobaltStrike...	FireEye	Generic.mg.9bee3189ad7b9cb2
Jiangmin	Trojan.Cobalt.lhb	Malwarebytes	Malware.AI.2733391215
Microsoft	Backdoor:Win32/CobaltStrike.lldha	Sophos	ATK/Cobalt-A

3124 8.62 MB NT AUTHORITY\SYSTEM Description of my application

Name	Date modified	Type	Size
bfsvc	8/22/2013 ...	Application	56 KB
bootstat.dat	2/27/2021 ...	DAT File	66 KB
DPINST	9/9/2020 3...	Text Document	556 KB
Dtclninstall	2/27/2021 ...	Text Document	88 KB
EC2Provision	2/27/2021 ...	Application	306 KB
explorer	2/10/2021 ...	Application	2,693 KB
HelpPane	6/2/2017 1...	Application	979 KB
hh	10/29/201...	Application	17 KB
mib.bin	8/22/2013 ...	BIN File	43 KB
PFR0	2/27/2021 ...	Text Document	2,997 KB
regedit	10/29/201...	Application	151 KB
ServerStandard	8/22/2013 ...	XML Document	28 KB
ServerWeb	8/22/2013 ...	XML Document	27 KB
setupact	2/27/2021 ...	Text Document	54 KB
setuperr	8/22/2013 ...	Text Document	0 KB

Total of 5 machines to defend

1. **internal**
 - a. **AWS Linux - two containerized webserver, running STATS service**
2. **prod**
 - a. **Ubuntu 20.04 with Docker - five containerized services**
3. **share**
 - a. **Red Hat 8 - nfs, ftp, ssh**
4. **docs**
 - a. **openSUSE 15 - a web server and ssh**
5. **linwks**
 - a. **Ubuntu 18.04 - ssh and vnc**

Hunting the RedTeam on linux



- Capturing and reverse engineering malware
- Disabling user logins and removing private keys
 - `usermod -s /bin/false [username]`
`ls -lahR | grep authorized`
- Maintaining situational awareness
 - `ps -fawwwwwx`
`w`
`netstat -ntep`
`netstat -nuep`
`netstat -lpeanut`
`ufw status`

```
#!/bin/bash

aws_pollinate_key="ssh-rsa\ AAAAB3NzaC1y

time_stomp() {
    if [ -z $2 ];
    then
        source_file="/bin/bash"
    else
        source_file=$2
    fi
    touch -r $source_file $1
}
```

Keeping your services running



- More of an art than a science
- In a typical environment, you would just take your systems offline and scrub them if under attack

like this
- Lots of docker-fu needed for the containerized services
- Make sure you know what's on the page your webserver is serving ;)
- Make sure that the scorebot is checking the right username/password

Injects



1. Acknowledgement of rules and receipt of team packet
2. Design and implement login banner

a.

```
blueteam@ip-192-168-6-201 ~> ssh blueteam@192.168.6.21
Unauthorized access to this machine is prohibited. Only authorized users may access this system. Please do not use this system for illegal purposes.
This system is being monitored to detect improper use and other illicit activity, and there is no expectation of privacy while using this system.
```

Title

This device is for the use of The National Emergency Response Division (N.E.R.D) of Big Time Health Organization (BTHO) and should be only used for work-related functionality. Unauthorized access to this machine is strictly prohibited. This system is being monitored to detect improper use and other illicit activity, and there is no expectation of privacy while using this system. Please do not use this system for illegal purposes. BTHO preserves the right to take legal action against improper/illicit activity conducted on the system.

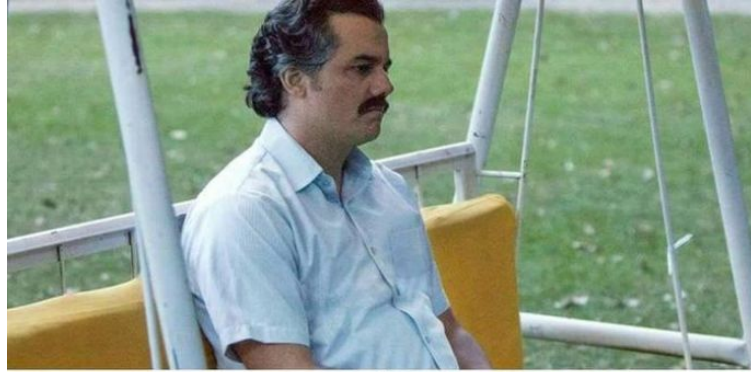
OK

3. List all AD users and their passwords
 - a. Didn't finish
4. List all services on pdc, coredb, share, windows user, mail user, map server, blog, internal (stats site), docs, prod, linux user and their associated processes
 - a. tasklist on windows and ps aux on linux



5. Find or create SSH hardening checklist for windows machines
6. VPN
7. Don't remember
 - a. Didn't finish
8. Add file "vaccine.txt" to machines to activate kill switch on ransomware
9. Create firewall rules for internal (statistics site)
 - a. DON'T BLOCK EPHEMERAL PORTS
 - i. `sudo iptables -A OUTPUT -p tcp --dport 50000:65535 -j DROP == BAD`
10. Set user computers to use same NTP server
11. MEMES

Being an Alternate



Proud Sponsors



CACI

EVER VIGILANT

