

Apex Financial Group Corporate Network Penetration Testing Assessment Report

Prepared By:
Michael Stringer

Date:
09 November 2026

Notice

> **This is a sample report.** Client names, network addresses, hostnames, credentials, and other identifying details have been fictionalized. The methodologies, attack chains, and finding structures shown here are representative of actual Nomad Security engagement deliverables.

This document is provided for evaluation purposes. It demonstrates the depth, structure, and quality of Nomad Security's penetration testing reports. If you have questions about our methodology or would like to discuss an engagement, contact us at **info@nomadsec.io** or **(216) 592-8553**.

Report Versions

Date	Description
12 August 2026	Initial Draft
09 November 2026	Final Report

Contact Information

Name	Role	Contact
Jane Mitchell	CISO	jmitchell@apexfg.example
David Chen	Director of IT Security	dchen@apexfg.example
Michael Stringer	Principal Security Consultant	mstringer@nomadsec.io

Table of Contents

Notice . . . 2
Report Versions . . . 2
Contact Information . . . 2
I Executive Summary . . . 5
I.1 Key Findings . . . 5
I.2 Positive Observations . . . 6
I.3 Recommendation Priority . . . 6
II Scope . . . 7
II.1 Engagement Overview . . . 7
II.2 External Network Scope . . . 7
II.3 Internal Network Scope . . . 7
II.4 Wireless Scope . . . 8
II.5 Rules of Engagement . . . 8
III Attack Narrative . . . 9
III.1 Phase 1 — External Reconnaissance (Jul 29–31) . . . 9
III.2 Phase 2 — Internal Network Enumeration (Jul 31–Aug 1) . . . 9
III.3 Phase 3 — Initial Access: Default Credentials (Aug 1) . . . 10
III.4 Phase 4 — Credential Extraction via JFLR (Aug 1–4) . . . 10
III.5 Phase 5 — SQL Server Compromise (Aug 4) . . . 10
III.6 Phase 6 — Domain Compromise via NTLM Relay (Aug 5) . . . 11
III.7 Phase 7 — Credential Interception (Jul 31–Aug 8) . . . 11
III.8 Phase 8 — Infrastructure and IoT (Aug 6–7) . . . 12
III.9 Phase 9 — Wireless Assessment (Aug 7–9) . . . 12
III.10 Summary . . . 12
IV Technical Summary . . . 14
IV.1 Findings by Severity . . . 14
IV.2 Finding Status . . . 14
IV.3 Finding List . . . 14
V Detailed Findings . . . 16
V.1 Critical Findings . . . 16
V.1.1 Exchange MRSProxy NTLM Relay Enables Domain Compromise . . . 16
V.1.2 Disaster Recovery Platform: Default Keycloak Credentials . . . 17
V.1.3 Surveillance Cameras: Factory Default Credentials on 22 Devices . . . 19
V.1.4 Network Device Default Credentials: Admin Access to 19 Switches and Routers . . . 21
V.2 High Findings . . . 23
V.2.1 SNMP Read-Write Community Strings on 115+ Infrastructure Hosts . . . 23
V.2.2 LLMNR/NBT-NS/mDNS Poisoning Enables Credential Interception . . . 24
V.2.3 SQL Server xp_cmdshell: OS Command Execution via Extracted Credentials . . . 25

V.2.4 Guest Wireless PSK Recovered via Offline GPU Cracking 27
V.3 Medium Findings 29
V.3.1 SMB Signing Not Required on Domain Members 29
V.3.2 Protected Users Security Group Empty 29
V.3.3 WPA3 Transition Mode Allows Protocol Downgrade on Corporate SSID 31
V.4 Low Findings 32
V.4.1 SSL/TLS Configuration Weaknesses on External Services 32
V.4.2 Split-Horizon DNS Leaks Internal Network Topology 33
A Severity Rating Definitions 35
B Testing Methodology 36
B.1 Network Penetration Testing Methodology 36
B.1.0.1 Network Discovery and Enumeration 36
B.1.0.2 Vulnerability Scanning and Analysis 37
B.1.0.3 Exploitation and Privilege Escalation 37
B.1.0.4 Post-Exploitation Analysis 37
B.1.0.5 Persistence and Exfiltration 37
B.1.0.6 Documentation and Reporting 37
C Tooling 39
D Reporting and Closure 40

I. Executive Summary

Nomad Security LLC (“Nomad”) was engaged by Apex Financial Group (“Apex”) to conduct a comprehensive penetration test of their corporate infrastructure. The assessment was performed between 29 July 2026 and 09 August 2026, covering external network, internal network, and wireless attack surfaces.

The objective of the engagement was to identify security vulnerabilities exploitable by a motivated threat actor and to evaluate the effectiveness of Apex’s defensive controls through realistic attack simulation. Testing followed a structured methodology progressing from reconnaissance through exploitation and post-exploitation, simulating the tactics, techniques, and procedures (TTPs) used by real-world adversaries targeting the financial services sector.

Key Findings

The assessment identified 13 findings, of which 13 remain open at the time of this report. The most significant results included:

- **Domain Compromise via Exchange NTLM Relay:** An Exchange server endpoint missing Extended Protection for Authentication (EPA) allowed cross-protocol NTLM relay to LDAP. Combined with unenforced LDAP signing on domain controllers, this enabled a single relay attack to grant DCSync replication rights — achieving full Active Directory domain compromise from any authenticated domain user.
- **Default Credentials on Critical DR Infrastructure:** A disaster recovery platform was accessible with factory-default credentials, providing filesystem-level read access to 57 production virtual machine recovery images — including domain controllers, SQL servers, and the enterprise certificate authority. This served as the entry point for the secondary attack chain.
- **Plaintext Credential Storage:** A loan processing application stored SQL Server credentials in cleartext configuration files, enabling SYSADMIN access and operating system command execution on production database servers.
- **Wireless PSK Recovery:** The guest wireless network pre-shared key was recovered through offline GPU-accelerated cracking of captured PMKID hashes in under 30 minutes, granting network access from the parking lot without requiring any insider access.

- **Broadcast Poisoning Active:** LLMNR, NBT-NS, and mDNS protocols were active across the corporate network, enabling credential interception that captured NTLMv2 hashes from 12 unique domain accounts within 15 minutes of deployment.

