PENETRATIION TESTING

Client: Smartknower

Prepared By: K Bhavani Venkata Karthik (The Tester)

CONFIDENTIALITY

In no event shall the tester be liable to anyone for special, incidental, collateral or consequential damages arising out of the use of this information. This document contains information, which is confidential and proprietary to the tester and Smartknower. Extreme care should be exercised before distributing copies of this document, or the extracted contents of this document.

The tester is authorizing point of contact at Smartknower, to view and disseminate this document as he/she sees fit in accordance with Smartknower data handling policy and procedures This document should be marked "CONFIDENCIAL" and therefore we suggest that this document be disseminated on a "need to know" basis.

Address questions regarding the proper and legitimate use of this document to:.

K Bhavani Venkata Karthik
Address1,
Address2
Attention: Contracts Manager

DISCLAIMER

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a "point in time" analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications

SCOPE

The scope of this assessment was limited to the company configured network with it's many devices including computers and mobiles. The assessment was conducted to test system security by creating a virus/trojans and injecting it into the system. Data encryption and steganography was also performed.

EXECUTIVE SUMMARY

The purpose of this vulnerability assessment is to gather vulnerability data on the Windows Operating System that the company system uses as well as the company subnet 10.0.2.15 and web applications. Also, data regarding possible exploits of employee android mobile phones was also conducted.

In performing detailed network penetration study against SmartKnower network, computers and mobiles, the tester identified several issues of concern, finding the overall vulnerability of the company systems to be very high and easily exploitable.

It was found that numerous exploits exist within the company systems which can easily expose the company to numerous losses. In conclusion, a lot of system vulnerabilities were tested and detected which can be easily fixed.

SUMMARY OF VULNERABILITIES

The vulnerabilities detected in the company systems were numerous and easily exploitable. The network used by the company was found to be secure as server loopholes were a minimum. But individual system data and other specific aspects of the network were found to extremely accessible. Thus making the loopholes of the network widely known.

Also, on performing various attack simulations on company systems, it was found that the company workstations were extremely vulnerable to numerous attacks. The attack simulation testing involved bombarding the operating system with numerous viruses including but not limited to a DOS attack, a virus attack and a trojan horse insertion. All the simulations were successful, leaving the systems vulnerable to complete and total exploitation.

The security of employee mobiles was tested using online MTF (Mobile Tracker Free) tool. The simulated attack was successful and employee call logs and contacts were extracted with ease. Also, camera access to employee mobile phones was also obtained. This indicates multiple vulnerabilities in employee practices and security of their mobile phones.

LIST OF TOOLS USED

- Tetrabit Virus Maker- Virus attack simulator
- LOIC Tool -DOS attack simulator
- Mobile Tracker Free (MTF)- Mobile spyware
- SNOW Tool – Message encryption and steganography software

- Manual Footprinting and BlindSQL Authentication Injection
- ProRat -Trojan Horse Attack Simulation software

VULNERABILITY ASSESSMENT

In an overall perspective, numerous vulnerabilities were detected upon simulating numerous attacks. It has been found that computers lack any form of protection from cyber-attacks aside from the default antivirus software which is weak and outdated. Network information was also easily accessible and employee mobile phones were also easily hackable. Below are all the vulnerabilities discovered.

