



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



Atividade Orientada a Ensino

Acadêmico: Gabriel Pastorello de Oliveira

RGA: 2018 1904 0313

Professor: Carlos Alberto da Silva

Atividade: Atividade Orientada a Ensino sobre estudos em segurança de redes, estudos das ferramentas presentes no BlackArch Linux e no Kali Linux.

Introdução

O Kali Linux e o BlackArch Linux são duas distribuições Linux populares amplamente utilizadas para fins de segurança cibernética, especialmente nas áreas de testes de penetração e análise forense digital.

Kali Linux

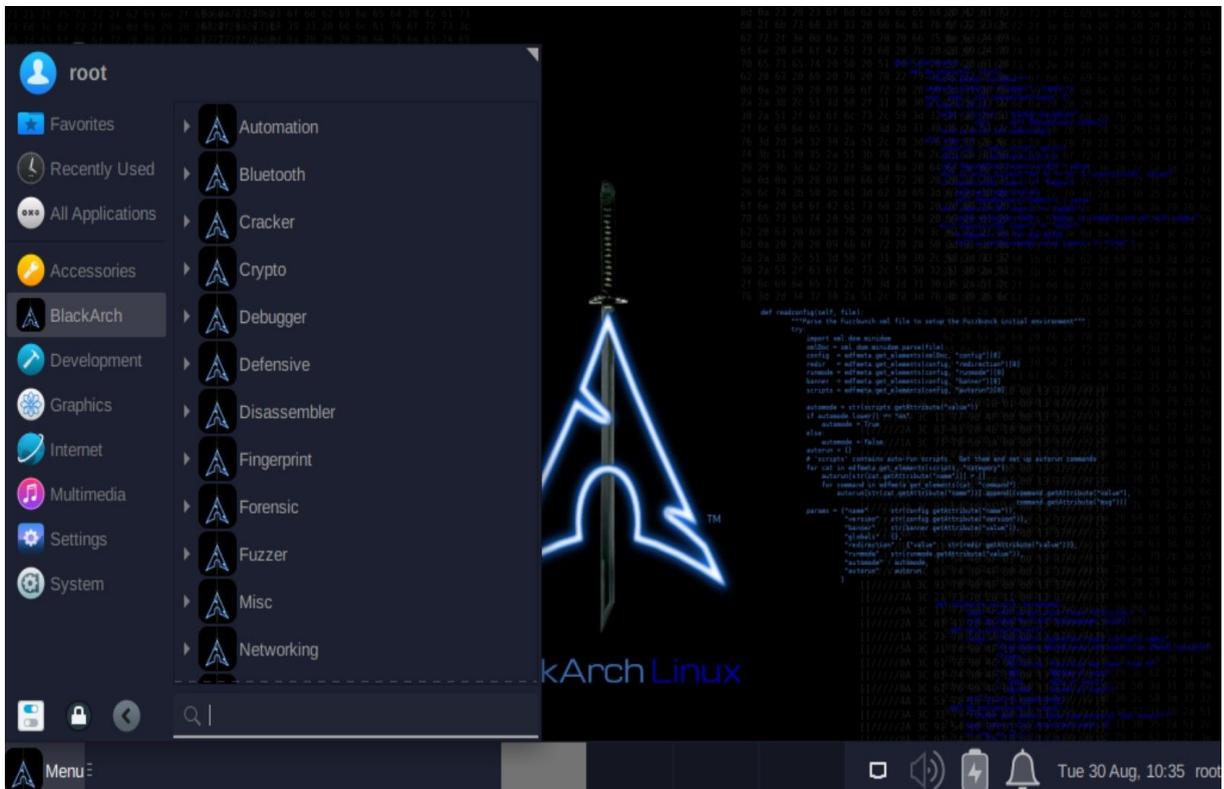
É uma distribuição Linux de auditoria de segurança baseada em Debian que foi projetada especificamente para fornecer recursos de análise forense digital e testes de penetração. Ele vem pré-instalado com uma ampla gama de ferramentas categorizadas em várias categorias, como coleta de informações, análise de vulnerabilidades, ataques *wireless*, segurança de aplicativos da *web*, ataques de senha, ferramentas de exploração e muito mais.

