



## Offensive Security Assessment

PUBLIC PORTFOLIO EDITION

# Network Penetration Test Report

A public, sanitized example of external-to-internal compromise analysis, Active Directory testing and remediation reporting.

PREPARED BY  
**Mitch Breton**

ASSESSMENT TYPE  
**External / Internal Network Penetration Test**

TARGET  
**Redacted / Representative Environment**

VERSION  
**Public Sanitized Edition 1.0**

### SANITIZED FOR PUBLIC DISTRIBUTION

Client and lab identities, IP addresses, credentials, exact payloads, account identifiers, canary values, screenshots and certification-specific metadata were removed or generalized. The assessment structure, technical themes, impact analysis and remediation guidance are preserved.

# What the assessment showed

EXECUTIVE RISK SUMMARY

Prepared for  
Representative Organization

6

CRITICAL

2

MEDIUM

1

LOW

Initial access through credential attack paths

Lateral movement through reused and stored secrets

Internal reconnaissance from an exposed server

High-privilege compromise of the Windows domain

Testing demonstrated that a chain beginning with public information and weak external authentication controls could be converted into internal access and eventually high-privilege domain compromise.

The dominant risk was not a single exploit. Credential hygiene, password reuse, exposed administration, missing segmentation and Active Directory configuration weaknesses amplified one another and made lateral movement progressively easier.

SCOPE & APPROACH

## What was tested

01

**External perimeter**  
Public information, exposed services and externally reachable administrative interfaces.

02

**Internal Windows environment**  
Authentication paths, SMB/RDP exposure, host configuration and lateral movement.

03

**Active Directory**  
Kerberos configuration, credential exposure and privilege boundaries.

METHODOLOGY

Net Phantom Security // Public Portfolio Artifact

Sanitized assessment sample

# How testing was performed

## 1 OSINT & attack-surface mapping

Identified public identity data, naming conventions and externally visible infrastructure.

## 2 External authentication testing

Evaluated rate limiting, password policy and administrative access controls.

## 3 Post-compromise discovery

Assessed credential storage, key material, server hardening and network reachability.

## 4 Internal enumeration

Validated credential reuse, service access and host-to-host trust relationships.

## 5 Active Directory testing

Reviewed Kerberos configuration and privilege-escalation paths.

## 6 Privilege validation

Demonstrated the business impact of exposed or embedded administrative secrets.

### POSITIVE CONTROLS

## Security strengths observed



### Hardened mail host

Direct root-level compromise of the exposed Linux service was not achieved through tested local escalation paths.



### Protected SSH key material

Recovered private keys were protected with passphrases rather than being completely unencrypted.



### Limited Domain Admin sprawl

Service accounts were not observed to be unnecessarily assigned Domain Admin membership.

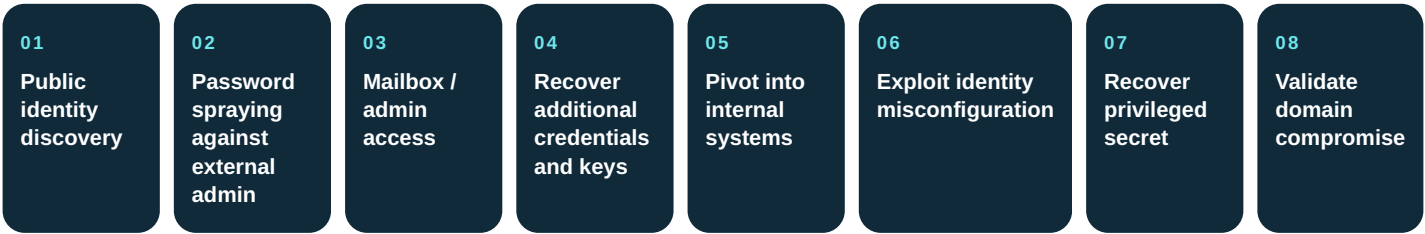
FINDINGS SUMMARY

# 9 documented security findings

| #  | Severity | Finding                                                                                                              |
|----|----------|----------------------------------------------------------------------------------------------------------------------|
| 01 | LOW      | <b>Public OSINT exposed employee and mail-service information</b><br>External attack surface                         |
| 02 | CRITICAL | <b>Insufficient authentication lockout enabled password spraying</b><br>Externally reachable administration          |
| 03 | CRITICAL | <b>Credentials and SSH keys were stored or transmitted in cleartext</b><br>Credential hygiene                        |
| 04 | MEDIUM   | <b>Insufficient endpoint controls enabled tooling and internal reconnaissance</b><br>Server hardening / segmentation |
| 05 | MEDIUM   | <b>Password reuse expanded access across internal services</b><br>Identity security                                  |
| 06 | CRITICAL | <b>Kerberos pre-authentication was disabled on multiple accounts</b><br>Active Directory                             |
| 07 | CRITICAL | <b>Plaintext credentials in deployment documentation enabled further compromise</b><br>Shared files / configuration  |
| 08 | CRITICAL | <b>Hardcoded administrative credentials enabled domain compromise</b><br>Application secrets                         |
| 09 | CRITICAL | <b>Legacy print service exposure enabled local privilege escalation</b><br>Windows patching                          |

ATTACK PATH

## How the weaknesses combined



# Technical observations and remediation

## FINDING 01

LOW

## Public OSINT exposed employee and mail-service information

OSINT

Reconnaissance

### What we found

Publicly available information disclosed employee naming patterns, corporate email conventions and the presence of externally reachable mail infrastructure.

