

Kali-Linux

Fernando Souza Rodrigues
Paulo Ferreira da Silva Júnior



O que é o Kali Linux?

O Kali Linux é uma distribuição de segurança baseada no Debian, que tem como objetivo realizar testes de penetração e análise forense. Com mais de 600 ferramentas pré-instaladas, como scanners de vulnerabilidades, sniffers de rede e ferramentas de engenharia reversa, o Kali Linux é amplamente utilizado por profissionais de segurança cibernética. Ele possui uma interface gráfica de usuário (GUI) amigável e intuitiva, o que o torna acessível até para iniciantes. Além disso, o Kali Linux suporta a execução em máquinas virtuais.



História do Kali Linux

O Kali Linux originou-se como o BackTrack Linux em 2006, uma distribuição focada em testes de penetração e análise forense. Em 2013, foi substituído pelo Kali Linux, que se tornou a distribuição de segurança mais popular do mundo. O Kali Linux é usado por hackers éticos, profissionais de segurança cibernética e pesquisadores para avaliar a segurança de sistemas e redes.



Principais recursos do Kali Linux

O Kali Linux utiliza o kernel Linux 6.10, que traz melhorias em segurança, desempenho e suporte a novos hardwares. O kernel personalizado possui patches de segurança e módulos específicos para ferramentas de hacking e testes de penetração, tornando o sistema operacional robusto e seguro para profissionais de segurança cibernética. Isso permite que os usuários realizem suas atividades com eficácia e confiança.



Principais recursos do Kali Linux

O Kali Linux é uma distribuição de segurança com mais de 600 ferramentas pré-instaladas. Ele inclui scanners de vulnerabilidades, sniffers de rede, ferramentas de engenharia reversa e muito mais. O Kali Linux é conhecido por suas ferramentas populares, como Metasploit, Nmap, Wireshark e Maltego. Além disso, ele suporta dispositivos ARM, permitindo seu uso em dispositivos móveis, proporcionando conveniência e flexibilidade aos usuários.



Principais Softwares do Kali Linux

- ***Maltego:** é uma ferramenta de inteligência visual de código aberto. Ela ajuda na coleta e análise de informações, mapeando relacionamentos entre pessoas, empresas e domínios, auxiliando em investigações e análises.*
- ***Wireshark:** É uma ferramenta de análise de tráfego de rede. Ele permite capturar e examinar pacotes de dados em tempo real, ajudando a identificar problemas de rede.*
- ***Metasploit Framework:** É um conjunto de ferramentas de teste de penetração. Ele fornece uma plataforma para descoberta de vulnerabilidades, desenvolvimento de exploits e realização de ataques controlados para testar a segurança de sistemas e redes.*