Lack of Information Security

Date of Discovery: 20/03/2021

CVSS Assessment:9.8 Critical

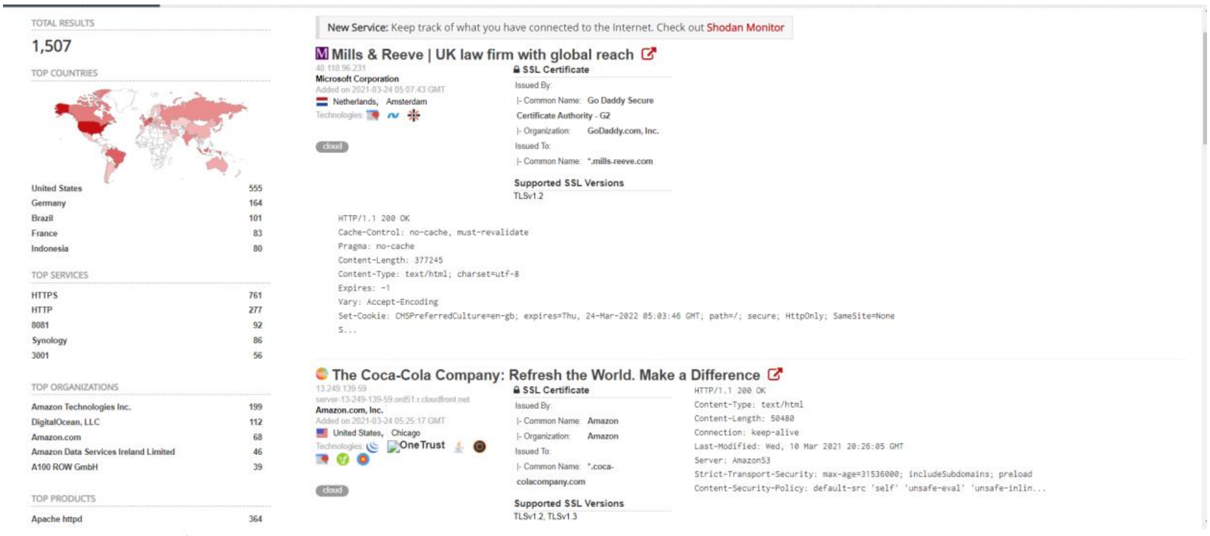
Shodan gathers information about all devices directly connected to the Internet. If a device is directly hooked up to the Internet then Shodan queries it for various publicly-available information. The types of devices that are indexed can vary tremendously: ranging from small desktops up to nuclear power plants and everything in between.

An attempt to gather data on the company's security was made using numerous web application information websites like Shodan.io, DNS dumpster etc. Data on the specifics of the computers and networks employed by the company were readily on the website.

This can be fatal as it exposes vulnerabilities of the company network to malicious attackers intent on illegal exploitation of the system.

Following are the steps to access the openly available sensitive data:

1. Open website Shodan.io.
2. Type out the website name in the search bar and search.
3. All the openly available sensitive details will be displayed.



TOTAL RESULTS

1,507

TOP COUNTRIES

United States	555
Germany	164
Brazil	101
France	83
Indonesia	80

TOP SERVICES

HTTPS	761
HTTP	277
8081	92
Synology	86
3001	56

TOP ORGANIZATIONS

Amazon Technologies Inc.	199
DigitalOcean, LLC	112
Amazon.com	68
Amazon Data Services Ireland Limited	46
A100 ROW GmbH	39

TOP PRODUCTS

Apache httpd	364

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Mills & Reeve | UK law firm with global reach

40.118.96.231
Microsoft Corporation
Added on 2021-03-24 05:07:43 GMT
Netherlands, Amsterdam
Technologies:

cloud

SSL Certificate
Issued By:
|- Common Name: Go Daddy Secure Certificate Authority - G2
|- Organization: GoDaddy.com, Inc.
Issued To:
|- Common Name: *.mills-reeve.com

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Content-Length: 377245
Content-Type: text/html; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Set-Cookie: CMSPreferredCulture=en-gb; expires=Thu, 24-Mar-2022 05:03:46 GMT; path=/; secure; HttpOnly; SameSite=None
S...
```

The Coca-Cola Company: Refresh the World. Make a Difference

13.249.139.59
server-13-249-139-59.ord51.r.cloudfront.net
Amazon.com, Inc.
Added on 2021-03-24 05:25:17 GMT
United States, Chicago
Technologies: OneTrust

cloud

SSL Certificate
Issued By:
|- Common Name: Amazon
|- Organization: Amazon
Issued To:
|- Common Name: *.coca-colacompany.com

Supported SSL Versions
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 50480
Connection: keep-alive
Last-Modified: Wed, 10 Mar 2021 20:26:05 GMT
Server: AmazonS3
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Content-Security-Policy: default-src 'self' 'unsafe-eval' 'unsafe-inlin...
```

Recommended course of action is to use VPNs as far as possible when dealing with internet related operations on company workstations. Legacy and unused services must be removed. Router firmware, preferably customizable, can be installed for the network. Port forwarding for IoT devices on LAN should be disabled. Employing an account lockout policy is a must. Use of SNOW tool for encryption of data during transferring is strongly recommended. Additionally, using default permissions should be avoided and applications should be properly and necessarily configured.

