Ex160 Test Report Submission

Gary Jones

Contents

Executive Summary

Project Overview

Based on the penetration test contract, agreed upon by all parties prior to the start of active investigation into the security of the artstailor.com network, the purpose of this project is to determine the presence of any vulnerabilities to the best of our ability. This assessment is required prior to the launch of the artstailor.com web application. This project will provide mitigation strategies to address any vulnerabilities found and in this pursuit the Art's Tailor Shop has agreed to the investigation of any physical or software applications that may be relevant, up to and including the use of phishing and social engineering tactics on personnel.

Goals

The goal of this project was to identify possible security issues with the artstailor.com network and provide mitigation strategies for any security flaws found.

Risk Ranking/Profile

Administrator access to the full artstailor.com network can be obtained through the external environment. This includes access user credentials, sensitive files, and administrator privileges to inner network routers. The exploits used during this process are readily available online and as such the reproduction of the exploits used in this project are a persistent threat until such time as they are addressed. As such, the risk ranking is Critical or alternatively the risk ranking has a DREAD score of 9.

Summary of Findings

The exploits used throughout this exercise are those well documented online and are a result of using outdated software or misconfigurations in network communication. Those exploits used that were not a product of outdated software resulted from human error where simple repetitive passwords were used across systems or where credentials were hard-coded in accessible applications.

Recommendation Summary

The primary recommendation from this project is that the Art's Tailor Shop should update all software run on any machine connected to the artstailor.com network to the latest version available. In addition employees should be trained on proper security for their passwords which includes increasing their complexity and not using the same passwords across devices and applications. In

addition credentials should be hard coded into software applications. Finally HTTPS should be used universally through all connections when operating on the internet.

Technical Report

Introduction

Finding: *Ex010:*

Risk Rating

The risk rating of this vulnerability is low. It revolves around the manual searching of known files and uses normal linux commands. This requires direct access to the system.

Vulnerability Description

Within the kali VM two sensitive files were identified. The first file identified was found by searching through the directory tree with the find command as the file name was integrated in the filename. The second file was identified by looking at the active processes.

Finding: *Ex020:*

Risk Rating

The risk rating of this vulnerability is medium. It revolves around gaining access personal information about people related to the Art's Tailor Shop and subsequently the extent to which that person is vulnerable to social engineering techniques.

Vulnerability Description

With the use of open source information I was able to track down the public profile and physical location of the provided target. To be more precise, the information found online enabled identification of the mortgagee for a house purchased in May of 1995 and the people they sold the house to in 2001.

Confirmation method

The information obtained was confirmed through the use of public databases and the information they provide to see the relevant legal documents.

Mitigation or Resolution Strategy

Train personnel about standard social engineering techniques. How to identify them and deal with them when they come up.

Finding: *Ex030:*

Risk Rating

The risk ranking of this vulnerability is medium as ex-filtration of sensitive information from the inner router is dependent on vulnerabilities from the outer router. However, identification of all associated networks are documented online and reproducibility of these findings are likely to occur by other parties.

Vulnerability Description

By using the fierce domain scanner several ip addresses were found in association with artstailor.com including ns.artstailor.com, mail.artstailor.com, inner-outer.artstailor.com, pdc.artstailor.com, pop.artstailor.com, and books.artstailor.com. In addition to these finding several subdomains were identified which should have remained non-visible such as costumes.artstailor.com, linuxserver.artstailor.com, KEY005-TrvlNmWThZ4Aj2EDyYQx1a.artstailor.com, ceo.artstailor.com, and devbox.artstailor.com. In these cases if the router is port forwarded then the private artstailor.com network can be communicated with by the external environment.

Confirmation method

When any of the networks discussed above are pinged there should not be a response

Mitigation or Resolution Strategy

This problem can be mitigated through requiring a VPN or allowing only certain IP addresses to access the network.

Finding: *Ex050:*

Risk Rating

The risk of this vulnerability is Critical as it allows a backdoor into the system and as the information for this exploit is online it can be reproduced by third parties.

Vulnerability Description

With the use of searchsploit two risks were identified. The first was a backdoor command found in the vsftpd 2.3.4 software used on the network which is a major risk as it can be exploited to gain access to the system and the second is a local privilege escalation software present in the Apache 2.4.17 software which is a medium risk as it can be exploited once access to the system has been gained.

Confirmation method

This vulnerability can be confirmed to exist by determining if the version for VSFTPD is 2.3.4.