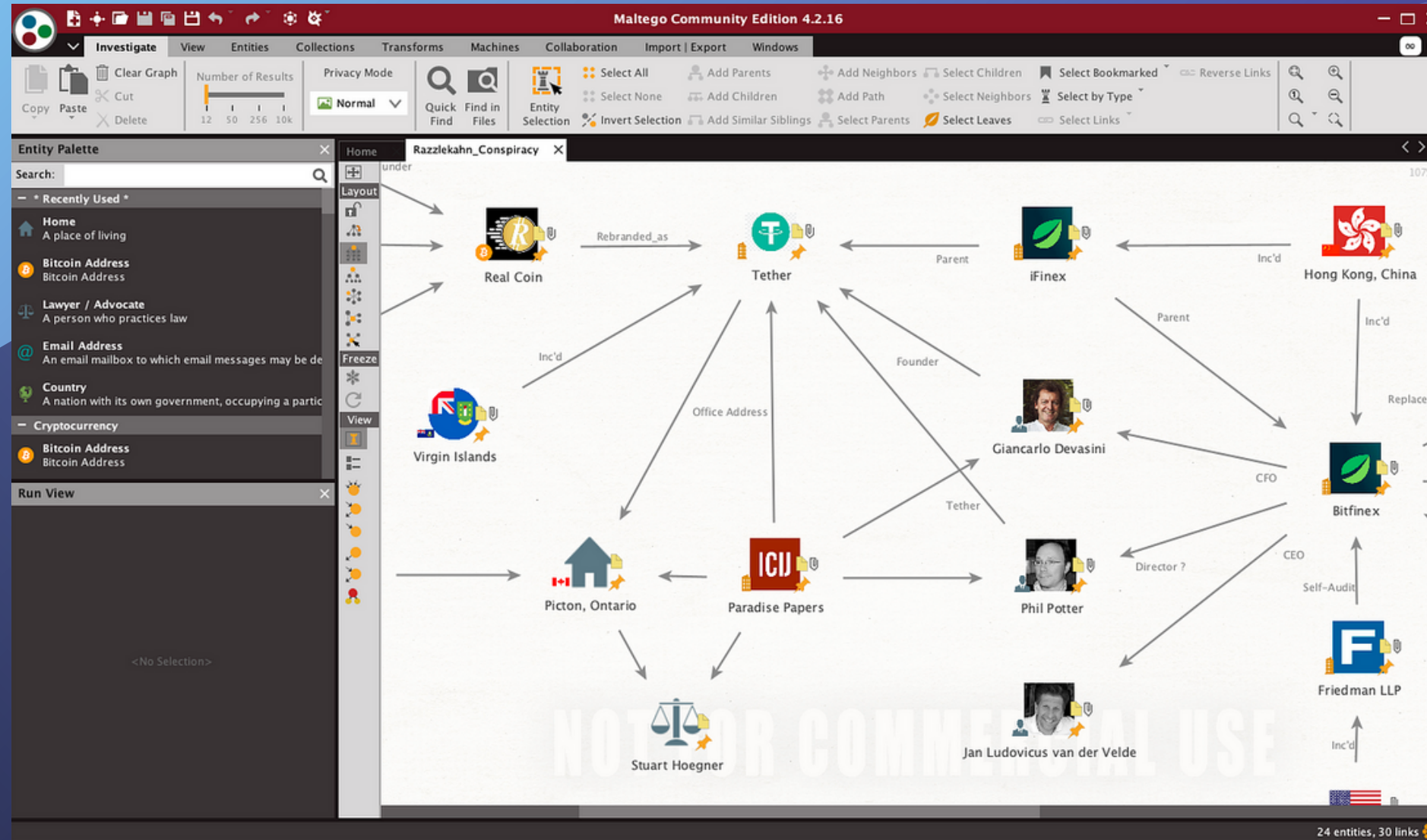


Principais Softwares do Kali Linux

- ***Burp Suite:** é uma suíte de ferramentas para testes de segurança de aplicativos web. Ele possui recursos como proxy, scanner de vulnerabilidades e explorador de sequências de caracteres, usados para identificar e corrigir falhas de segurança em sites e aplicativos.*
- ***Nmap:** É um scanner de rede que permite descobrir hosts, serviços e portas em uma rede. Ele é usado para mapear e verificar a segurança da rede.*
- ***Hydra:** é uma ferramenta de quebra de senhas e autenticação em serviços remotos. Ela realiza ataques de força bruta ou de dicionário para testar a força das senhas e identificar vulnerabilidades em sistemas autenticados.*