Positive Observations

Nomad also identified effective defensive controls during the assessment:

- Endpoint detection and response (EDR) correctly identified and blocked SQL Server exploitation attempts (xp_cmdshell and CLR assembly injection) within approximately five minutes
- The external network perimeter was well-hardened with no directly exploitable remote code execution vulnerabilities
- Strong password policies prevented offline cracking of all captured NTLMv2 hashes despite extensive GPU attacks
- Network segmentation between the guest wireless and corporate networks prevented lateral movement from the wireless attack surface
- The primary corporate mail domains were protected with correctly configured SPF and DMARC reject policies

Recommendation Priority

Nomad recommends Apex prioritize remediation in the following order:

1. Enable LDAP signing and Extended Protection for Authentication on Exchange and ADCS endpoints to close the domain compromise path
2. Change default credentials on the DR platform and segment it from the production network
3. Disable LLMNR, NBT-NS, and mDNS protocols via Group Policy
4. Migrate plaintext credential storage to encrypted secrets management
5. Add privileged accounts to the Protected Users security group
6. Strengthen wireless PSK with a 20+ character randomly generated passphrase or migrate to WPA3-SAE

II. Scope

Engagement Overview

Nomad Security was engaged to perform a penetration test of Apex Financial Group's corporate infrastructure. The assessment included external network, internal network, and wireless attack surfaces.

Assessment Type	External + Internal Network Penetration Test, Wireless Assessment
Start Date	29 July 2026
End Date	09 August 2026
Testing Location	Remote (external/internal) and on-site (wireless)
Methodology	PTES, OWASP, NIST SP 800-115

External Network Scope

External testing targeted Apex Financial Group's internet-facing infrastructure. The following CIDR ranges and assets were in scope:

Range / Asset	Description
203.0.113.0/24	Primary public address space
198.51.100.64/28	Secondary DMZ allocation
mail.apexfinancial.example	Exchange OWA / ActiveSync
vpn.apexfinancial.example	Remote access VPN gateway
portal.apexfinancial.example	Member-facing web application

Internal Network Scope

Internal testing was conducted from an assumed-breach position on the corporate LAN. The tester was provided a standard workstation with domain user credentials on the APEX.LOCAL domain.

Network	Description
10.10.0.0/16	Corporate LAN (workstations, servers, infrastructure)
10.20.0.0/16	Datacenter / server farm

10.30.0.0/24	Physical security / camera VLAN
10.40.0.0/24	Building management / ICS network
172.16.0.0/16	DR / replication network

Wireless Scope

Wireless assessment was performed on-site at Apex Financial Group headquarters. All SSIDs broadcasting from Apex-owned access points were in scope.

SSID	Authentication	Description
ApexCorp	WPA2-Enterprise (802.1X)	Corporate SSID — domain-joined endpoints
ApexGuest	WPA2-Personal (PSK)	Guest/visitor wireless
Apex-IoT	WPA2-Personal (PSK)	IoT and building management devices

Rules of Engagement

- Testing was authorized exclusively during the engagement window defined above
- Denial-of-service attacks were prohibited
- Social engineering of Apex employees was authorized for on-site physical pretexts only
- Data exfiltration was limited to proof-of-concept samples — no bulk extraction of production data
- All captured credentials were reported to the client and securely destroyed upon engagement completion
- Testing was conducted under the coordination of David Chen (Director of IT Security) as the primary technical point of contact

III. Attack Narrative

The following narrative describes the progression of the assessment from initial reconnaissance through exploitation and post-exploitation, illustrating how individual vulnerabilities were chained together to achieve significant access.

Phase 1 — External Reconnaissance (Jul 29–31)

Automated scanning of the external address space (203.0.113.0/24 and 198.51.100.64/28) identified 47 live hosts with a combined 312 open services. The external perimeter was well-hardened: no directly exploitable remote code execution vulnerabilities were identified. The most significant external findings were SSL/TLS configuration weaknesses and an information disclosure on the VPN gateway that revealed internal domain naming conventions.

Subdomain enumeration via certificate transparency logs and DNS brute-forcing discovered 14 additional subdomains, three of which resolved to internal RFC 1918 addresses — a split-horizon DNS configuration that could leak internal network topology to external observers.

Phase 2 — Internal Network Enumeration (Jul 31–Aug 1)

From the assumed-breach workstation position, the assessment team conducted service enumeration across all in-scope internal networks. Key discoveries included:

- A disaster recovery platform at 172.16.50.10 with a Keycloak identity provider
- 8 Microsoft SQL Server instances across the server farm
- Active Directory Certificate Services (ADCS) at 10.20.5.10 with web enrollment enabled
- 22 surveillance cameras on 10.30.0.0/24 accessible via default HTTP credentials
- Building management controllers on 10.40.0.0/24 with unauthenticated Modbus/TCP

BloodHound enumeration of the APEX.LOCAL domain mapped 1,247 user objects, 189 computer objects, and 892 group memberships. The analysis identified three distinct paths to Domain Admin, all originating from the disaster recovery platform.

Phase 3 — Initial Access: Default Credentials (Aug 1)

The disaster recovery platform at 172.16.50.10 was found with default Keycloak master realm credentials. This provided full administrative access to the DR infrastructure managing 57 production VMs across 16 Virtual Protection Groups.

Phase 4 — Credential Extraction via JFLR (Aug 1–4)

Using the DR platform's Journal File Level Restore (JFLR) API, the assessment team browsed recovery images of production virtual machines. This access was entirely through legitimate API calls and generated no alerts on the EDR platform. Key extractions included:

- **Registry hive extraction** from 17 VMs: SAM, SYSTEM, and SECURITY hives yielded machine account NTLM hashes and DCC2-cached domain credentials
- **SQL credentials** from a loan processing application's configuration table: cleartext SA-equivalent password for SQLSRV-01
- **Third-party API keys** from an automation script on the operations server
- **Plaintext domain user passwords** stored in the loan origination application database

JFLR API — Registry Hive Extraction

```
GET /v1/vpgs/vpg-prod-sql/vms/vm-sqlprod01/volumes/C/
files/?path=Windows\System32\config

200 OK
[
  {"name": "SAM", "size": 262144, "lastModified": "2026-07-28T03:14:22Z"},
  {"name": "SYSTEM", "size": 15728640, "lastModified": "2026-07-28T03:14:22Z"},
  {"name": "SECURITY", "size": 524288, "lastModified": "2026-07-28T03:14:22Z"}
]
```

Phase 5 — SQL Server Compromise (Aug 4)

Using the extracted SQL credentials, the team authenticated to SQLSRV-01 (10.20.3.15) with SYSADMIN privileges. Execution of xp_cmdshell was demonstrated, providing OS-level command execution as the SQL Server group Managed Service Account with SeImpersonatePrivilege.