Algumas das ferramentas incluídas no Kali Linux são Nmap, Wireshark, Aircrack-ng, Metasploit Framework, John the Ripper, Burp Suite, Hydra, Nikto e SQLMap.



BlackArch Linux

O BlackArch Linux, por outro lado, é uma distribuição Linux baseada no Arch Linux e foi projetada especificamente para *pentesters* e pesquisadores de segurança, possuindo uma interface muito menos amigável. Ele fornece um grande repositório de ferramentas especializadas para diversas tarefas de segurança cibernética. Essas ferramentas também incluem Aircrack-ng, Metasploit Framework, Nmap, Wireshark, John the Ripper, Hydra, Nikto, SQLMap, Burp Suite e muitas outras mais.



Visão geral e casos de uso das ferramentas presentes no Kali Linux e no Black Arch Linux

Kali Linux e Black Arch Linux oferecem uma gama abrangente de ferramentas para profissionais de segurança cibernética. Essas ferramentas cobrem vários aspectos de *hacking* e testes de penetração. Ambas as distribuições fornecem ferramentas conhecidas e disponíveis gratuitamente.

Metasploit

Metasploit é uma ferramenta para desenvolvimento e lançamento de *exploits* amplamente utilizada em auditorias e testes de penetração. O *framework* consiste em uma série de ferramentas, *exploits* e códigos que podem ser usados através de diferentes interfaces.



Exemplos de casos de uso do Metasploit incluem testar a segurança de uma rede explorando vulnerabilidades, conduzindo testes de penetração para identificar pontos fracos em sistemas e simulando ataques cibernéticos do mundo real para testar as defesas de uma rede ou sistema.

Inicialização do Metasploit:

```

dBBBBBBb dBBBP dBBBBBBP dBBBBBb
' dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBP

dBBBBBP dBBBBBb dBP dBBBBP dBP dBBBBBBP
dB' dBP dB'.BP
dBP dBBBB' dBP dB'.BP dBP dBP
dBP dBP dBP dB'.BP dBP dBP
dBBBBP dBP dBBBBP dBBBBP dBP dBP

To boldly go where no
shell has gone before

=[ metasploit v5.0.85-dev ]
+ -- --[ 2002 exploits - 1093 auxiliary - 342 post ]
+ -- --[ 560 payloads - 45 encoders - 10 nops ]
+ -- --[ 7 evasion ]

Metasploit tip: You can use help to view all available commands

msf5 > search
```

Uso do Nmap como auxiliar:



```
Nmap scan report for [REDACTED]
Host is up (0.00049s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
```

Verificação de existência de exploit no Metasploit:

```
msf5 > search vsftpd

Matching Modules
=====

#  Name                                     Disclosure Date  Rank      Check  Description
-  - - - - -                               - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Con

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
RHOSTS    yes              yes       The target host(s), range CIDR identifier, or hosts file with syntax
RPORT     21               yes       The target port (TCP)

Exploit target:

Id  Name
--  -
0   Automatic
```

NMap

Nmap é uma poderosa ferramenta de varredura de rede que permite aos usuários descobrir hosts e serviços em uma rede de computadores.



Exemplos de casos de uso do Nmap incluem mapeamento de arquiteturas de rede, identificação de portas e serviços abertos, detecção de vulnerabilidades potenciais em dispositivos de rede e realização de reconhecimento de rede.

Wireshark

Wireshark é uma ferramenta de análise de pacotes que fornece informações detalhadas sobre o tráfego de rede.

Exemplos de casos de uso do Wireshark incluem análise de protocolos de rede, solução de problemas de rede, captura e inspeção de pacotes para fins de segurança e detecção de atividades maliciosas em uma rede.

Captura e inspeção de pacotes:

A captura de tela do Wireshark mostra uma interface com uma barra de menu (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) e uma barra de ferramentas. Abaixo, há uma barra de filtro de exibição com o texto "Apply a display filter ... <Ctrl-/>".

