Internal Network Penetration Test

For: Sample Company

Submitted by:

SecureTrust Cyber

https://securetrust.io

Table of Contents

Executive Summary

SecureTrust Cyber, LLC (SecureTrust) performed an internal and external penetration test of in scope items provided by Sample Company from February 27th, 2023, through March 3rd, 2023. This report describes penetration testing that represents a point-in-time snapshot of the network security posture of the scope in question, which can be found in the following section.

Overall, there were ten total findings during the external assessment – four high, four medium, and two low. One of the high-risk findings, excessive local administrator rights, leads to a full domain compromise from the starting point of a normal domain user. Three other vulnerabilities, weak active directory password policy, overprivileged access, and lack of multifactor authentication (MFA) on external VPN connections, also pose a high risk to the organization.

In the case of the external VPN not requiring MFA, if a user's credentials were reused on a separate service and that service was breached, at attacker could now access to Sample Company's internal network. From there, simple enumeration would enable them to escalate privileges, obtain domain administrator credentials, and compromise the entire internal network. This method of attack is evident in many of the highly publicized breaches that are seen regularly in the news.

Analysis of Overall Security Posture

The overall risk to Sample Company from an internal perspective is HIGH. This determination is made upon the risk inherent in the usage of local administrator rights on multiple hosts combined with a weak password policy. Upon accessing the internal network, a malicious actor would face minimal resistance in moving laterally through the network and escalating privileges to domain administrator. This would enable the malicious actor to access critical business information and customer data.

The overall risk to Sample Company from an external perspective is HIGH. This determination is made based upon the lack of multifactor authentication on external VPN access. If a user's VPN credentials become compromised, MFA would protect the internal network from access by a malicious actor. It was noted that multiple passwords for Sample Company employees were found in breaches of other organizations, but none of those passwords allowed VPN access. This method of gaining access to internal networks is frequently used due to the low technical requirements and the prevalence of credential reuse.

Key Recommendations

There are several key recommendations that would significantly enhance the security posture of Sample Company.

- Increase the strength of the active directory password policy and force a password change for all users.
- Enable 2FA on VPN logins.
- Modify policies to disable local administrator access on hosts in question.
- Audit and decrease user permissions across the network.

Testing Methodology

Testing commenced by utilizing the industry standard vulnerability scanner Nessus Professional and/or similar scanning tools to locate live hosts and services on the in-scope IP addresses provided. The output of this tooling was then manually examined, and the hosts and services were manually enumerated to uncover any missed vulnerabilities and weaknesses. Additionally, automated tooling and manual enumeration were used to identify default credentials used throughout the network, and open-source intelligence gathering was used to find live credentials exposed on the internet.

Testers utilized their *test* user credentials to move laterally throughout the network. Upon discovering that all domain users were local administrator of multiple hosts on the network, testers were able to utilize these administrator privileges to obtain the credentials of domain administrators. This allowed unfettered access to most hosts within the environment, including data stores and POS devices.

A qualitative risk analysis was conducted using NIST Special Publication (800-30 R1) - Guide for Conducting Risk Assessments to map findings to a risk rating. This model is used to define the likelihood and impact of a given vulnerability. For additional detail about how the risk ratings were determined see Appendix B.

Summary of Findings

Finding	Severity
Local Administrator Rights Leading to Domain Compromise	High
Weak Password Policy	High
Missing MFA on VPN Access	High
Over-privileged Access	High
SMB Signing Disabled	Moderate
VMWare vCenter Out of Date	Moderate
IPMI Password Hash Disclosure	Moderate
SNMP Agent Default Community Name (public)	Moderate
Unauthenticated Access to Printers via HTTP and Telnet	Low
Grandstream HT818 VOIP Gateway Default Credentials	Low

Detailed Findings

Excessive Local Administrator Rights Leading to Domain Compromise

Current Rating	CVSS
Critical	10

Finding Summary:

Testers were able to successfully authenticate to multiple hosts on the internal network with their testing credentials. On these hosts, it was discovered that the *test* user was a local administrator. This allowed stored credentials on these hosts to be obtained.