Trojan Horse

Date of Discovery: 20/03/2021

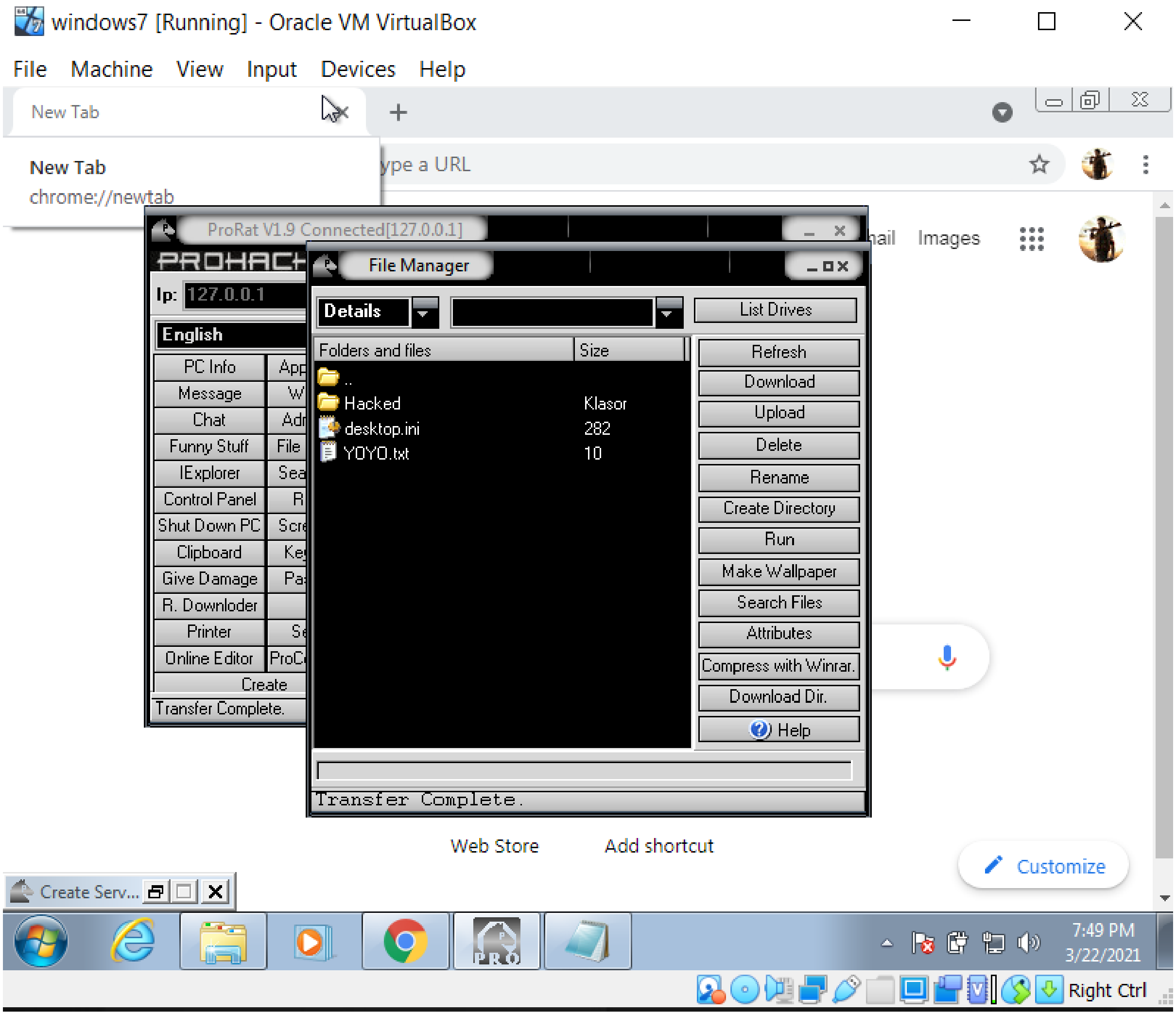
CVSS Assessment: 7.8 High

A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. The exploitative and disruptive potential of a trojan horse is high. A Trojan acts like a bona fide application or file to trick the user. It seeks to deceive one into loading and executing the malware on the device in use. Once installed, a Trojan can perform the action it was designed for.