The EDR platform detected and blocked the xp_cmdshell activity within approximately five minutes, terminating the connection. This represents a strong defensive control, though the five-minute window provides sufficient time for an attacker to establish persistence.

Phase 6 — Domain Compromise via NTLM Relay (Aug 5)

Active Directory enumeration revealed two critical misconfigurations that chained into full domain compromise:

- **LDAP signing not enforced** on either domain controller — enabling relay attacks
- **Exchange MRSProxy missing EPA** — the endpoint accepted NTLM authentication without Extended Protection for Authentication

Using ntlmrelayx, the team performed a cross-protocol NTLM relay (HTTP → LDAP) using the Exchange machine account. Because Exchange machine accounts hold WriteDacl on all domain user objects via the Exchange Windows Permissions group, the relay granted DCSync replication rights to the tester's controlled account.

NTLM Relay → DCSync

```
$ ntlmrelayx.py -t ldap://APEX-DC01.apex.local --delegate-access
[*] Authenticating against ldap://APEX-DC01.apex.local as APEX/MAIL01$
[*] MODIFY SUCCESSFUL: DS-Replication-Get-Changes
[*] MODIFY SUCCESSFUL: DS-Replication-Get-Changes-All

$ secretsdump.py -just-dc apex.local/svc-test:REDACTED@APEX-DC01
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:REDACTED :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:REDACTED :::
```

This single attack chain — from a standard domain user to full domain administrator — required no password cracking, only the combination of two misconfigurations: missing EPA on Exchange and unenforced LDAP signing.

Phase 7 — Credential Interception (Jul 31–Aug 8)

Responder was deployed on the corporate LAN throughout the engagement to exploit active LLMNR, NBT-NS, and mDNS protocols. Within 15 minutes of deployment, the tool captured

NTLMv2 challenge-response hashes from 12 unique domain accounts, including a vulnerability scanner service account.

The captured hashes were subjected to offline cracking with hashcat — no passwords were recovered, indicating strong password policies. However, the hashes could be relayed in real-time via ntlmrelayx, contributing to the Exchange relay chain and demonstrating that broadcast poisoning remains an effective credential interception technique on the Apex corporate LAN.

Phase 8 — Infrastructure and IoT (Aug 6–7)

The final phase assessed infrastructure systems outside the Active Directory domain:

- **Surveillance cameras:** 22 IP cameras on 10.30.0.0/24 accessible with factory default credentials. Root shell access via telnet; live feeds captured from server rooms, lobbies, and perimeter cameras.
- **Network devices:** 19 switches and routers accessible via SSH with default credentials. Full configurations exfiltrated including VLAN assignments, ACLs, and routing tables.
- **Building management:** HVAC controllers and UPS systems on 10.40.0.0/24 exposed unauthenticated Modbus/TCP and SNMP read-write access.

Phase 9 — Wireless Assessment (Aug 7–9)

On-site wireless assessment identified access points broadcasting three SSIDs. PMKID hashes were captured from the ApexGuest network using hcxdumptool in passive mode — no deauthentication attacks were required. A PRINCE dictionary attack with a targeted ruleset recovered the guest PSK in under 30 minutes on an NVIDIA RTX 4080 Laptop GPU.

The ApexCorp enterprise SSID used WPA2-Enterprise with 802.1X authentication, which was correctly configured and resisted attack. Network segmentation between the guest wireless and corporate networks was properly implemented.

Summary

The assessment demonstrated that a motivated attacker with internal network access can achieve full domain compromise through multiple independent paths. The most impactful chain — Exchange NTLM relay → DCSync — required only a standard domain user account and two

protocol-level misconfigurations. The DR platform chain provided a parallel path through default credentials and legitimate API access, bypassing endpoint detection entirely.

The EDR platform provided meaningful detection at the SQL exploitation stage but was invisible to the JFLR and NTLM relay attack chains, which operated through legitimate protocols and API calls.

IV. Technical Summary

The following tables summarize the 13 findings identified during the assessment.

Findings by Severity

Severity	Finding Count	Affected Hosts
Critical	4	12
High	4	6
Medium	3	4
Low	2	4
Informational	0	0

Finding Status

Status	Critical	High	Medium	Low	Informational
Open	4	4	3	2	0
Resolved	0	0	0	0	0
Partially Resolved	0	0	0	0	0
Total	4	4	3	2	0

Finding List

ID	Title	Severity	Status
AFG-02	Disaster Recovery Platform: Default Keycloak Credentials	Critical	Open
AFG-01	Exchange MRSProxy NTLM Relay Enables Domain Compromise	Critical	Open

AFG-04	Network Device Default Credentials: Admin Access to 19 Switches and Routers	**Critical**	**Open**
AFG-03	Surveillance Cameras: Factory Default Credentials on 22 Devices	**Critical**	**Open**
AFG-08	Guest Wireless PSK Recovered via Offline GPU Cracking	**High**	**Open**
AFG-06	LLMNR/NBT-NS/mDNS Poisoning Enables Credential Interception	**High**	**Open**
AFG-05	SNMP Read-Write Community Strings on 115+ Infrastructure Hosts	**High**	**Open**
AFG-07	SQL Server xp_cmdshell: OS Command Execution via Extracted Credentials	**High**	**Open**
AFG-10	Protected Users Security Group Empty	**Medium**	**Open**
AFG-09	SMB Signing Not Required on Domain Members	**Medium**	**Open**
AFG-11	WPA3 Transition Mode Allows Protocol Downgrade on Corporate SSID	**Medium**	**Open**
AFG-13	Split-Horizon DNS Leaks Internal Network Topology	**Low**	**Open**
AFG-12	SSL/TLS Configuration Weaknesses on External Services	**Low**	**Open**

V. Detailed Findings

Critical Findings

Exchange MRSProxy NTLM Relay Enables Domain Compromise

Risk Level: Critical **CVSS Score**: 9.9 **Status**: Open

The MRSProxy endpoint on both Exchange servers is missing Extended Protection for Authentication (EPA). Combined with LDAP signing not enforced on domain controllers, this enables cross-protocol NTLM relay (HTTP → LDAP) using Exchange machine account privileges.