In this effort, the domain admins *[redacted]admin* and *[redacted]service* password hashes, along with many others were obtained. This enabled full access and full control over the internal active directory domain. This includes DBO access to the MSSQL instance at 192.168.0.32 which appears to contain business and customer information.

Notably, the *test* account was not local administrator on the machine they were allotted, but it appears that *all domain users* are local administrator on multiple hosts. These hosts are listed in the affected resources section below.

Evidence:

```
PS P:\Users\pentest> Get-LocalGroupMember -group 'Administrators'

ObjectClass Name                          PrincipalSource
----------- ----                          ---------------
Group       [redacted]\Domain Admins      ActiveDirectory
Group       [redacted]\Domain Users       ActiveDirectory
User        WIN10STAFF-12\Administrator   Local
User        WIN10STAFF-12\[redacted]admin Local
User        WIN10STAFF-12\[redacted]service Local
```

Figure 1: Local admin group on 192.168.0.113

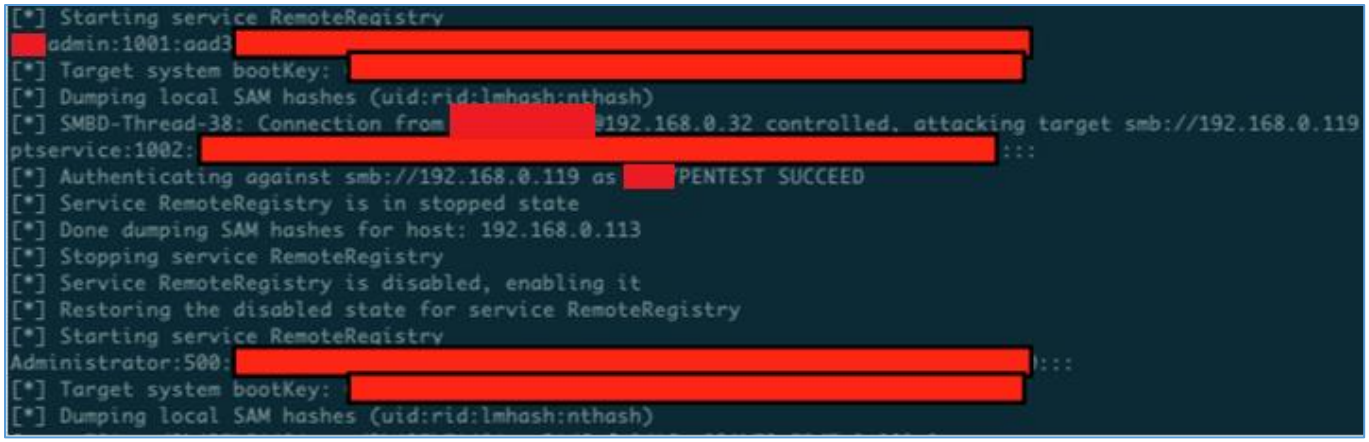

Figure 2: Testers successfully authenticating to multiple hosts on the network and dumping hashes from the registry.

Affected Resources:

192.168.0.113, 192.168.0.115, 192.168.0.119, 192.168.0.122, 192.168.0.130, 192.168.0.137, 192.168.0.139, 192.168.0.140, 192.168.0.144, 192.168.0.167

Recommendations:

Remove local administrator access for domain users on these hosts.

References:

https://SecureTrust.io/local-administrator-accounts

Weak Password Policy

Current Rating	CVSS
High	8

Finding Summary:

Testers determined the domain password policy of the active directory environment to be weak. Namely, a password length minimum of 7 characters is too low. Passwords of this length are easily guessed and/or the hashes are easily cracked.