No.	Time	Source	Destination	Protocol	Length	Info
164	67.232111	40.90.185.223	192.168.1.1	TCP	1514	443 → 52377 [ACK] Seq=1461 Ack=214 Win=4204800 Len=146
165	67.232131	192.168.1.1	40.90.185.223	TCP	54	52377 → 443 [ACK] Seq=214 Ack=2921 Win=132352 Len=0
166	67.232364	40.90.185.223	192.168.1.1	TCP	1514	443 → 52377 [ACK] Seq=2921 Ack=214 Win=4204800 Len=146
167	67.232622	40.90.185.223	192.168.1.1	TCP	1514	443 → 52377 [ACK] Seq=4381 Ack=214 Win=4204800 Len=146
168	67.232627	40.90.185.223	192.168.1.1	TLSv1.2	365	Server Hello, Certificate, Certificate Status, Server
169	67.232739	192.168.1.1	40.90.185.223	TCP	54	52377 → 443 [ACK] Seq=214 Ack=6152 Win=132352 Len=0
170	67.234127	192.168.1.1	40.90.185.223	TLSv1.2	154	Certificate, Client Key Exchange, Change Cipher Spec,
171	67.238043	40.90.185.223	192.168.1.1	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
172	67.238515	192.168.1.1	40.90.185.223	TCP	1494	52377 → 443 [ACK] Seq=314 Ack=6203 Win=132352 Len=1440
173	67.238515	192.168.1.1	40.90.185.223	TLSv1.2	201	Application Data
174	67.238544	192.168.1.1	40.90.185.223	TCP	1494	52377 → 443 [ACK] Seq=1901 Ack=6203 Win=132352 Len=144
175	67.238546	192.168.1.1	40.90.185.223	TLSv1.2	627	Application Data
176	67.242941	40.90.185.223	192.168.1.1	TCP	56	443 → 52377 [ACK] Seq=6203 Ack=1901 Win=4204800 Len=0
177	67.243678	40.90.185.223	192.168.1.1	TCP	56	443 → 52377 [ACK] Seq=6203 Ack=3914 Win=4204800 Len=0
178	67.266832	40.90.185.223	192.168.1.1	TCP	1514	443 → 52377 [ACK] Seq=6203 Ack=3914 Win=4204800 Len=14
179	67.267386	40.90.185.223	192.168.1.1	TLSv1.2	1077	Application Data
180	67.267415	192.168.1.1	40.90.185.223	TCP	54	52377 → 443 [ACK] Seq=3914 Ack=8686 Win=132352 Len=0
181	67.283796	192.168.1.1	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
182	67.283836	192.168.1.1	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
183	68.281806	192.168.1.1	52.139.250.253	TLSv1.2	97	Application Data
184	68.287468	52.139.250.253	192.168.1.1	TLSv1.2	179	Application Data
185	68.327555	192.168.1.1	52.139.250.253	TCP	54	52229 → 443 [ACK] Seq=87 Ack=251 Win=515 Len=0
186	70.917820	AztechE1_14:10:5f	Tp-LinkT_25:9c:5e	ARP	42	Who has 192.168.1.1? Tell 192.168.1.254

Abaixo da lista de pacotes, o painel de detalhes mostra as informações de um pacote de protocolo ARP:

```
> Ethernet II, Src: AztechE1_14:10:5f (e0:8e:3c:14:10:5f), Dst: Tp-LinkT_25:9c:5e (64:70:02:25:9c:5e)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: AztechE1_14:10:5f (e0:8e:3c:14:10:5f)
    Sender IP address: 192.168.1.254
    Target MAC address: Tp-LinkT_25:9c:5e (64:70:02:25:9c:5e)
    Target IP address: 192.168.1.1
```



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



AircraCk-ng

Aircrack-ng é um conjunto de ferramentas usado para testes de penetração de redes sem fio, incluindo captura e quebra de senhas WPA/WPA2-PSK.

Exemplos de casos de uso do Aircrack-ng incluem testar a segurança de redes sem fio, identificar vulnerabilidades em protocolos de criptografia Wi-Fi, realizar testes de penetração sem fio e lançar ataques sem fio, como desautenticação e criação de pontos de acesso não autorizados.

John the Ripper

John the Ripper é uma ferramenta de quebra de senhas que pode ser usada para testar a força das senhas e avaliar sua vulnerabilidade.

Exemplos de casos de uso de John the Ripper incluem auditoria de segurança de senha, recuperação de senhas perdidas ou esquecidas e teste da eficácia de políticas de senha.