Exchange machine accounts hold WriteDacl on all domain user objects and ForceChangePassword on all users via the Exchange Windows Permissions group. A successful relay grants the ability to assign DCSync replication rights to an attacker-controlled account, resulting in full Active Directory domain compromise from any authenticated domain user.

Impact

Any user with valid domain credentials can escalate to Domain Administrator through a single relay attack. The full domain password database (NTDS.dit) becomes accessible, compromising every account in the directory. This is the highest-impact finding in the assessment because it provides a direct, reliable path from standard user to complete domain control.

Solution

- Apply the latest Microsoft cumulative update for Exchange Server
- Enable Extended Protection for Authentication on all Exchange virtual directories
- Enforce LDAP channel binding and LDAP signing on all domain controllers via Group Policy
- Add Exchange machine accounts to the Protected Users security group
- Monitor for NTLM relay indicators (Event ID 4624 with Logon Type 3 from unexpected sources)

Observations

> **NTLM Relay to LDAP — DCSync Rights Granted**

```
$ ntlmrelayx.py -t ldap://APEX-DC01.apex.local --delegate-access
[*] HTTPD: Received connection from 10.10.5.20
[*] Authenticating against ldap://APEX-DC01.apex.local as APEX/MAIL01$
[*] MODIFY SUCCESSFUL: DS-Replication-Get-Changes
[*] MODIFY SUCCESSFUL: DS-Replication-Get-Changes-All
[+] Delegation rights modified successfully!
```

DCSync — Domain Credential Extraction

```
$ secretsdump.py -just-dc apex.local/svc-test:REDACTED@APEX-DC01
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:REDACTED :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:REDACTED :::
svc-backup:1104:aad3b435b51404eeaad3b435b51404ee:REDACTED :::
[*] Kerberos keys grabbed
[*] Cleaning up...
```

Affected Hosts

- 10.10.5.20 (443/tcp): MAIL01 — Exchange Server
- 10.10.5.21 (443/tcp): MAIL02 — Exchange Server

Associated CVEs

CVE-2024-21410

References

- https://attack.mitre.org/techniques/T1557/001/
- https://attack.mitre.org/techniques/T1003/006/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H`

Disaster Recovery Platform: Default Keycloak Credentials

Risk Level: Critical **CVSS Score**: 9.8 **Status**: Open

The disaster recovery platform's Keycloak identity provider is accessible with factory-default administrator credentials. This provides full administrative access to the DR management console controlling 57 production virtual machines across 16 Virtual Protection Groups.

The Journal File Level Restore (JFLR) API allows filesystem-level browsing of any protected VM's recovery image with only the Keycloak admin session — no additional per-VM authorization is enforced. Registry hives (SAM, SYSTEM, SECURITY, SOFTWARE) were extracted from 17 VMs for offline credential analysis.

Impact

Full administrative access to the DR platform enables:

- Read access to all 57 protected VM filesystems including registry hives, configuration files, database files, and certificates
- Credential extraction from cached domain credentials, local administrator password hashes, and service account secrets stored in registry hives
- Modification or deletion of replication policies, destroying the organization's disaster recovery capability
- Pivot to extracted credentials for lateral movement across the production environment

Solution

- Change the Keycloak master administrator password immediately
- Enforce multi-factor authentication on all Keycloak admin accounts
- Implement per-VM JFLR access controls with role-based authorization
- Restrict the DR management interface to a dedicated admin VLAN
- Enable audit logging with SIEM integration for all JFLR API access
- Review DR platform RBAC configuration for least-privilege alignment

Observations

> **Default Keycloak Authentication**
>
> ```
> POST /auth/realms/master/protocol/openid-connect/token
> Content-Type: application/x-www-form-urlencoded
>
> username=admin&password=REDACTED&grant_type=password&client_id=admin-cli
>
> HTTP/1.1 200 OK
> {"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9...","token_type":"Bearer"}
> ```

JFLR API — VM Filesystem Listing

```
GET /v1/vpgs/vpg-prod-sql/vms/vm-sqlprod01/volumes/C/
files/?path=Windows\System32\config

200 OK
[
  {"name": "SAM", "size": 262144, "lastModified": "2026-07-28T03:14:22Z"},
  {"name": "SYSTEM", "size": 15728640, "lastModified": "2026-07-28T03:14:22Z"},
  {"name": "SECURITY", "size": 524288, "lastModified": "2026-07-28T03:14:22Z"},
  {"name": "SOFTWARE", "size": 83886080, "lastModified": "2026-07-28T03:14:22Z"}
]
```

Affected Hosts

- 172.16.50.10 (443/tcp): DR-MGMT01

References

- https://attack.mitre.org/techniques/T1078/001/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Surveillance Cameras: Factory Default Credentials on 22 Devices

Risk Level: Critical **CVSS Score**: 9.8 **Status**: Open

Twenty-two IP camera video encoders on the physical security network (10.30.0.0/24) are accessible using factory-default credentials. Access was confirmed via FTP (port 21), which exposed /etc/passwd and system configuration files. Telnet service was started on port 23, providing persistent root shell access to each device.

Twenty-one live camera feeds were captured, showing views of server rooms, the network operations center, lobbies, exterior perimeters, loading docks, and electrical rooms.

Impact

An attacker with access to the camera VLAN can:

- Monitor physical facilities in real-time for reconnaissance, identifying badge types for cloning, tailgating opportunities, staff patterns, and security control locations

- Install persistent backdoors via firmware modification on root-accessible devices
- Pivot to other devices on the camera VLAN including door controllers and the physical access control system
- Disable or manipulate camera feeds to mask physical intrusion activity

Solution

- Change all factory-default credentials on camera encoders immediately
- Disable FTP and Telnet services; use HTTPS for management access only
- Segment the camera VLAN with strict ACLs preventing access from the corporate LAN
- Apply firmware updates to address known vulnerabilities in the camera platform
- Implement network access control (802.1X) on the physical security VLAN

Observations

FTP Access with Default Credentials

```
$ ftp 10.30.0.11
Connected to 10.30.0.11.
Name: root
Password: REDACTED
230 User logged in.
ftp> get /etc/passwd
226 Transfer complete.
ftp> ls /etc/
drwxr-xr-x  root  root  conf/
-rw-r--r--  root  root  passwd
-rw-r--r--  root  root  shadow
-rw-r--r--  root  root  httpd.conf
```