Evidence:

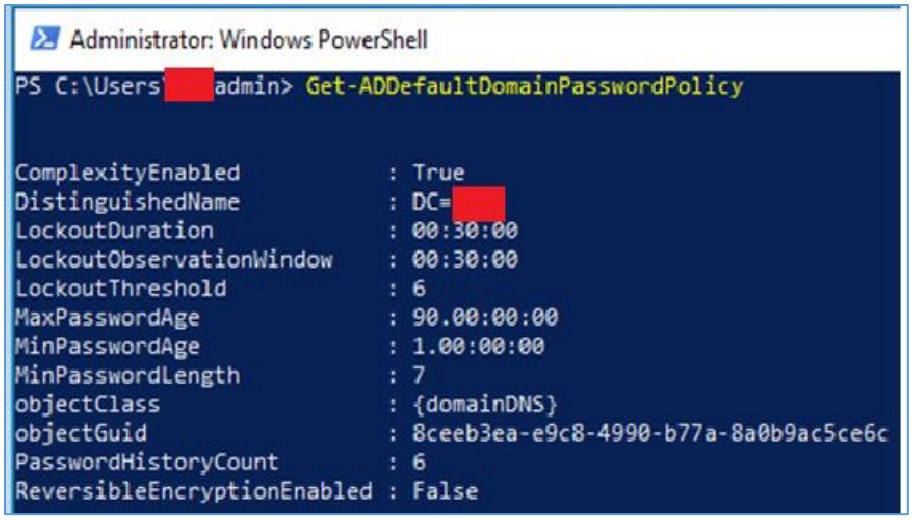

Figure 3: Password policy as seen via the Get-ADDefaultDomainPasswordPolicy command.

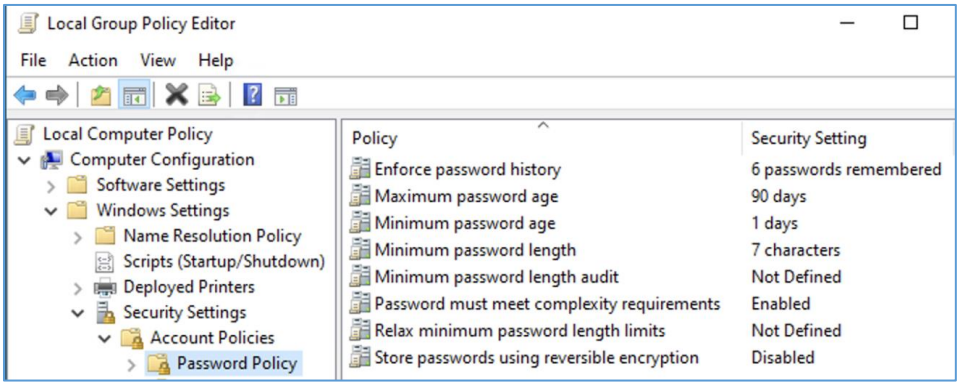

Figure 4: Password policy as seen in the group policy editor.

After compromising the domain controller, the testers dumped the ntds.dit file, containing domain usernames and their password hashes. The testers audited the password strength by conducting offline password cracking techniques. Using commonly available wordlists, the testers were able to crack 27 passwords, including a domain administrator account.

Affected Resources:

Internal active directory users.

Recommendations:

We recommend a policy requiring a minimum password length of 12 characters. Update the password policy and then force a password change for all users as quickly as possible.

References:

https://cwe.mitre.org/data/definitions/521.html

Lack of MFA on VPN Access

Current Rating	CVSS
High	8

Finding Summary:

Testers noted that VPN access does not require multifactor authentication. In the case of compromised credentials, an attacker would then have unfettered access to the internal network.

Affected Resources:

vpn.SampleCompany.com

Recommendations:

Enable multifactor authentication on all authentication services.

Over-Privileged Access

Current Rating	CVSS
High	7.5

Finding Summary:

Testers identified overly permissive accounts within the network. Non-domain administrator accounts were able to authenticate to the domain controller. Additionally, it was determined that there are a total ten domain administrators.

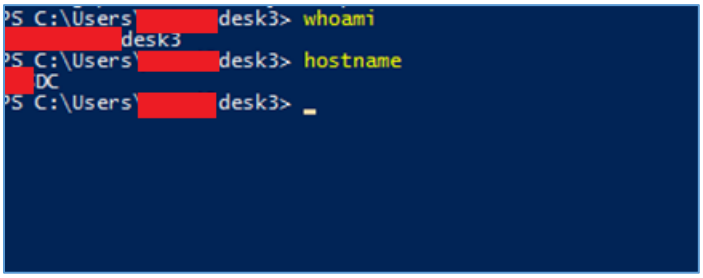

Figure 5: A non-domain admin account successfully authenticated the DC

Affected Resources:

Domain Administrators

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Recommendations:

The principle of least privilege is intended to prevent "over-privileged access" by users, applications, or services to help reduce the risk of exploitation should user credentials be compromised by an outside attacker or malicious insider. Thus, users are granted only enough authority for an entity to complete a specific task or job.