Principais Softwares do Kali Linux



Maltego

```
msfconsole

.:ok000kdc'      'cdk000ko:.
.x0000000000000c      c000000000000x.
:000000000000000k,      ,k000000000000000:
'000000000k00000: :0000000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occcx0000.MX'x00d.
,kol'M.0000000000000.M'dOk,
:kk;.00000000000000.;Ok:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.2.20-dev ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Metasploit



Principais Softwares do Kali Linux

tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsec_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

Queries

> cdn-0.nflximg.com: type A, class IN

Answers

> Authoritative nameservers

0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5....?l....

0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl

0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com

0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images

0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg

0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et.../...

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Whireshark

Burp Suite Professional V2.202 - Temporary Project - licensed to Exploits Information Security LLC (single user license)

Burp Project Intruder Repeater Window Help

Versions Heartbleed SSL Scanner CSurfer Deserialization Scanner Additional Scanner Checks Errors Headers Analyzer AWS Security Checks ExifTool

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Tasks

Filter Running Paused Finished

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope. 110 items added to site map

Capturing: ☒ 6 responses processed 0 responses queued

2. Live audit from Proxy (all traffic)

Audit checks - passive Issues: 2 5 5 requests (0 errors) View details >>

Event log

Filter Critical Error Info Debug Search...

Time	Type	Source	Message
14:56:09 6 Aug 2019	Error	Proxy	[958] Failed to connect to detectportal.firefox.com:80
14:56:09 6 Aug 2019	Error	Proxy	[958] Failed to connect to detectportal.firefox.com