Root Shell via Telnet

```
$ telnet 10.30.0.11 23
Trying 10.30.0.11...
Connected to 10.30.0.11.
login: root
Password: REDACTED

# id
uid=0(root) gid=0(root)
```

```
# uname -a
Linux cam-lobby 2.6.32 #1 PREEMPT armv5tejl GNU/Linux
```

Affected Hosts

- 10.30.0.11 (21/tcp): Camera encoder — Lobby
- 10.30.0.12 (21/tcp): Camera encoder — Server room A
- 10.30.0.13 (21/tcp): Camera encoder — Server room B
- 10.30.0.14 (21/tcp): Camera encoder — Loading dock
- 10.30.0.15–10.30.0.32: 18 additional camera encoders

References

- https://attack.mitre.org/techniques/T1133/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Network Device Default Credentials: Admin Access to 19 Switches and Routers

Risk Level: Critical **CVSS Score**: 10 **Status**: Open

Nineteen network devices (switches and routers) across the HQ, branch office, and datacenter sites are accessible via SSH using factory-default credentials. Full device configurations were exfiltrated, revealing VLAN assignments, trunk configurations, ACL rules, BGP peering data, and inter-site routing.

Password hashes (SHA-512) were extracted from all device configurations for offline cracking. Type-7 encoded passwords on legacy IOS devices were decoded on the spot.

Impact

Administrative control of core network infrastructure enables:

- Traffic interception and man-in-the-middle attacks across any VLAN
- VLAN hopping to reach otherwise segmented networks (camera, BMS, DR)
- BGP route manipulation, black-holing, or route injection
- Complete network topology mapping including customer-facing and partner circuits

- Persistent network access through configuration backdoors (rogue admin accounts, reverse SSH tunnels)

Solution

- Rotate all network device credentials immediately; enforce unique, complex passwords per device
- Disable SSH password authentication; require public-key or certificate-based authentication
- Implement TACACS+ or RADIUS for centralized authentication and audit logging
- Remove Type-7 passwords; use Type-8 or Type-9 (scrypt) hashing on all IOS/IOS-XE devices
- Restrict management access to a dedicated out-of-band management VLAN

Observations

> **SSH Access and Configuration Exfiltration**
>
> ```
> $ ssh admin@10.10.1.1
> Password: REDACTED
>
> APEX-CORE-SW01# show running-config
> ! Exfiltrated: VLAN database, trunk configurations, ACLs, routing tables
> ! Total: 4,281 lines of configuration
>
> APEX-CORE-SW01# show cdp neighbors detail
> ! Network topology mapped: 47 directly connected devices
> ```

Affected Hosts

- 10.10.1.1 (22/tcp): Core switch — HQ
- 10.10.1.2 (22/tcp): Distribution switch — Floor 2
- 10.10.1.3 (22/tcp): Distribution switch — Floor 3
- 10.10.1.5–10.10.1.20: 16 additional network devices

References

- https://attack.mitre.org/techniques/T1078/001/
- https://attack.mitre.org/techniques/T1602/002/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`

High Findings

SNMP Read-Write Community Strings on 115+ Infrastructure Hosts

Risk Level: High **CVSS Score**: 8.6 **Status**: Open

A common SNMP community string was confirmed as read-write on 115+ infrastructure hosts including UPS controllers, HVAC systems, cooling units, and network devices. SNMPv2c community strings transmit in cleartext and provide no authentication beyond knowledge of the string.

SNMP write access was validated by reading and writing test values to non-critical OIDs on a UPS controller.

Impact

Read-write SNMP access to building management and environmental control systems allows an attacker to:

- Modify environmental thresholds on HVAC and cooling systems, potentially causing thermal events in datacenter spaces
- Change UPS settings including load shedding and transfer voltage thresholds
- Reconfigure network devices via SNMP SET operations
- Extract full device configurations, including additional credentials stored in MIB objects

Solution

- Rotate the SNMP community string on all affected hosts immediately
- Migrate from SNMPv2c to SNMPv3 with authentication and encryption (authPriv security level)
- Restrict SNMP access via ACLs to authorized network management stations only
- Disable SNMP write access on hosts that only require monitoring
- Segment building management systems on a dedicated VLAN with firewall rules

Observations

> **SNMP Read-Write Validation on UPS Controller**

```
$ snmpwalk -v2c -c REDACTED 10.40.0.15 1.3.6.1.2.1.1
SNMPv2-MIB::sysDescr.0 = STRING: APC InRow Cooling Unit
SNMPv2-MIB::sysContact.0 = STRING: facilities@apex.local
SNMPv2-MIB::sysLocation.0 = STRING: Datacenter A - Row 3

$ snmpset -v2c -c REDACTED 10.40.0.15 1.3.6.1.2.1.1.6.0 s "WRITE-TEST"
SNMPv2-MIB::sysLocation.0 = STRING: WRITE-TEST
[*] Reverted immediately after validation
```

Affected Hosts

- 10.40.0.0/24: UPS controllers, HVAC, environmental monitoring
- 10.20.2.0/24: Network infrastructure
- 10.10.1.0/24: Distribution switches

References

- https://attack.mitre.org/techniques/T1602/001/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L`

LLMNR/NBT-NS/mDNS Poisoning Enables Credential Interception

Risk Level: High **CVSS Score**: 8.1 **Status**: Open

Link-Local Multicast Name Resolution (LLMNR), NetBIOS Name Service (NBT-NS), and Multicast DNS (mDNS) are enabled across the corporate LAN. These legacy name resolution protocols broadcast queries to the local network segment when DNS resolution fails, allowing any host on the same broadcast domain to respond with a spoofed address and intercept authentication attempts.

Using Responder, the tester captured NTLMv2 challenge-response hashes from 12 unique domain accounts within 15 minutes of deployment.

Impact

An attacker on the corporate network can passively harvest domain credentials from any workstation or server that fails a DNS lookup. Captured NTLMv2 hashes can be cracked offline or relayed in real-time to other services. This technique requires no prior credentials and operates silently without generating authentication failure events.