Evaluate the need for a user to be a domain administrator in an effort to reduce the total number of these users wherever possible. Modify access rights to the domain controller to only allow authentication for users that absolutely need to access the domain controller.

SMB Signing Disabled

Current Rating	CVSS
Medium	5.5

Finding Summary:

Testers found multiple hosts on the internal network with SMB signing disabled. This allows attackers to perform man-in-the-middle attacks to move laterally and elevate privileges.

Evidence:

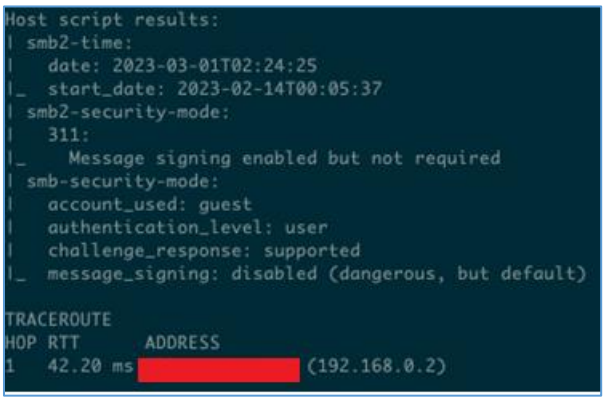

Figure 6: Sample nmap output showing smb signing disabled for host 192.168.0.2

Affected Resources:

192.168.0.2, 192.168.0.19, 192.168.0.32, 192.168.0.33, 192.168.0.34, 192.168.0.111, 192.168.0.113, 192.168.0.115, 192.168.0.119, 192.168.0.120, 192.168.0.121, 192.168.0.122, 192.168.0.125, 192.168.0.126, 192.168.0.130, 192.168.0.137, 192.168.0.139, 192.168.0.140, 192.168.0.144, 192.168.0.151, 192.168.0.152, 192.168.0.167, 192.168.0.181, 192.168.0.187, 192.168.0.191, 192.168.0.200, 192.168.50.3, 192.168.50.9

Recommendations:

Enable SMB signing.

References:

https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

https://techcommunity.microsoft.com/t5/itops-talk-blog/how-to-defend-users-from-interception-attacks-via-smb-client/ba-p/1494995

VMWare vCenter Out of Date

Current Rating	CVSS
Medium	5

Finding Summary:

Testers found the vCenter instance running at 192.168.0.34 to be out-of-date and susceptible to a significant number of vulnerabilities.

Evidence:

```
VMware vCenter version     : 6.7
Installed build            : 14792528
Fixed build                : 18485166
```

Figure 7: Nessus output detailing the current version of vCenter.

Affected Resources:

192.168.0.34

Recommendations:

Update to the latest version and build of vCenter.

References:

https://SecureTrust.io/owasp-top-ten-vulnerable-and-outdated-components

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

https://www.vmware.com/security/advisories/VMSA-2021-0027.html

IPMI Password Hash Disclosure

Current Rating	CVSS
Medium	5.5

Finding Summary:

Testers found the ASRockRack IPMI instance at 192.168.0.201 host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC.

The password hash was obtained, but the hash was unable to be cracked.

Evidence:

```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > set rhosts 192.168.0.201
rhosts => 192.168.0.201
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 192.168.0.201:623 - IPMI - Hash found: admin:b036e8148fbf5c00033888e
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 8: Testers used the Metasploit module to dump the IPMI admin hash.

Affected Resources:

192.168.0.201

Recommendations:

There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0.

Suggested mitigations include:

- Disabling IPMI over LAN if it is not needed.
- Using strong passwords to limit the successfulness of off-line dictionary attacks.
- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

References:

https://www.cvedetails.com/cve/CVE-2013-4786

SNMP Agent Default Community String (public)

Current Rating	CVSS
Low	3.5

Finding Summary:

Testers found the host at 192.168.253.20 using the default SNMP Community Name – *public*. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Evidence:

