SECUREU
WE MAKE SECURITY ACCESSIBLE

NETWORK PENETRATION TESTING

SECURITY REPORT

DEMO CORP

DATE : DD MONTH YYYY

VERSION : 1.0

Confidential Document

Email : contact-us@secureu.in **Phone : +91 8010450348** **www.secureu.in**

CONTENTS ...

1. Confidentiality Statement

This document is the exclusive property of Demo Corp and SECUREU. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires the consent of both Demo Corp and SECUREU.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2. Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

3. Contact Information

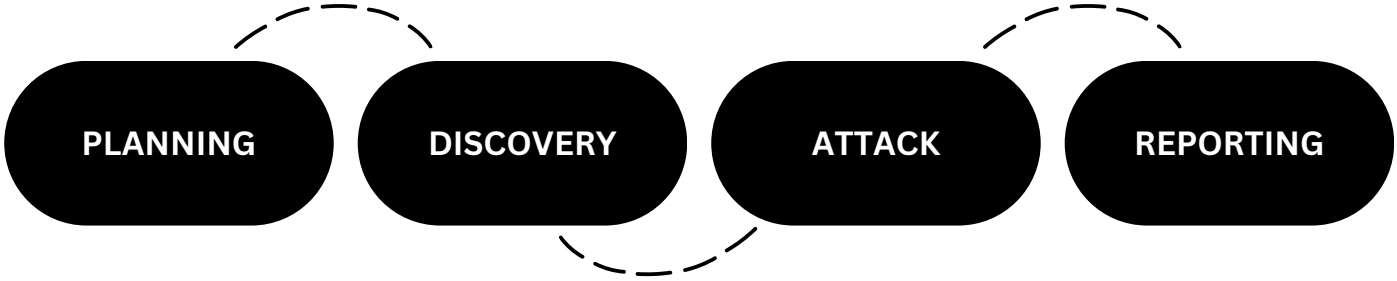
Name	Title	Contact Information
John	Lead Penetration Tester	john@secureu.in
Albert	Security Engineer	albert@secureu.in
Gilbert	Penetration Tester	gilbert@secureu.in

4. Assessment Overview

From <month> xth, 20XX to <month> yth, 20XX SECUREU attempted to evaluate the security posture of the network infrastructure of Demo Corp and compared it to the current industry best practices by performing a network penetration test

Phases of penetration testing activities include the following:

- **Planning** – Customer goals are gathered and rules of engagement are obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discoveries upon new access.
- **Reporting** – Document all found vulnerabilities, exploits, failed attempts, and company strengths and weaknesses.



5. Assessment Components

5.1. Network Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the assets to identify potential vulnerabilities.

6. Finding Severity Ratings

The following table defines levels of severity and the corresponding CVSS score range used throughout the document to assess vulnerability and risk impact.

SEVERITY	CVSS V3 SCORE RANGE	DEFINITIONS
Critical	9.0-10.0	**Exploitation:** • Exploitation is straightforward. • Results in system-level compromise. **Plan of Action:** • Patch immediately.
High	7.0-8.9	**Exploitation**: • Exploitation is more difficult. Could cause elevated privileges. • Potential to cause loss of data or downtime. **Plan of Action**: • Patch as soon as possible.
Medium	4.0-6.9	**Exploitation:** • Vulnerabilities exist but are not exploitable. • Might require extra steps to make the vulnerability exploitable. **Plan of Action**: • Patch after high-priority issues has been resolved.
Low	0.1-3.9	**Exploitation:** • Vulnerabilities are non-exploitable. • Mitigation would reduce an organization's attack surface. **Plan of Action:** • Patch during the next maintenance window.
Informational	N/A	• No vulnerability exists. • Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7. Risk Factors

Risk is measured by two factors: Likelihood & Impact

7.1. Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

7.2. Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity and availability of client systems and/or data, reputational harm, and financial loss.