Hydra

Hydra é uma ferramenta para força bruta e quebra de senhas por meio de vários protocolos, como SSH, FTP e Telnet.

Exemplos de casos de uso do Hydra incluem teste de segurança de credenciais de login, realização de ataques de quebra de senha e realização de testes de penetração em sistemas com senhas fracas ou padrão.



Nikto

Nikto é um scanner de vulnerabilidades da web que verifica vulnerabilidades comuns em servidores web e CMSs.

Exemplos de casos de uso do Nikto incluem identificação de vulnerabilidades de segurança em aplicativos da web, teste da eficácia das configurações do servidor da web, detecção de versões desatualizadas de software e realização de uma avaliação abrangente de segurança de um site.

Funcionamento:

```
(kali@kali)-[~]
└─$ nikto -h [REDACTED]
- Nikto v2.1.6

+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 443

+ SSL Info:      Subject: /CN=[REDACTED]
                Ciphers: TLS_AES_256_GCM_SHA384
                Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Start Time:   2022-11-27 11:54:01 (GMT-5)

+ Server: Apache/2.4.29
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent.
+ Uncommon header 'link' found, with contents: [REDACTED]
+ [REDACTED]; rel="alternate"; type="application/javascript"
shortlink
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to
ent fashion to the MIME type
```

SQLMap

SQLMap é uma ferramenta usada para detecção e exploração automatizada de vulnerabilidades de injeção SQL em aplicações web.

Exemplos de casos de uso do SQLMap incluem identificação e exploração de vulnerabilidades de injeção de SQL, extração de dados de bancos de dados vulneráveis, teste de segurança de aplicativos web que interagem com bancos de



dados e condução de uma avaliação de segurança abrangente de aplicativos *web* orientados a banco de dados.

Funcionamento SQLMap:

```
http://sqlmap.org
The following cookies are stored on your computer:
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 14:02:22
[14:02:22] [INFO] resuming back-end DBMS 'mysql'
[14:02:22] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
Payload: id=2' OR NOT 3803=3803#&Submit=Submit
Type: error-based
Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
```

```
clause (FLOOR)
Payload: id=2' AND ROW(7136,4714)>(SELECT COUNT(*),CONCAT(0x716b7a7871,(SELECT (ELT(7136=7136,1))),0x7162717a71,FLOOR(RAND(0)*2))x FROM (SELECT 3340 UNION SELECT 2306 UNION SELECT 5944 UNION SELECT 6368)a GROUP BY x)-- VAFp&Submit=Submit
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=2' AND SLEEP(5)-- VBwI&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=2' UNION ALL SELECT CONCAT(0x716b7a7871,0x48717761555177594c4e6d4f4756476e6569594f437670564d6f5a61766f545576646c4f4145556d,0x7162717a71),NULL#&Submit=Submit
[14:02:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[14:02:22] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
[*] shutting down at 14:02:22
```



Burp Suite

Burp Suite é uma ferramenta de teste de segurança de aplicativos da *web* que permite aos usuários interceptar, modificar e analisar solicitações e respostas HTTP/S.

Exemplos de casos de uso do Burp Suite incluem identificação e exploração de vulnerabilidades em aplicativos da *web*, teste da eficácia dos mecanismos de validação de entrada e codificação de saída, interceptação e análise de informações confidenciais trocadas entre um cliente e um servidor e realização de avaliações abrangentes de segurança de aplicativos da *web*.

Interceptando requisição com o Burp Suite:

```
1 POST /rails Goat/users/6.json HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 289
10 Origin: [REDACTED]
11 Connection: close
12 Referer: [REDACTED]
13 Cookie: _rails Goat_session=
BAh7CEkiD3Nl c3Npb25fawQGOgZFRkkiJTA0MzlmNDNiZTFkZTk3OTc3NjNhYTBlOTc2YzkyMjEjBj sAVEkief9j c3JmX3Rva2VuBjsARkkiMVYyQnBqNmh2b;
ca26198bbe55d6745be81f2d72f02; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
14
15 utf8=%E2%9C%93&_method=put&authenticity_token=0rBpj6hvomcdTeTscbjSJka45x60L%2F%2FiZUI%9pN0a9k%3D&user%5Buser_id%5D=6&user!
user%5Blast_name%5D=yang&user%5Bpassword%5D=12345678&user%5Bpassword_confirmation%5D=12345678
```




Exemplos de casos de uso do Reaver incluem testar a segurança de redes sem fio tentando quebrar o PIN WPS, avaliando a vulnerabilidade de roteadores e pontos de acesso a ataques WPS, avaliando a eficácia das medidas de segurança de dispositivos habilitados para WPS e conduzindo testes de penetração em redes sem fio. redes.