Using ProRat, a trojan horse simulation software, a trojan horse aimed at taking complete system control was made and inserted into the targeted company machine as a notepad. The operating system being run was Wndows. Control was obtained with moderate ease due to lack of proper security measures. The windows default antivirus program provided some extent of protection to the system by detecting and preventing execution of said malicious file. But ultimately, the file was executed and the system accessed by the trojan. Key logs were accessed and files were uploaded and deleted to test the extent of control on the system. Such an attack with malicious intent can cause great harm to a company as the potential for the use of a trojan once it gains access are numerous and dangerous.

Following are the steps followed to simulate trojan attack.

1. Download ProRat.
2. Go to create -> create ProRat Server.
3. Go to general settings -> name the virus.
4. Go to Bind with file -> select file to bind the virus
5. Go to server icon-> select server icon. In this case it was selected as that of a notepad.
6. Click on “create server”
7. Go back to main screen -> click on connect.
8. To upload and download a file, click on file manager -> Upload and download buttons.\
9. To access key logs , go to KeyLogs file.



windows7 [Running] - Oracle VM VirtualBox

ProRat V1.9 Connected[127.0.0.1]

Ip: 127.0.0.1

File Manager

Folders and files	Size
..	
Hacked	Klasor
desktop.ini	282
YOYO.txt	10

Transfer Complete.

Recommended course of action is to have trojan antivirus installed on all devices. Preventative measures include regular scans for suspicious files as well as immediately quarantining and deleting suspicious looking or disguised .exe files.

Virus Attack

Date of Discovery: 24/03/2021

CVSS Assessment: 7.8 High

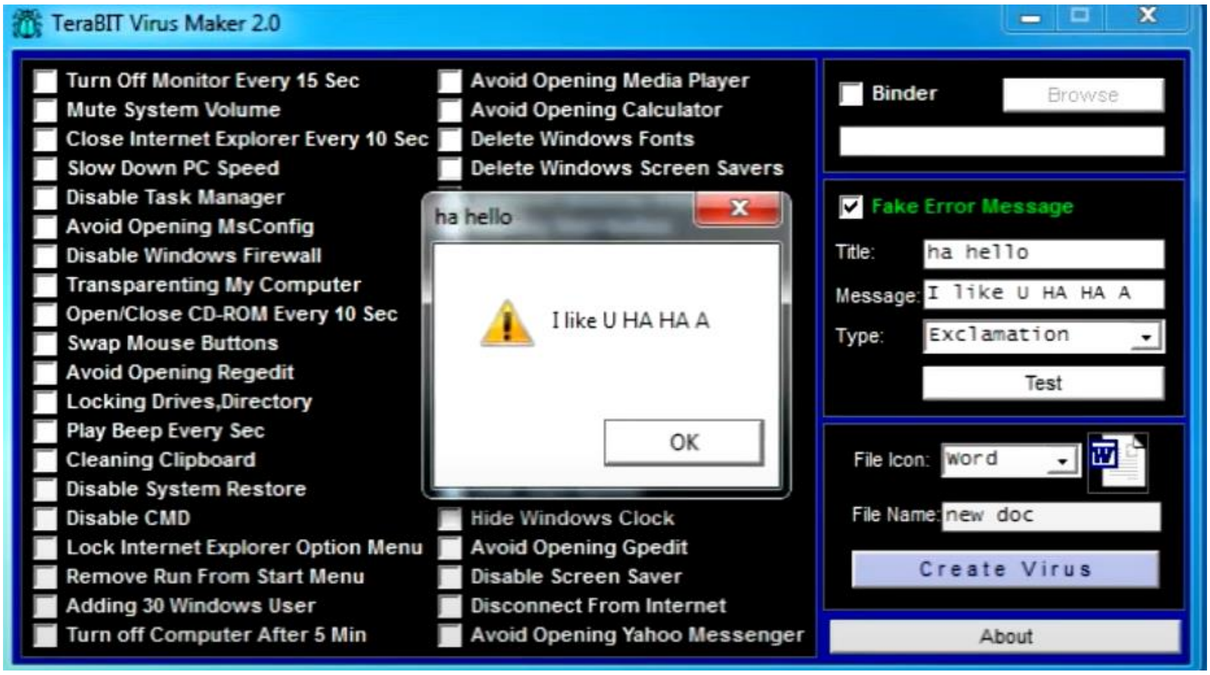
A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.

In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Using tetrabit virus maker, a virus was created to display an unusual message upon opening. The virus was disguised as a word document and also displayed successful virus creation message upon creation of infected file. The file was injected into a company workstation and executed to test the ease of a possible virus attack. The attack was successful as the unusual message was displayed upon executing virus file which did not open but displayed the message.. The victim machine was running Windows operating system with default antivirus program.