8. Scope

ASSESSMENT	DETAILS
Network vulnerability scan	192.168.0.1-255

8.1. Scope Exclusions

SECUREU did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

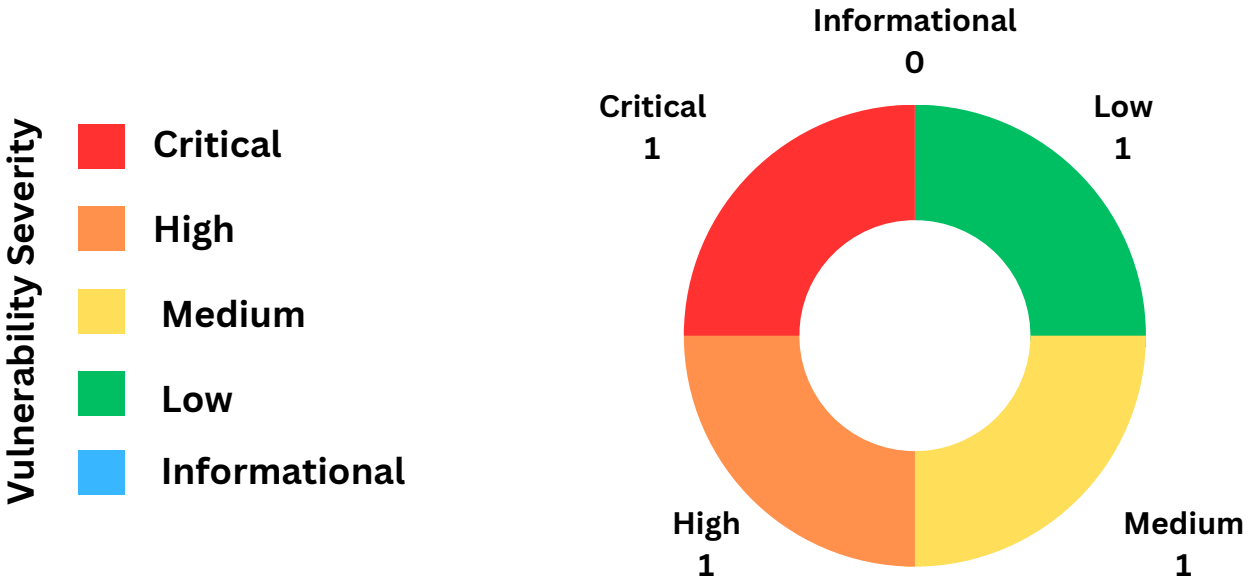
All other attacks not specified above were covered in penetration testing of the domain

9. Executive Summary

SECUREU evaluated Demo Corp's network security posture through an internal penetration test from <month> xth, 20XX to <month> Yth, 20XX. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Security Rating

VULNERABILITY DISTRIBUTION



9.1. Scoping and Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

9.2. Testing Summary

The network assessment evaluated **democorp's** security posture. The SECUREU team performed vulnerability scanning against the systems mentioned in the scope.

LLMNR and NBT-NS protocols were **found to be enabled** which are **vulnerable to poisoning attacks** that **result** in the **disclosure of user credentials and facilitate the further expansion of the attack surface**.

Our team was also able to **mount unauthenticated NFS shares** on one system. The mounted share looked like a webroot directory which is a serious security loophole as an attacker can upload backdoors and web shells on that share.

It was also found that **Redis servers** installed across **the network do not prompt for authentication before any interaction**. This can help an **attacker to gain sensitive information stored** in those servers which **can facilitate him to maximize the impact** of the attack.

Along with this, our team discovered **that the Polycom portal uses default credentials** which is a **serious security issue as this misconfiguration can provide full access to the telecommunication system.**

10. Key Strengths and Weaknesses

The following identifies the **key strength**s found during the assessment:

- Use of technologies that have no exploits available out in the open.

The following identifies the **key weaknesses** found during the assessment:

- Good security practices are not being followed.
- Use of outdated technologies.

11. Vulnerability Distribution Table

The following table illustrates the vulnerabilities found by severity and recommended remediations:

FINDINGS	SEVERITY	RECOMMENDATIONS
INPT-001:LLMNR and NBT-NS protocols enabled	**Critical**	Disable LLMNR and NBT-NS. Both of them should be disabled because if only LLMNR is disabled, it will automatically attempt to use NBT-NS instead.
INPT-002:NFS shares mountable without authentication	**High**	Configure NFS on the remote host so that only authorized hosts can mount.
INPT-003: Polycom Administrative Panel Default Credentials	**Medium**	Change the default password of the administrative user.
INPT-004: Unauthenticated Redis servers	**Low**	Enable the 'requirepass' directive in the “redis.conf” configuration file.