Mitigation or Resolution Strategy

This vulnerability can be addressed by updating the VSFTPD software to current standards and not allowing root privileges in its configuration settings.

Finding: *Ex060:*

Risk Rating

The risk of this vulnerability is Critical as it allows third parties to ex-filtrate user credentials that have a ':)'..

Vulnerability Description

Through the use of Nessus the vsftpd Smiley Face Backdoor vulnerability was identified which allows the ex-filtration of credentials that have a ':)'. Alongside this vulnerability it was found that the vsftpd 2.3.4 backdoor could be used with metasploit to gain access to the system. Through these exploits the file system on www.artstailor.com was compromised and access to the system files were granted.

Confirmation method

This vulnerability can be confirmed to exist by determining if the version for VSFTPD is 2.3.4.

Mitigation or Resolution Strategy

This vulnerability can be addressed by updating the VSFTPD software to current standards.

Finding: *Ex070:*

Risk Rating

This vulnerability is medium as it allows backdoor access to the network and that an overflow buffer can be used to augment executable commands thus giving third parties direct access into the network. Despite allowing access to the network reproducing the vulnerability using online resources are unlikely to occur.

Vulnerability Description

A backdoor was identified as being built into the www.artstailor.com network on port 1337 and due to a buffer overflow issue when inputting the administrators username the command list is able to be changed. Through this vulnerability it was found that any command could be executed including those which grant shell access thus providing remote access from external sources.

Confirmation method

Connect to the backdoor and try to execute a buffer overflow when inputting the administrator credentials. After 16 characters the commands the buffer will overflow if still available.

Mitigation or Resolution Strategy

The backdoor should be removed. Alternatively a dynamic buffer should be used, or the BUFLEN in the fgets command should be replaced with NAMELEN.

Finding: *Ex080:*

Risk Rating

Because the default credentials for pfSense were never changed any user with access to the network can modify the network configurations. For this reason this vulnerability is critical.

Vulnerability Description

By utilizing the sprayingtoolkit the tester was able to identify the username and password of an active user through https://mail.artstailor.com and then gain access to the remote desktop. In addition due to an open port on the innerouter the tester was able to gain access to the router settings and make modifications to the infrastructure configurations.

Confirmation method

This vulnerability can be confirmed to exist through attempting to log into pfSense with default credentials.

Mitigation or Resolution Strategy

This vulnerability can be removed by changing the default credentials of pfSense.

Finding: *Ex090:*

Risk Rating

The risk of this vulnerability is High because it allows execution of malicious code by any third party and its documentation is readily available online. However, this exploit is available only on Costumes.artstailor.com

Vulnerability Description

It was found that the Windows 10 software was vulnerable to the Background Intelligent Transfer Service (BITS). This is because Windows 10 allows users to change the path to the binary and thus allow malicious code into the system upon system restart. By connecting to the host and using PowerDown script an administrator account was created. From here the system was further compromised by being able to turn off the real time virus protection and utilized mimikatz.exe to locate and log various hashes from the system.

Confirmation method

This vulnerability can be confirmed by looking at the configuration of BITS and looking for ”SERVICE ALL ACCESS” for authenticated users.

Mitigation or Resolution Strategy

This vulnerability can be removed by only letting root personel to change the BITS configurations.

Finding: *Ex0a0:*

Risk Rating

The risk rating here is High because of the simplicity of the passwords used and their successful cracking granted access to the network system.

Vulnerability Description

By utilizing John the Ripper code the hashes ex-filtrated from Ex090 were cracked and the credentials of system users were identified.

Confirmation method

This vulnerability is confirmed by the successful login into the network with the given credentials.

Mitigation or Resolution Strategy

This vulnerability can be removed by having employees use more complex passwords, changing them periodically, and not using them across devices or systems.

Finding: *Ex0b0:*

Risk Rating

This vulnerability is Critical as any third party is able to gain access to the inner network of artstailor.com through the use of costumes.artstailor.com. The use of chisel, proxychains, and pivoting is readily available online so the ability of third parties to reproduce this finding is likely.

Vulnerability Description

The inner network of artstailor.com was found to be accessible by external forces through pivoting off the accessible connection point costumes.artstailor.com. By connecting to costumes.artstailor.com and then running a proxychain the artstailor.com inner network was susceptible to probing by nmap. By probing on this network the status of the Art's web application was discovered.