Following are the steps followed to simulate the attack:

1. Install tetrabit virus maker.
2. Upon opening select type of virus. In this case , it was selected as the option “Avoid opening media files”.
3. Choose type of file, symbol and name.
4. Fille out message details.
5. Click on create virus.
6. “Virus created successfully” will be displayed.
7. Insert malicious file in victim machine.
8. Execute file in victim machine.



□ Turn Off Monitor Every 15 Sec
□ Mute System Volume
□ Close Internet Explorer Every 10 Sec
□ Slow Down PC Speed
□ Disable Task Manager
□ Avoid Opening MsConfig
□ Disable Windows Firewall
□ Transparenting My Computer
□ Open/Close CD-ROM Every 10 Sec
□ Swap Mouse Buttons
□ Avoid Opening Regedit
□ Locking Drives,Directory
□ Play Beep Every Sec
□ Cleaning Clipboard
□ Disable System Restore
□ Disable CMD
□ Lock Internet Explorer Option Menu
□ Remove Run From Start Menu
□ Adding 30 Windows User
□ Turn off Computer After 5 Min
□ Avoid Opening Media Player
□ Avoid Opening Calculator
□ Delete Windows Fonts
□ Delete Windows Screen Savers
□ Hide Windows Clock
□ Avoid Opening Gpedit
□ Disable Screen Saver
□ Disconnect From Internet
□ Avoid Opening Yahoo Messenger

ha hello

I like U HA HA A

□ Binder

☑ Fake Error Message

Title: ha hello

Message: I like U HA HA A

Type: Exclamation

File Icon: word

File Name: new doc

Recommended counter measures involve use of up-to-date antivirus, firewalls, and strong password restricted access. Additionally, use of pop-up blocker, regular software updating and backing up data are all advisable countermeasures. Preventative measures include not accessing suspicious or unknown links or e-mails.

Mobile Spyware Attack

Date of Discovery: 24/03/2021

CVSS Assessment: 5.3 Medium

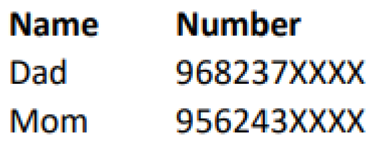
Mobile spyware is a classification of software programs that monitors and records information about an end user's actions without the end user's knowledge or permission. If the end user is aware that monitoring software has been installed, the software is not considered to be spyware.

Like desktop spyware, mobile spyware is often installed unwittingly by the end user when he or she sideloads a third-party software app, visits or is redirected to a malicious website or leaves the computing device physically unattended. Once a mobile device is infected with spyware, the spy can eavesdrop on conversations held on (or near) a compromised smartphone or access data that is stored on or transmitted by the device. Bluetooth also offers a largely unsecured interface that can be exploited by those in close proximity, through techniques like Bluesnarfing. Smartphone accelerometers have been used in keyboard vibration attacks to detect what is typed on a computer with surprising accuracy when the phone was sitting on the desk near the keyboard.

Using online mobile tracker free tool, complete control of employee mobile phone was acquired and call logs as well as contact information was extracted from it. Mobile free tracker is a tool to gain complete access to a mobile's data and controls. The victim phone used the Android operating system.

Following are steps to simulate attack:

1. Create an MTF account.
2. Install MTF app on victim phone and grant all permission.
3. Extract call logs and contact list.
4. Access them in result tab.
5. Download them into excel file and save as pdf.



Name	Number
Dad	968237XXXX
Mom	956243XXXX

Mobile spyware is highly invasive. Besides having a strong antivirus software, it is recommended to scan mobiles regularly for unauthorized and unknown app downloads as well as careful management of app permission.