WPScan

WPscan é um scanner de vulnerabilidade WordPress que identifica problemas de segurança em sites WordPress.

Exemplos de casos de uso do WPscan incluem identificação de vulnerabilidades conhecidas em instalações do WordPress, teste de segurança de plugins e temas, verificação de configurações incorretas e senhas fracas em sites WordPress e realização de avaliações de segurança de sites WordPress.

Escaneamento de vulnerabilidades de sites WordPress utilizando WPScan:

```
-$ wpscan --url https://www.mato.gov.br --random-user-agent --api-token 6096f6m2w7j20R2167VLEP26K04WpK2MMW9q300q80E

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://www.mato.gov.br
[+] Started: Mon Nov 27 18:39:05 2023

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: nginx
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: https://www.mato.gov.br/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://www.mato.gov.br/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://www.mato.gov.br/readme.txt
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Debug Log found: https://www.mato.gov.br/debug.log
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

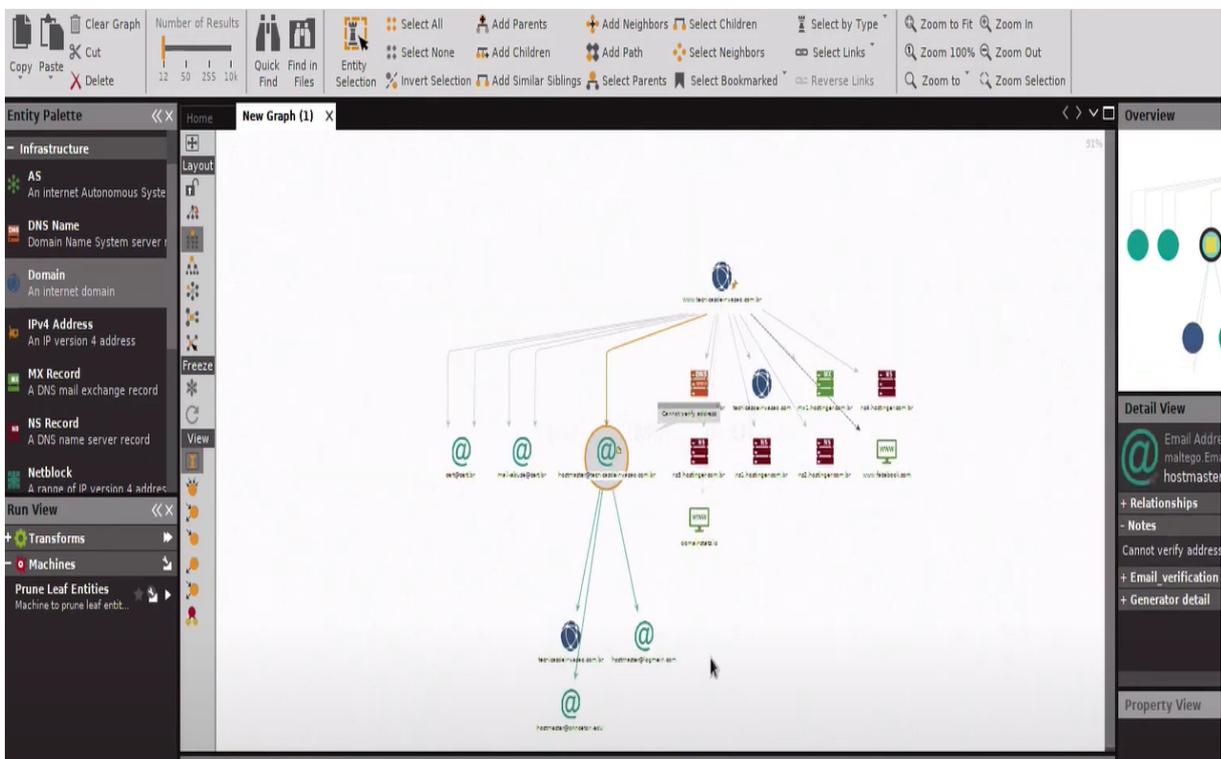


Maltego

Uma poderosa ferramenta de inteligência e análise forense de código aberto. Ele fornece uma interface gráfica que permite aos usuários explorar visualmente relacionamentos e conexões entre diversas entidades, como pessoas, organizações e recursos online.

Exemplos de casos de uso do Maltego incluem a condução de investigações digitais, a coleta de inteligência sobre indivíduos ou organizações, o mapeamento de redes e relacionamentos em um ambiente-alvo, a identificação de ameaças e vulnerabilidades potenciais e a realização de avaliações de engenharia social

Exemplo de mapeamento de redes e relacionamentos:





Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



OpenVAS

OpenVAS é outra ferramenta popular de avaliação de vulnerabilidades que fornece recursos abrangentes de verificação e geração de relatórios.

Exemplos de casos de uso do OpenVAS incluem a identificação de vulnerabilidades e configurações incorretas em redes e sistemas, a realização de auditorias de segurança regulares para garantir a segurança contínua, a avaliação da eficácia dos controles e mitigações de segurança, a avaliação da conformidade com padrões e regulamentos de segurança e gerando relatórios detalhados para a administração e partes interessadas.

Fluxion

É uma ferramenta projetada especificamente para conduzir testes de penetração em redes sem fio e ataques de engenharia social.