14:53:34 6 Aug 2019	Info	Task 14	[2] Maximum time exceeded in dynamic code analysis of: /mutill
14:34:26 6 Aug 2019	Info	Task 8	[2] Maximum time exceeded in dynamic code analysis of: /mutill
14:26:55 6 Aug 2019	Error	Proxy	Failed to connect to shavar.services.mozilla.com
14:26:55 6 Aug 2019	Error	Proxy	Failed to connect to shavar.services.mozilla.com:443
14:22:49 6 Aug 2019	Info	Task 5	[3] Maximum time exceeded in dynamic code analysis of: /mutill
14:20:59 6 Aug 2019	Info	Task 5	Maximum time exceeded in dynamic code analysis of: /mutillidae
14:12:06 6 Aug 2019	Info	Task 2	Maximum time exceeded in dynamic code analysis of: /mutillidae
14:10:40 6 Aug 2019	Error	Proxy	[2] java.net.SocketException: Connection reset
14:10:40 6 Aug 2019	Error	Proxy	[2] Connection reset
14:09:43 6 Aug 2019	Error	Proxy	[2] No response received from remote server.
14:03:35 6 Aug 2019	Info	Extender	HeartBleed: deprecated Extender API used - registerMenuItem()
14:03:33 6 Aug 2019	Info	Proxy	Proxy service started on 127.0.0.1:8080
14:03:30 6 Aug 2019	Info	Suite	Running as super-user, embedded browser sandbox will be disab

Issue activity

Filter High Medium Low Info Certain Firm Tentative Search...

#	Task	Time	Action	Issue type
425	14	14:52:58 6 Aug 2019	Issue found	Lack or Misconfiguration of Security H
424	14	14:52:58 6 Aug 2019	Issue found	Interesting Header(s)
423	14	14:52:58 6 Aug 2019	Issue found	Content Sniffing not disabled
422	14	14:52:58 6 Aug 2019	Issue found	Browser cross-site scripting filter misc
421	14	14:52:58 6 Aug 2019	Issue found	Lack or Misconfiguration of Security H
420	14	14:52:58 6 Aug 2019	Issue found	Interesting Header(s)
419	14	14:52:58 6 Aug 2019	Issue found	Content Sniffing not disabled
418	14	14:52:58 6 Aug 2019	Issue found	Browser cross-site scripting filter misc
417	14	14:52:58 6 Aug 2019	Issue found	Possible DOM-based Cross-site scripti
416	14	14:52:58 6 Aug 2019	Issue found	Cross-domain POST
415	13	14:52:45 6 Aug 2019	Issue found	Path-relative style sheet import