Denial-of-Service (DoS) Attack

Date of discovery: 24/03/2021

CVSS Assessment: 7.3 High

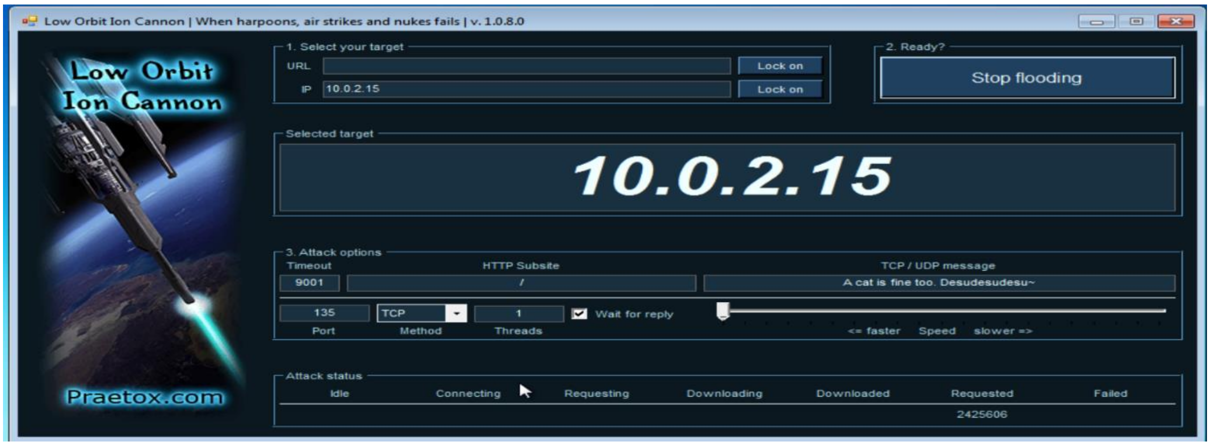
A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

A DoS attack on a company workstation operating with a windows system was simulated using the LOIC tool to determine vulnerability to DoS attack. It was found that the system was easy to flood and there was a big spike in cpu usage during the flooding process. The system in general, also began slowing down and heating up.

Following are the steps to follow to simulate the attack:

1. Download LOIC tool
2. Open a command (cmd) terminal use command “ipconfig” in victim machine.
3. Copy the IPv4 address.
4. Open LOIC tool and paste in IP section.
5. Click on corresponding ‘Lock’ button.
6. In command terminal, enter ‘netstat -an’ in victim machine.
7. Copy the last digits of the first local address.
8. Put it in port.
9. Click on ‘IMMA CHARGIN MAH LAZER’ button.



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

URL

IP 10.0.2.15

Selected target

10.0.2.15

3. Attack options

Timeout 9001

HTTP Subsite /

TCP / UDP message A cat is fine too. Desudesudesu~

Port 135

Method TCP

Threads 1

☑ Wait for reply

Attack status

Requested 2425606

To protect against DoS attack, countermeasures include constant and strict monitoring of company data traffic. A strict zero trust policy is necessary to implement to mitigate the possibility of DoS attack.

BlindSQL Injection

Date of Discovery: 24/03/2021

CVSS Assessment: 6.5 Medium

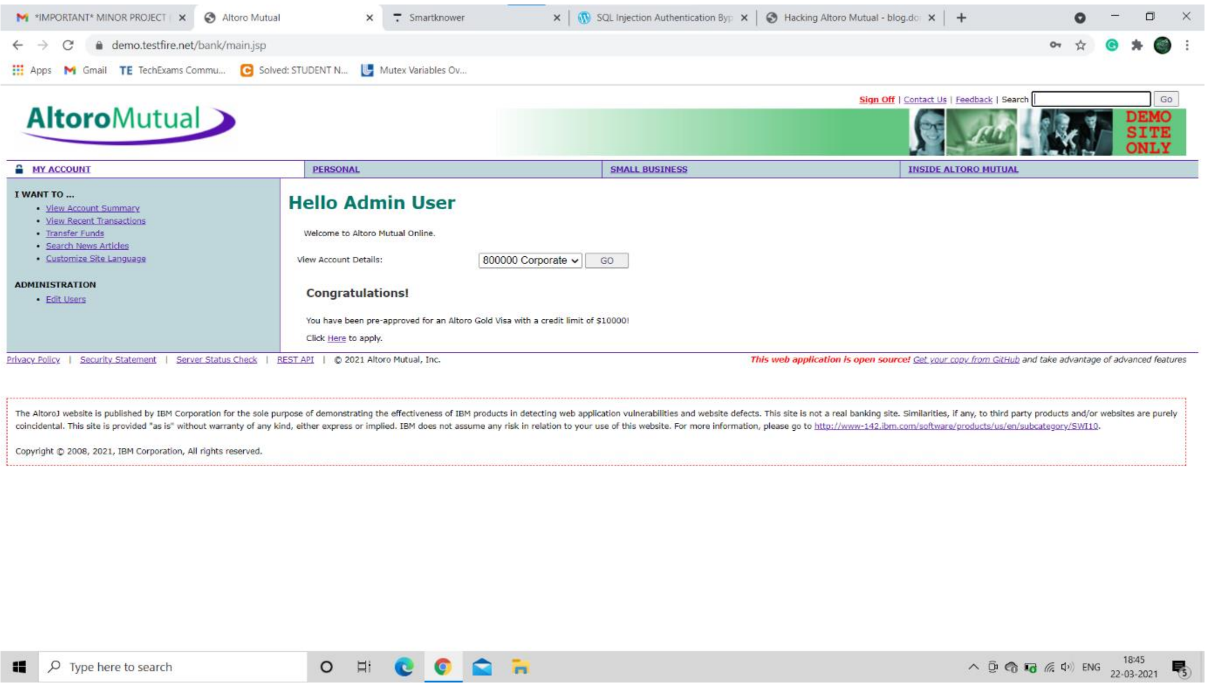
Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