12. Network Penetration Testing FIndings

INPT-001: LLMNR and NBT-NS protocols enabled (Critical)

DESCRIPTION:	LLMNR and NBT-NS protocols are used in name resolution on the network. When enabled, if a user or host fails DNS name resolution, the victim will then broadcast an LLMNR or NBT-NS request to see if other computers on the network know where the DNS entry is located. An attacker can respond to these broadcasts and get a NTLMv2 hash from the victim along with his username. These hashes can be extracted and then cracked to reveal credentials.
IP:	192.168.0.24, 192.168.0.33 and 192.168.0.42
REFERENCES:	1. LLMNR and NBT-NS poisoning(Cynet) 2. LLMNR poisioning and SMB relay

Evidence

Below shows the hash capture of Domain Administrator user DemoCorp\johndoemanadmin:

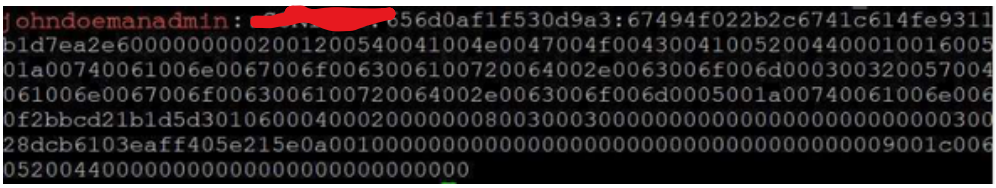


Fig 1: NTLMv2 hash captured

Risk

- **Likelihood**

  The likelihood of LLMNR and NBT-NS poisoning attacks depends on the network's security measures and the attacker's motivations. These attacks are more likely to occur in less secure networks and when an attacker has gained access to the network. In general, the **likelihood is high**.

- **Impact**

  LLMNR and NBT-NS poisoning attacks can have a significant impact. **Attackers can intercept sensitive information**, such as usernames and passwords, and potentially use it for malicious purposes. **This attack can also be used to launch other types of attacks**, such as man-in-the-middle attacks or ransomware attacks. The **impact can be severe if the attacker gains access to highly sensitive information.**

Remediation

it is recommended to disable LLMNR and NBT-NS protocols if they are not needed, or to use alternative protocols like DNS. It is also important to implement strong network security measures, such as secure authentication and encryption, and to monitor network traffic for signs of suspicious activity

- **More Information**
  - LLMNR Poisoning and how can you prevent it?(MakeUseOf)
  - LLMNR poisoning and how to secure against it(systemweakness)

INPT-002: NFS shares mountable without authentication (High)

DESCRIPTION:	**NFS shares exported** by the remote server **could be mounted without authentication**. It is possible to read and write files on the remote host.
IP:	192.168.0.16
REFERENCES:	1. Exploiting NFS share 2. Exploiting a Misconfigured NFS Share

Evidence

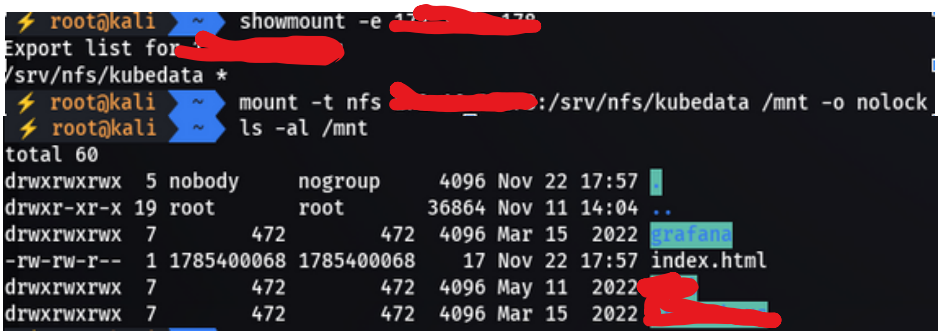


Fig 2: Mounting shares and browsing

The attempt to mount NFS share without a password was successful (see fig 2). The NFS share was allowing R/W access which is a serious security issue.By the looks of it, the mounted share looked like a webroot directory which could have serious implications which are discussed more below in the impact.