```
(user㉿MacBook-Pro)-[~]$ snmpwalk -v 2c -c public 192.168.253.20
SNMPv2-MIB::sysDescr.0 = STRING: Palo Alto Networks PA-220 series firewall
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.25461.2.3.38
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (364953265) 42 days, 5:45:32.65
SNMPv2-MIB::sysContact.0 = STRING: Not Set
SNMPv2-MIB::sysName.0 = STRING: KMS-PEO-PA-220
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysServices.0 = INTEGER: 127
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (11) 0:00:00.11
```

Figure 9: Testers used the community string public to authenticate to snmp and list information.

Affected Resources:

192.168.253.20

Recommendations:

Change the default community string or disabled SNMP if it is not used. Utilize SNMP version 3 whenever possible.

References:

https://www.rapid7.com/db/vulnerabilities/SNMP-READ-0001

Unauthenticated Access to Printers via HTTP and Telnet

NIST Score Summary:

Current Rating	CVSS
Low	3

Finding Summary:

Testers found multiple printers on the internal network allowed unauthenticated Telnet and HTTP access. Printers may be used by attackers to move laterally through the network or to cause service disruption.

Evidence:

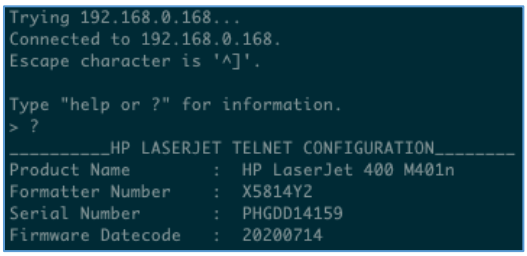

Figure 10: Testers logged in to a printer via Telnet.

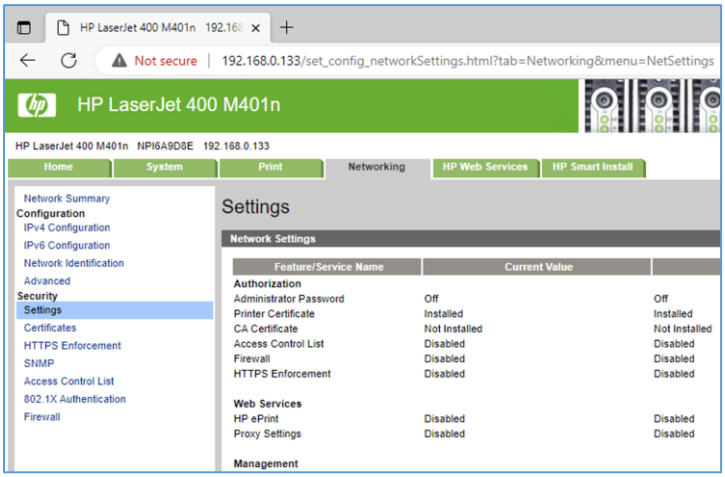

Figure 11: Testers logged in to a printer via the web interface.

Affected Resources:

192.168.0.133, 192.168.0.141, 192.168.0.149, 192.168.0.168

Recommendations:

It is recommended to disable Telnet if possible. Set an administrator password via the GUI or Telnet.

References:

https://SecureTrust.io/credentials-gone-wild

https://truedigitalsecurity.com/blog/this-printer-configuration-can-compromise-your-entire-windows-domain

Grandstream HT818 VOIP Gateway Default Credentials

NIST Score Summary:

Current Rating	CVSS
Low	3

Finding Summary:

Testers were able to authenticate the Grandstream device at 192.168.0.110 with default credentials *user:123*. A malicious actor would be able to disrupt VOIP operations for the organization.

Evidence:

Figure 12: Testers logged into the Grandstream VOIP Gateway.

Affected Resources:

192.168.0.110

Recommendations:

Change the password on this device.

References:

https://SecureTrust.io/credentials-gone-wild/

CVSS v3.0 Reference Table

Qualitative Rating	CVSS Score
None/Informational	N/A
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table 1 : Common Vulnerability Scoring System Version 3.0