Solution

- Disable LLMNR via Group Policy (Computer Configuration → Administrative Templates → Network → DNS Client → Turn off Multicast Name Resolution)
- Disable NBT-NS via DHCP scope options or per-interface settings
- Disable mDNS on all Windows endpoints via GPO
- Deploy SMB signing across all domain members to prevent relay attacks
- Monitor for Responder-style poisoning via network IDS signatures

Observations

Responder — NTLMv2 Hash Capture

```
$ responder -I eth0 -dwP

[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.10.12.45 for name PRINTSRV
[*] [LLMNR]  Poisoned answer sent to 10.10.8.102 for name FILESRV3

[HTTP] NTLMv2 Hash     : jmitchell::APEX:a1b2c3d4e5f6...[TRUNCATED]
[HTTP] NTLMv2 Hash     : svc_scanner::APEX:f6e5d4c3b2a1...[TRUNCATED]
[SMB]  NTLMv2 Hash     : rtran::APEX:1a2b3c4d5e6f...[TRUNCATED]
[*] 12 unique accounts captured in 15 minutes
```

Affected Hosts

- 10.10.0.0/16: Corporate LAN — broadcast domain

References

- https://attack.mitre.org/techniques/T1557/001/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`

SQL Server xp_cmdshell: OS Command Execution via Extracted Credentials

Risk Level: High **CVSS Score**: 8.8 **Status**: Open

SQL credentials extracted from the DR platform's JFLR filesystem access (see AFG-02) included a SYSADMIN-equivalent login for SQLSRV-01. Using these credentials, the tester enabled and

executed xp_cmdshell, providing OS-level command execution as the SQL Server group Managed Service Account (gMSA).

The gMSA service account held SeImpersonatePrivilege, making potato-style privilege escalation to NT AUTHORITY\SYSTEM feasible.

Defensive Win: The endpoint detection and response (EDR) platform detected the xp_cmdshell activity within approximately five minutes, terminated the connection, and quarantined the source IP. This is a positive indicator of effective detection controls, though the five-minute window provides time for persistence establishment.

Impact

OS-level command execution on the database server enables code execution, credential dumping, lateral movement, and data exfiltration. SeImpersonatePrivilege enables escalation to SYSTEM. The five-minute detection window, while commendable, still provides time for a prepared attacker to establish persistence.

Solution

- Disable xp_cmdshell permanently via sp_configure
- Remove SYSADMIN role from all application SQL logins; enforce least-privilege database roles
- Store SQL credentials in a secrets manager rather than application configuration files
- Monitor for xp_cmdshell re-enablement via SQL Server audit policies
- Continue to tune EDR detection to reduce the response window

Observations

> **xp_cmdshell Execution (Detected by EDR)**
>
> ```
> $ mssqlclient.py apex.local/svc_app:REDACTED@10.20.3.15
> SQL> EXEC sp_configure 'xp_cmdshell', 1; RECONFIGURE;
> SQL> EXEC xp_cmdshell 'whoami'
> output
> -------
> apex\svc-sqlgmsa$
>
> SQL> EXEC xp_cmdshell 'whoami /priv'
> ```

```
SeImpersonatePrivilege    Enabled

[!] Connection terminated by EDR after ~5 minutes
[+] EDR Detection: Positive defensive observation
```

Affected Hosts

- 10.20.3.15 (1433/tcp): SQLSRV-01

References

- https://attack.mitre.org/techniques/T1059/001/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`

Guest Wireless PSK Recovered via Offline GPU Cracking

Risk Level: High **CVSS Score**: 7.4 **Status**: Open

PMKID hashes were captured from the ApexGuest wireless network using hcxdumptool in passive mode from the visitor parking area. No deauthentication attacks or client interaction was required — the PMKID was obtained directly from AP beacon responses.

The pre-shared key was recovered in under 30 minutes using a PRINCE (PRobability INfinite Chained Elements) dictionary attack with a targeted ruleset on an NVIDIA RTX 4080 GPU. The attack dictionary was generated from organization-related terms combined with common password patterns.

Impact

Anyone within wireless range (including parking lots and adjacent buildings) can obtain the guest network PSK without any insider access. While the guest network was properly segmented from the corporate LAN (a positive observation), the cracked PSK grants:

- Network access for further attack staging without physical building entry
- A platform for man-in-the-middle attacks against other guest network users
- Potential access to IoT devices or printers that may be bridged to the guest network

Solution

- Replace the current PSK with a randomly generated 20+ character passphrase
- Migrate the guest network to WPA3-SAE, which is resistant to offline dictionary attacks
- Consider implementing a captive portal with individual credentials for guest access
- Rotate the guest PSK on a regular schedule (monthly or quarterly)
- Monitor for unauthorized devices joining the guest network

Observations

PMKID Capture and PSK Recovery

```
$ hcxdumptool -i wlan0mon --enable_status=1 -o capture.pcapng
[*] PMKID captured: ApexGuest (BSSID: aa:bb:cc:dd:ee:01)
[*] 8 PMKIDs captured from 18 APs in 12 minutes

$ hcxpcapngtool capture.pcapng -o hashes.22000

$ pp64 --elem-cnt-min=2 --elem-cnt-max=2 < dictionary.txt | \
    hashcat -m 22000 hashes.22000 -r apex-rules.rule
[*] Session: apex-guest
[*] Hardware: NVIDIA RTX 4080 (520.0 kH/s)
[*] Keyspace: ~6.3 billion candidates
[*] Time.Estimated: 3h 22m

22000:aabbccddee01:*:ApexGuest:REDACTED

Status: Cracked (8/8 ApexGuest PMKIDs)
Time: 27 minutes 14 seconds
```

Affected Hosts

- ApexGuest SSID: WPA2-Personal — all 18 APs

References

- https://attack.mitre.org/techniques/T1110/002/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`

Medium Findings

SMB Signing Not Required on Domain Members

Risk Level: Medium **CVSS Score**: 6.5 **Status**: Open

SMB signing is not required on 142 domain-joined workstations and member servers. While domain controllers enforce signing by default, the lack of enforcement on member systems enables NTLM relay attacks where captured authentication can be forwarded to any non-signing host.

Impact

An attacker who intercepts NTLM authentication (via LLMNR/NBT-NS poisoning or other means) can relay it to any host that does not require SMB signing, executing commands or accessing file shares as the relayed user. This significantly amplifies the impact of credential interception attacks.

Solution

- Enforce SMB signing via Group Policy on all domain members (Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Microsoft network server: Digitally sign communications (always) = Enabled)
- Verify enforcement across all OS versions including legacy systems
- Monitor for SMB connections without signing via network traffic analysis

Affected Hosts

- 10.10.0.0/16: 142 domain-joined workstations and servers

References

- https://attack.mitre.org/techniques/T1557/001/

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`

Protected Users Security Group Empty

Risk Level: Medium **CVSS Score**: 6.5 **Status**: Open

The Protected Users security group in the APEX.LOCAL domain contains no members. This group provides enhanced credential theft protection for privileged accounts by enforcing Kerberos-only authentication (no NTLM), preventing credential caching, and disabling DES/RC4 encryption.