Risk

- **Likelihood**

  As this vulnerability has very low complexity to exploit, it is **highly likely** for an attacker to find and exploit this vulnerability.

- **Impact**

  Unauthenticated NFS shares can seriously **impact confidentiality**. The **NFS share** mounted in this case **is a web-root directory**, an **attacker can upload a backdoor** webshell to this share and execute it via the client side from the browser **thus escalating this vulnerability to complete Remote Code Execution** which can seriously impact the CIA triad.

Remediation

Configure NFS on the remote host so that only authorized hosts can mount.

- **More Information**
  - General guidelines for securing Network File System - IBM Documentation
  - Security and NFS (tldp.org)

INPT-003: Polycom Administrative Panel Default Credentials (Medium)

DESCRIPTION:	The web administrative panel for the Polycom devices use default administrative credentials.
URL:	192.168.0.50
REFERENCES:	1. HSTSpreload 2. Wikipedia HSTS

Evidence

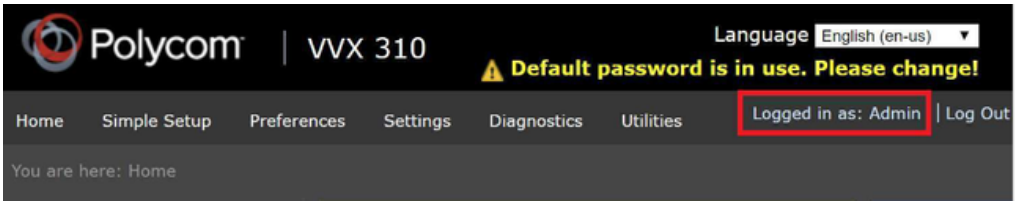


Fig 3: Logged in using default credentials

Risk

- **Likelihood**
  It is **highly likely** for this attack to take place as the portal uses default credentials.

- **Impact**
  Access to the Polycom portal allows for an attacker to control all aspects of the device, including routing, ring tones and more.

Remediation

Change the default password of the administrative user.

- **More Information**
  - How to change default password od polycom portal

INPT-004: Unauthenticated Redis servers (Low)

DESCRIPTION:	**Redis servers** across the network **do not require credentials for authentication.**
URL:	192.168.0.7, 192.168.0.17, 192.168.0.20 and 192.168.0.21
REFERENCES:	1. Software Security | Unauthenticated Service: Redis 2. RCE on Unauthenticated Redis server | by Trevor saudi | Medium

Evidence

It was found that the Redis servers listed in the IPs above do not require authentication to execute commands (see fig 4). We are including only one machine for evidence but all the other IPs listed above were found to be vulnerable to the same vulnerability.

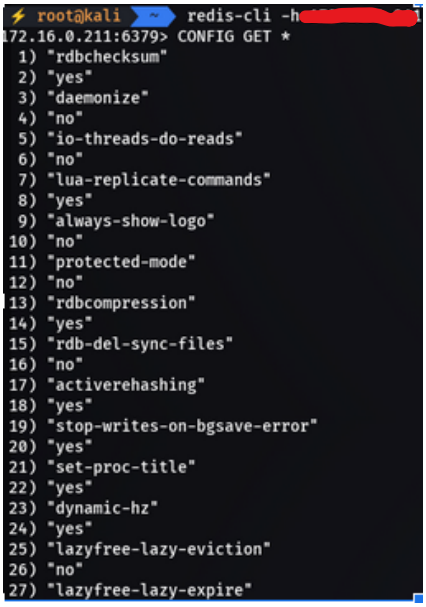


Fig 4: Unauthenticated Redis servers

Risk

- **Likelihood**

  As this vulnerability has very low complexity to exploit, it is **highly likely** for an attacker to find.

- **Impact**

  Redis servers are used to store cache, keys, etc. A **breach of this data** can be catastrophic for the organization. An **attacker can even gain Remote Code execution** from unauthenticated Redis servers and completely breach the security of the target.

Remediation

Enable the 'requirepass' directive in the “redis.conf” configuration file.

- **More Information**
  - How to set password for Redis? - Stack Overflow
  - AUTH | Redis

SECUREU

WE MAKE SECURITY ACCESSIBLE

Questions? Contact us at
Email : contact-us@secureu.in Phone : +91 8010450348