Confirmation method

Confirmation of this vulnerability can be established by checking if the Art's web application is discoverable on the network.

Mitigation or Resolution Strategy

By limiting the ip addresses allowed to access the network this vulnerability can be mitigated.

Finding: *Ex0c0:*

Risk Rating

This vulnerability is ranked Medium because the antivirus software does identify the malicious code. However, this does not occur immediately and there is a window of opportunity that would allow malicioud code to be executed.

Vulnerability Description

It was found that the windows antivirus software dynamically identifies the python payload/handler veil-evasion meterpreter session that is sent to books.artstailor.com. However, the meterpreter session is established for a few moments before this happens which allows a window of opportunity for malicious code to be executed and summarily comprise the integrity of the system.

Confirmation method

By launching the meterpreter and seeing if connection is established the continued existence of this vulnerablity can be confirmed.

Mitigation or Resolution Strategy

Mitigation of this vulnerability can stem from ensuring windows is fully updated as the security protocol does recognize the malicious software and current security patches may have addressed this.

Finding: *Ex0d0:*

Risk Rating

This vulnerability is ranked High as the 'net user' command can be used by anyone to gain administrator privileges and its documentation is available online. Therefore reproduction by third parties are likely to happen.

Vulnerability Description

It was found that the Windows application is vulnerable to a 'net user' vulnerability where execution of that command allows the creation of an administrator account from the login screen. Once access to the books.artstailor.com was granted, using the aforementioned exploit, the full directory tree was available where the files UsefulFacts under the n.nomen application directory and creds.txt under the t.turing documents directory were located.

Confirmation method

This vulnerability can be checked by using the 'net user' command and trying to create an account.

Mitigation or Resolution Strategy

This vulnerability can be removed by changing the login screen to not allow command prompt access.

Finding: *Ex0e0:*

Risk Rating

This vulnerability is ranked Critical as it allows the analysis and capture of sensitive information through unsecured channels over the web. This information can be captured by any third party.

Vulnerability Description

It was found that the ceo.artstailor.com is susceptible to ssl stripping attacks because the domain does not persistently use HTTPS and instead uses HTTP in certain communication channels.

Confirmation method

This vulnerability can be confirmed by looking for any web page that uses HTTP instead of HTTPS.

Mitigation or Resolution Strategy

This vulnerability can be removed by ensuring the uniform use of HTTPS throughout all networks and devices on the artstailor.com domain.

Finding: *Ex0f0:*

Risk Rating

This vulnerability is ranked High as anyone who has gained access to t.turing can raise their privilege to administrator. This vulnerability is also documented online which will allow third parties to easily reproduce our results. However, this exploit only impacts devbox.artstailor.com.

Vulnerability Description

It was found that the use of a sudo exploit grants root privilege into the linux environment. Once access was granted to the system, through the use of the exploit, it was also found that root privilege was granted to the user and access to the entire file system was granted including access to MyDream.png.

Confirmation method

This vulnerability can be confirmed by checking the version of sudo. Any version older than 1.8.27 is susceptible to this vulnerability.

Mitigation or Resolution Strategy

This vulnerability can be removed by updating the sudo software.

Finding: *Ex100:*

Risk Rating

The risk rating of this vulnerability is Medium as the wpad service can be compromised by any third party that also has root privilege on devbox.artstailor.com with access to the t.turing account. Because of this, reproducing our results are diminished despite the used exploits being detailed online.

Vulnerability Description

It was found that on devbox.artstailor.com the wpad service can be poisoned and subsequently return system user credential to the outside environment. In addition, the use of HTTP communication allows the un-encrypted communication to be analyzed by outside observers.

Confirmation method

This vulnerability can be confirmed by checking if HTTP is being used instead of HTTPS by devbox.artstailor.com.

Mitigation or Resolution Strategy

This vulnerability can be removed by disabling wpad. This will prevent the cache from being compromised. Also by ensuring HTTPS is used will mitigate any risks.

Finding: *Ex140:*

Risk Rating

This vulnerability is ranked High as any third party can view the code and identify the hard coded credentials in the code.

Vulnerability Description

It was found that within the apk file structure the username and password is hard-coded under the ItemListActivity/Async directory on line 146. This is easily decrypted to show the credentials.

Confirmation method

go to line 146 in the directory ItemListActivity/Async and see if the credentials remain.

Mitigation or Resolution Strategy

Do not hardcode usernames or passwords in the software of applications.