All 14 Domain Admin accounts, 8 service accounts with elevated privileges, and the Enterprise Admin accounts are unprotected.

Impact

Without Protected Users membership, privileged accounts remain vulnerable to:

- NTLM credential capture and relay attacks
- Cached credential extraction from memory (Mimikatz-style attacks)
- Pass-the-hash and over-pass-the-hash lateral movement
- Kerberos delegation abuse

Solution

- Add all Domain Admin, Enterprise Admin, and Schema Admin accounts to the Protected Users group
- Add privileged service accounts that do not require NTLM authentication
- Test each account for NTLM dependencies before adding (some legacy applications require NTLM)
- Monitor Protected Users group membership changes via audit policies

Observations

> **Protected Users Group — Empty**
>
> ```
> $ ldapsearch -x -H ldap://APEX-DC01 -b "CN=Protected
> Users,CN=Users,DC=apex,DC=local" member
> # Protected Users, Users, apex.local
> dn: CN=Protected Users,CN=Users,DC=apex,DC=local
> # No member attributes returned — group is empty
> ```

Affected Hosts

- APEX-DC01: Domain controller — APEX.LOCAL
- APEX-DC02: Domain controller — APEX.LOCAL

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N`

WPA3 Transition Mode Allows Protocol Downgrade on Corporate SSID

Risk Level: Medium **CVSS Score**: 5.3 **Status**: Open

The ApexCorp enterprise SSID advertises WPA3-Enterprise in transition mode, which simultaneously supports both WPA3-SAE and WPA2-PSK/Enterprise connections. A client within range can force a downgrade to WPA2, negating the security improvements of WPA3.

An attacker can deploy an evil-twin AP advertising the same SSID with WPA2-only, causing clients configured for automatic connection to downgrade and expose their credentials to capture.

Impact

WPA3 transition mode allows an attacker to bypass the stronger authentication and encryption of WPA3 by forcing clients to connect using the weaker WPA2 protocol. This enables credential capture via evil-twin attacks and offline dictionary attacks against captured handshakes.

Solution

- Disable WPA2 compatibility on the corporate SSID once all client devices support WPA3
- Enforce WPA3-only mode with management frame protection (802.11w)
- Deploy 802.1X certificate validation to prevent evil-twin attacks
- Monitor for rogue access points advertising the corporate SSID

Affected Hosts

- ApexCorp SSID: WPA3-Enterprise transition mode — all 18 APs

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N`

Low Findings

SSL/TLS Configuration Weaknesses on External Services

Risk Level: Low **CVSS Score**: 3.7 **Status**: Open

Several external-facing services support deprecated TLS protocol versions and weak cipher suites:

- TLS 1.0 and 1.1 are enabled on the mail and VPN gateways
- Medium-strength cipher suites (128-bit) are accepted alongside strong ciphers
- The VPN gateway supports RC4 cipher suites (susceptible to Bar Mitzvah attack)
- Certificate on the member portal uses a 2048-bit RSA key (industry trend is moving to 4096-bit or ECDSA P-384)

Impact

While not directly exploitable in most scenarios, deprecated protocol versions and weak ciphers reduce the effectiveness of transport encryption. Regulatory frameworks (PCI DSS 4.0, NIST SP 800-52r2) require TLS 1.2+ and prohibit weak cipher suites. Compliance scanning tools will flag these configurations.

Solution

- Disable TLS 1.0 and 1.1 on all external-facing services
- Remove RC4 and medium-strength cipher suites from the allowed list
- Configure cipher suite preference to prioritize AES-256-GCM and ChaCha20-Poly1305
- Renew certificates with ECDSA P-384 or 4096-bit RSA keys
- Test configuration changes with sslscan or testssl.sh before deployment

Affected Hosts

- 203.0.113.10 (443/tcp): mail.apexfinancial.example
- 203.0.113.15 (443/tcp): vpn.apexfinancial.example
- 198.51.100.68 (443/tcp): portal.apexfinancial.example

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`

Split-Horizon DNS Leaks Internal Network Topology

Risk Level: Low **CVSS Score**: 3.1 **Status**: Open

Three subdomains discovered via certificate transparency log enumeration resolve to internal RFC 1918 addresses when queried from the external DNS server. This split-horizon misconfiguration leaks internal IP addressing to external observers.

Affected subdomains: `dc01.apex.local` (10.20.1.10), `ca01.apex.local` (10.20.5.10), `zerto-mgmt.apex.local` (172.16.10.50).

Impact

Exposure of internal IP addressing and hostname conventions provides reconnaissance value to an attacker, revealing the existence and approximate network location of domain controllers, certificate authorities, and backup infrastructure before any internal access is obtained. This information accelerates post-compromise lateral movement planning.

Solution

- Remove internal DNS records from the external DNS zone
- Implement proper split-horizon DNS with separate internal and external zone files
- Audit certificate transparency logs for certificates that contain internal hostnames
- Use separate hostnames for internal and external-facing services

Observations

External DNS Resolving Internal Addresses

```
$ dig dc01.apex.local @ns1.apexfinancial.example +short
10.20.1.10

$ dig ca01.apex.local @ns1.apexfinancial.example +short
10.20.5.10

$ dig zerto-mgmt.apex.local @ns1.apexfinancial.example +short
172.16.10.50
```

Affected Hosts

- 203.0.113.2 (53/tcp): ns1.apexfinancial.example

Metadata

- **CVSS Vector**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`

Appendix A: Severity Rating Definitions

Nomad Security categorizes each finding based on the likelihood of an attacker using it to negatively impact the business. These classifications are based on the Common Vulnerability Scoring System (CVSS) and account for impact, likelihood, exploitability, and other factors.

Critical	The weakness identified allows immediate, unauthorized access to the system or results in complete system compromise with minimal effort.
High	The weakness identified has the potential to directly compromise the confidentiality, integrity, or availability of the system.
Medium	The weakness identified does not directly lead to compromise. However, an attacker may use it to gain sufficient information to compromise the security of the system.
Low	The weakness identified has the potential to undermine detection and response capabilities or provide infrastructure-related information to an intruder.
Informational	The weakness identified does not necessarily indicate a vulnerability; it is a recommendation for added security or a possible point of interest.