### Why it matters

The information materially improved attacker targeting and enabled construction of username lists for follow-on authentication attacks.

### Recommended action

- Minimize unnecessary publication of employee contact patterns and administrative details.
- Monitor for exposed infrastructure metadata and credential leaks.
- Assume public identity data will be used for targeted authentication attacks.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 02

CRITICAL

## Insufficient authentication lockout enabled password spraying

Password Spraying

Rate Limiting

### What we found

A public-facing administrative login permitted a large number of authentication attempts without effective throttling or lockout controls.

### Why it matters

Weak credentials could be discovered through password spraying, providing an initial foothold and access to administrative functions.

### Recommended action

- Implement rate limiting, progressive delays and account lockout controls.
- Require MFA for externally reachable administration.
- Restrict administrative interfaces to trusted networks or VPN access where possible.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 03

CRITICAL

## Credentials and SSH keys were stored or transmitted in cleartext

Secrets Management

SSH

### What we found

Mail and user-accessible content contained passwords and private key material in cleartext locations that could be recovered after initial access.

### Why it matters

Compromised mailbox access could be converted into additional server access, allowing rapid expansion from one account to multiple systems.

### Recommended action

- Remove credentials from email, drafts, documentation and shared storage.
- Use a managed secrets vault and rotate exposed credentials and keys.
- Use strong passphrases and lifecycle controls for SSH keys.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 04

MEDIUM

## Insufficient endpoint controls enabled tooling and internal reconnaissance

File Upload

EDR

Segmentation

### What we found

A compromised internet-facing server accepted offensive tooling and provided network reachability that enabled internal host discovery.

### Why it matters

The exposed server functioned as a staging point for internal reconnaissance, increasing the blast radius of the initial compromise.

### Recommended action

- Apply endpoint protection and file-content controls appropriate to server roles.
- Place internet-facing services in segmented network zones.
- Restrict east-west connectivity from exposed systems to internal networks.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 05

MEDIUM

## Password reuse expanded access across internal services

Credential Reuse

Lateral Movement

### What we found

Credentials recovered from one service were valid against additional internal systems and protocols.

### Why it matters

A single credential compromise could be reused for service discovery and lateral movement, significantly increasing compromise scope.

### Recommended action

- Enforce unique passwords across services and accounts.
- Use MFA and conditional access for privileged services.
- Detect authentication of the same identity across unusual hosts or protocols.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 06

CRITICAL

## Kerberos pre-authentication was disabled on multiple accounts

AS-REP Roasting

Kerberos

### What we found

Multiple domain accounts were configured without Kerberos pre-authentication, allowing encrypted authentication material to be requested and attacked offline.

### Why it matters

Weak account passwords could be recovered without prior authentication and then used for internal access or privilege escalation.

### Recommended action

- Require Kerberos pre-authentication for all accounts unless a documented exception exists.
- Use long, random passwords for service identities and rotate them regularly.
- Monitor for anomalous AS-REQ/AS-REP activity.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 07

CRITICAL

## Plaintext credentials in deployment documentation enabled further compromise

Default Credentials

Documentation

### What we found

Accessible configuration and setup documentation contained reusable service credentials that remained valid after deployment.

### Why it matters

An attacker with access to shared files could pivot directly into additional systems using documented credentials.

### Recommended action

- Remove default credentials from deployment documents after installation.
- Rotate setup credentials immediately after provisioning.
- Restrict access to sensitive installation and configuration material.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 08

CRITICAL

## Hardcoded administrative credentials enabled domain compromise

Hardcoded Secrets

Domain Admin

### What we found

Administrative credentials were embedded in a locally deployed application and could be recovered from the packaged application artifacts.

### Why it matters

Recovering the embedded secret provided privileged access sufficient to compromise the domain environment.

### Recommended action

- Remove hardcoded credentials from application code and packages.
- Use managed secrets with short-lived access tokens or service identities.
- Rotate all exposed administrative credentials and audit downstream use.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

## FINDING 09

CRITICAL

# Legacy print service exposure enabled local privilege escalation

Patch Management

CVE-2021-34527

## What we found

Multiple Windows hosts exposed a known print-spooler vulnerability associated with unsafe legacy configuration and incomplete patching.

## Why it matters

Successful exploitation could create administrative access on affected hosts and further accelerate lateral movement.

## Recommended action

- Apply current vendor security updates and disable unnecessary Print Spooler service exposure.
- Prioritize patching for known exploited vulnerabilities.
- Continuously inventory and validate host patch state.

**Public artifact note:** exact payloads, credentials, target identifiers and evidentiary screenshots have been intentionally removed or generalized.

# What should be dealt with first

## 1 Lock down exposed administration

Move management interfaces behind VPN/trusted access, require MFA and enforce throttling/lockout.

## 2 Rotate and centralize secrets

Treat all discovered passwords, keys and embedded credentials as compromised; migrate to managed secrets.

## 3 Eliminate password reuse

Use unique passwords, stronger service-account controls and modern local administrator password management.

## 4 Segment internet-facing systems

Place exposed services in a DMZ and sharply limit east-west access to internal hosts.

## 5 Harden Active Directory

Require Kerberos pre-authentication, strengthen service-account passwords and monitor anomalous authentication.

## 6 Patch and reduce attack surface

Prioritize known exploitable vulnerabilities and disable unnecessary legacy services.

## About this artifact

This is a reconstructed public-facing version of a technical assessment. It is intentionally safer to publish than a black-box overlay redaction: removed details are not present in the PDF's underlying text or images. The original confidential source reports remain unchanged.