When an attacker exploits SQL injection, sometimes the web application displays error messages from the database complaining that the SQL Query’s syntax is incorrect. Blind SQL injection is nearly identical to normal SQL Injection, the only difference being the way the data is retrieved from the database. When the database does not output data to the web page, an attacker is forced to steal data by asking the database a series of true or false questions. This makes exploiting the SQL Injection vulnerability more difficult, but not impossible.

A BlindSQL Injection attempt was made on the web application of the company, https://demo.testfire.net/. The injection was successful and unauthorized access was granted. This shows the lack of implementation of proper security protocols and norms in the web application. Specifically, the website does not implement least privilege to application accounts and there is an overly trust on user input. Which means the verification of the username and password in terms of code is not thorough and outdated.

Following are the steps to follow to simulate attack:

1. Open website.
2. Open the cheat sheet website: https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/
3. Test for vulnerability using Blind SQL cheat sheet.
4. Enter given usernames and a random password
5. Access is granted by entering admin' – as username.



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

© 2021 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2021, IBM Corporation, All rights reserved.

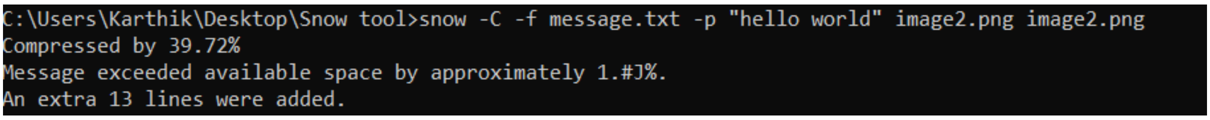
Solution: SNOW Encryption Tool

The program SNOW is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected. SNOW exploits the Steganographic Nature Of Whitespace. Locating trailing whitespace in text is like finding a polar bear in a snowstorm (which, by the way, explains the logo). And it uses the ICE encryption algorithm, so the name is thematically consistent.

SNOW is a good tool to counter data security loopholes and secure communications such as e-mails and transfer of data in general. A text file was hidden in an image with the help of SNOW tool to demonstrate the efficiency of it’s encryption.

Following are the steps to implement SNOW tool:

1. Install SNOW tool.
2. Open command terminal.
3. Navigate to directory where SNOW tool is present via ‘cd’ command.
4. Use the following command , replacing ‘’message.txt’’ with file to be encrypted and ‘’image2.png’’ with file that is going to be used for encryption. Replace “hello world” with decryption password.



```
C:\Users\Karthik\Desktop\Snow tool>snow -C -f message.txt -p "hello world" image2.png image2.png
Compressed by 39.72%
Message exceeded available space by approximately 1.#J%.
An extra 13 lines were added.
```

Here,

-C =Used for compression and encryption

-f = Used to select file to be encrypted

-p = Specify password. To be used during decryption.

<u>Conclusion</u>

The state of network security is weak and could use a lot of improvement. Mandatory use antivirus software, firewalls and VPNs is recommended as well as implementation of cyber-security policies such as zero trust policy is also necessary. Familiarisation and usage of various encryption tools like SNOW is also recommended and demonstrated. Implementing the necessary policies and integrating recommended countermeasures into the work place of the company will ensure safety and security from any future cyber-attacks.