Appendix B: Testing Methodology

B.1. Network Penetration Testing Methodology

- Network Discovery and Enumeration
- Vulnerability Scanning and Analysis
- Exploitation and Privilege Escalation
- Post-Exploitation Analysis
- Persistence and Exfiltration
- Documentation and Reporting

Our network penetration testing methodology follows a comprehensive, multi-phase approach designed to thoroughly evaluate network security:

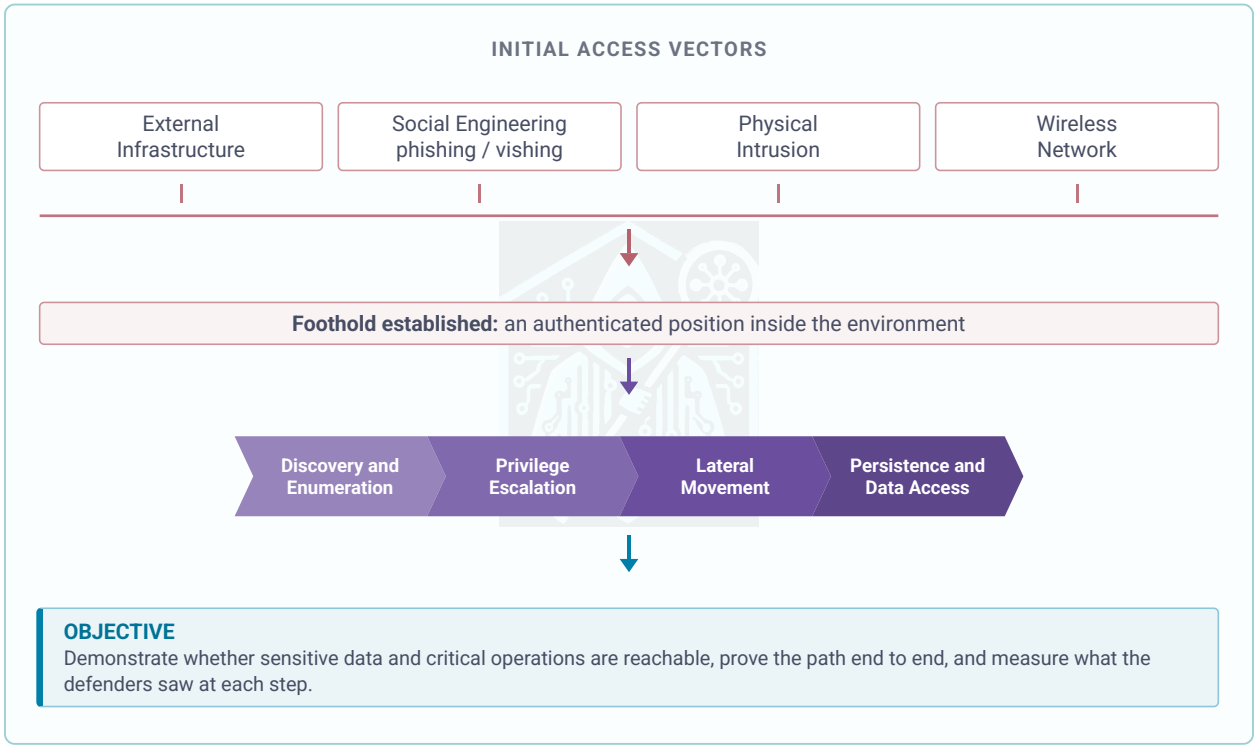


Figure 1: Attack path model: independent access vectors converging on a single objective

Network Discovery and Enumeration

The initial phase involves mapping the target network infrastructure to identify active hosts, open ports, running services, and network topology. We utilize both passive and active reconnaissance techniques to gather information about the target environment while minimizing potential impact.

Vulnerability Scanning and Analysis

Following discovery, we conduct detailed vulnerability scanning using industry-standard and proprietary tools to identify potential security weaknesses. All findings are manually verified to eliminate false positives and understand the real-world impact of each vulnerability.

Exploitation and Privilege Escalation

Identified vulnerabilities are carefully exploited using controlled methods to demonstrate actual risk. When initial access is achieved, we attempt to escalate privileges to determine the full extent of potential compromise. All exploitation activities are conducted with extreme care to avoid system disruption.

Post-Exploitation Analysis

Once access is obtained, we analyze the compromised systems to understand the potential impact of the breach. This includes reviewing sensitive data access, analyzing network positioning for lateral movement, and identifying additional security weaknesses only visible from an internal perspective.

Persistence and Exfiltration

We evaluate the ability to maintain long-term access and extract sensitive data, simulating techniques used by real threat actors. This helps identify gaps in detection and monitoring capabilities while demonstrating the potential business impact of a successful breach.

Documentation and Reporting

Throughout the engagement, we maintain detailed documentation of all activities, findings, and potential impacts. The final report includes:

- Executive summary for leadership
- Technical details of all discovered vulnerabilities
- Proof of concept evidence
- Strategic remediation recommendations
- Tactical guidance for addressing each finding

Appendix C: Tooling

The following tools were used during this assessment:

Tool	Purpose
Nmap	Network discovery and service enumeration
Nessus Professional	Automated vulnerability scanning
BloodHound / SharpHound	Active Directory attack path analysis
Impacket	Network protocol exploitation (secretsdump, ntlmrelayx, smbexec)
CrackMapExec / NetExec	AD lateral movement and credential validation
Responder	LLMNR/NBT-NS/mDNS poisoning and credential interception
Hashcat	Offline password hash cracking (GPU-accelerated)
Certipy	Active Directory Certificate Services enumeration and exploitation
Aircrack-ng / hcxdumptool	Wireless network capture and WPA/WPA2 assessment
Wireshark	Network traffic analysis
Metasploit Framework	Exploitation framework for PoC validation
Burp Suite Professional	Web application and API testing

Appendix D: Reporting and Closure

- The executive summary is written in non-technical language to ensure a broad understanding of the assessment results and any risks to the organization.
- Documentation of vulnerabilities, proof-of-concept (PoC) code, severity rating, impact, and recommendations for closing all vulnerabilities is included in Section V of the report.
- All reports are written based on standards set by NIST, CWE, CERT, SANS, and OWASP.
- Upon completion of the assessment, a debrief meeting is scheduled with key stakeholders to discuss findings and address immediate questions.
- The final report is delivered in PDF format with all sensitive information properly secured and encrypted during transmission.