414	13	14:52:45 6 Aug 2019	Issue found	Input returned in response (reflected)
413	13	14:52:42 6 Aug 2019	Issue found	Input returned in response (reflected)
412	13	14:52:34 6 Aug 2019	Issue found	Link manipulation (reflected)
411	13	14:52:32 6 Aug 2019	Issue found	Input returned in response (reflected)
410	13	14:52:24 6 Aug 2019	Issue found	j2EEScan - Local File Include
409	13	14:52:24 6 Aug 2019	Issue found	Input returned in response (reflected)

Advisory

Lack or Misconfiguration of Security Header(s)

Issue: **Lack or Misconfiguration of Security Header(s)**

Severity: **Low**

Confidence: **Certain**

Host: **http://192.168.56.28**

Path: **/mutillidae/a/a%5c%b%22c%3e%3f%3e%25%7d%7d%25%25%3ec%3c[%3f%5%7b%7b%25%7d%7d%5c%5c**

Note: This issue was generated by the Burp extension: Headers Analyzer.

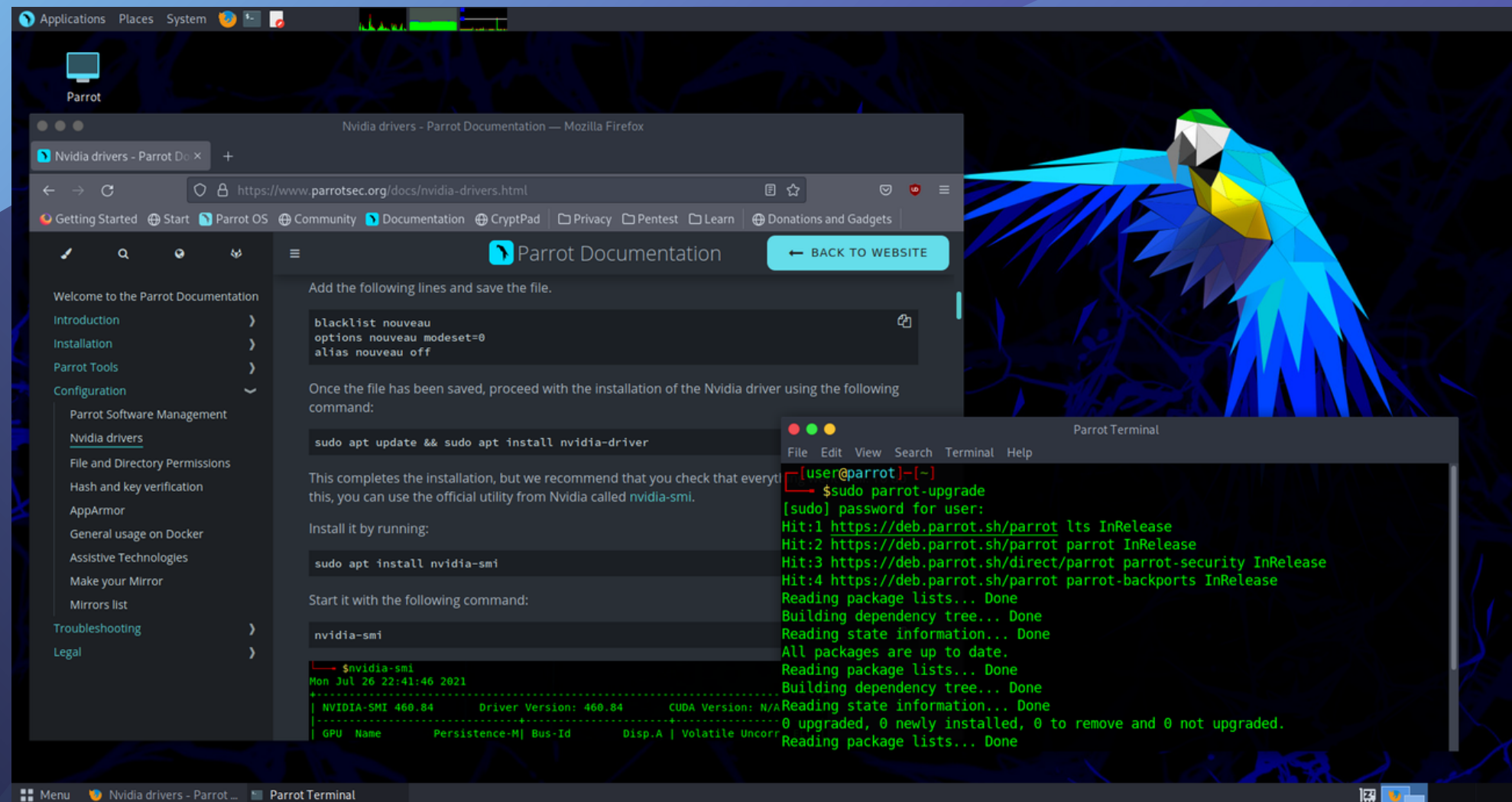
Issue detail

The response lacks or includes the following misconfigured security headers.

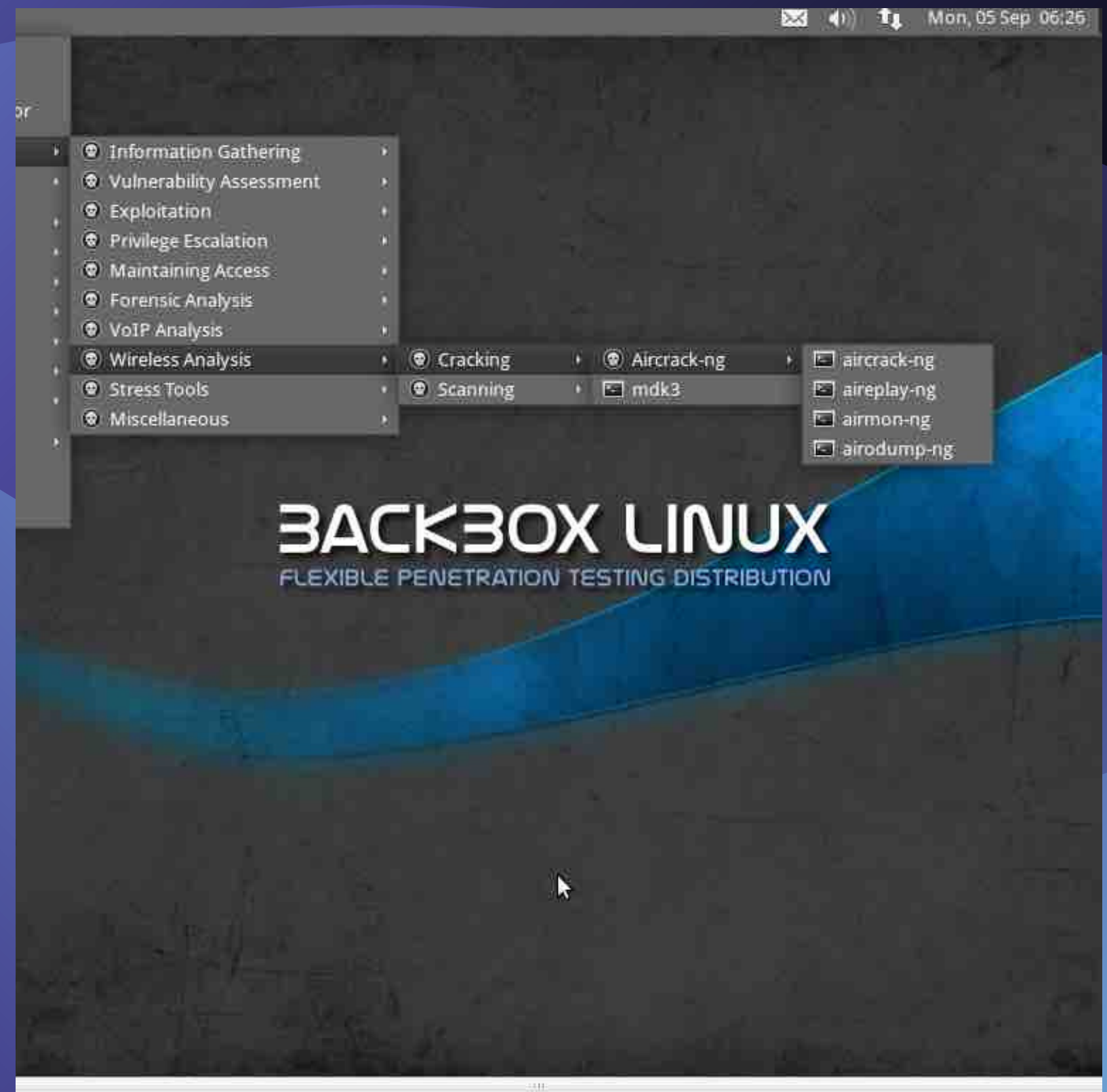
Please note that some of these issues could be false positives, a manual review is recommended

Burp Suite

Spin-Offs



Parrot Security



BackBox

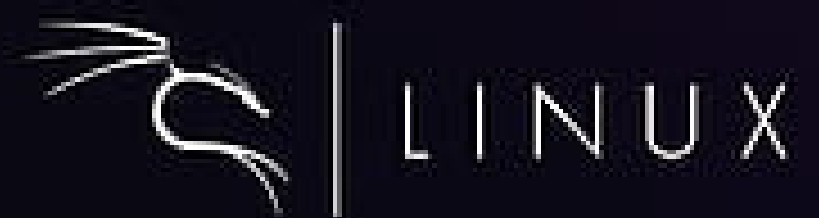
Respostas referentes às perguntas feitas na apresentação

TPM2, SecureBoot e descriptografia de armazenamento automatizado:

- Kali Linux tem suporte para o TPM 2.0 (Trusted Platform Module 2.0) que é um processador de criptografia instalado nas placas-mãe que oferece segurança durante a inicialização do sistema operacional.*

Gerenciador de Pacotes:

- O gerenciador de pacotes padrão do Kali é o APT (Advanced Package Tool) que facilita a instalação, atualização, remoção e gerenciamento de pacotes de software. Além do APT, o Kali Linux também suporta o uso de outros gerenciadores de pacotes, como o dpkg (que é a ferramenta de baixo nível subjacente ao APT) e o aptitude. Os tipos de pacotes padrão aceitos pelo APT são .deb, extensão padrão dos sistemas derivados do Debian.*



***#MELHOR DISTRO DO LINUX
OBRIGADO. 😊***