Exemplos de casos de uso do Fluxion incluem a realização de ataques simulados de *phishing* para testar a conscientização do usuário e a suscetibilidade à engenharia social, testar a segurança de redes sem fio explorando vulnerabilidades e fraquezas em protocolos de criptografia, capturar *handshakes* WPA/WPA2 para quebra de senha *offline*, conduzir ataques *man-in-the-middle* para interceptar e manipular o tráfego de rede e analisar a eficácia das medidas de segurança de rede.



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



Netcat

É uma ferramenta de rede versátil que pode ser usada para diversos fins, incluindo verificação de portas, transferência de arquivos entre sistemas, estabelecimento de conexões remotas e solução de problemas de conectividade de rede.

Exemplos de casos de uso do netcat incluem realizar varreduras de portas para identificar portas abertas em um sistema de destino, transferir arquivos ou dados entre sistemas usando protocolos TCP ou UDP, estabelecer conexões remotas com servidores para fins administrativos, solucionar problemas de conectividade de rede

enviando e recebendo pacotes de dados, e realizar a captura de banners para coletar informações sobre um sistema ou serviço alvo.

Estes são apenas alguns exemplos das ferramentas disponíveis no Kali Linux e no Black Arch Linux. Estas ferramentas fornecem aos profissionais de segurança cibernética os recursos necessários para testar e proteger redes de computadores, identificar vulnerabilidades e garantir a integridade geral dos sistemas.

Conclusão dos estudos

Quando se trata de escolher entre as ferramentas disponíveis no Kali Linux e no Black Arch Linux, isso depende, em última análise, das necessidades e preferências específicas do usuário. A escolha entre um sistema ou outro acaba sendo mais pela experiência de usuário que cada um proporciona e qual o usuário melhor se adapta e se sente mais confortável na utilização já que tanto o Kali Linux quanto o BlackArch Linux oferecem uma ampla gama de ferramentas para vários testes de segurança e testes de penetração. Os usuários podem selecionar as ferramentas que melhor se alinham aos seus requisitos e conhecimentos, a fim de realizar avaliações de segurança eficazes e garantir a resiliência da rede.



Serviço Público Federal
Ministério da Educação

Fundação Universidade Federal de Mato Grosso do Sul



O estudo realizado e aqui exposto das ferramentas presentes no BlackArch Linux e no Kali Linux se mostrou muito interessante, não apenas proporcionando grande satisfação e realização pessoal, mas também agregando valor do ponto de vista profissional, e abrindo possíveis oportunidades para o futuro pós graduação.

Campo Grande, 25 de novembro de 2023.

Gabriel Pastorello