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.

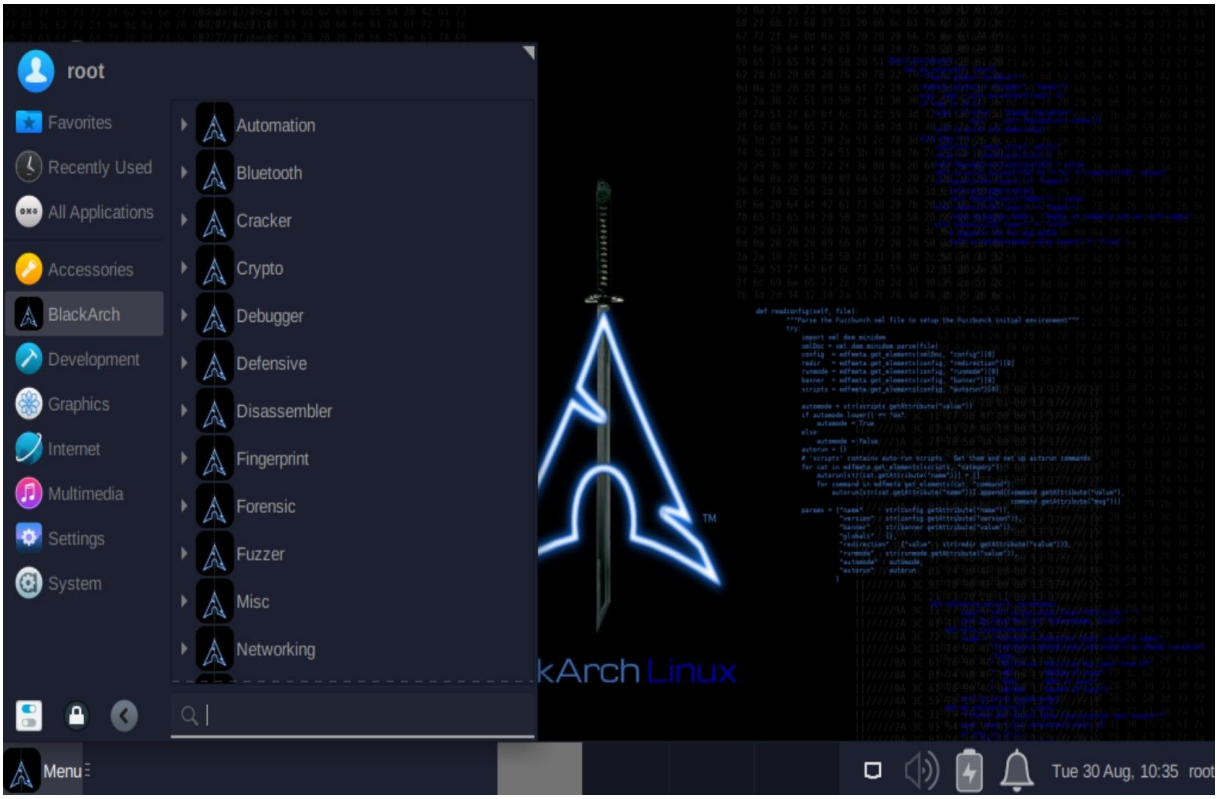
Kali Linux

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

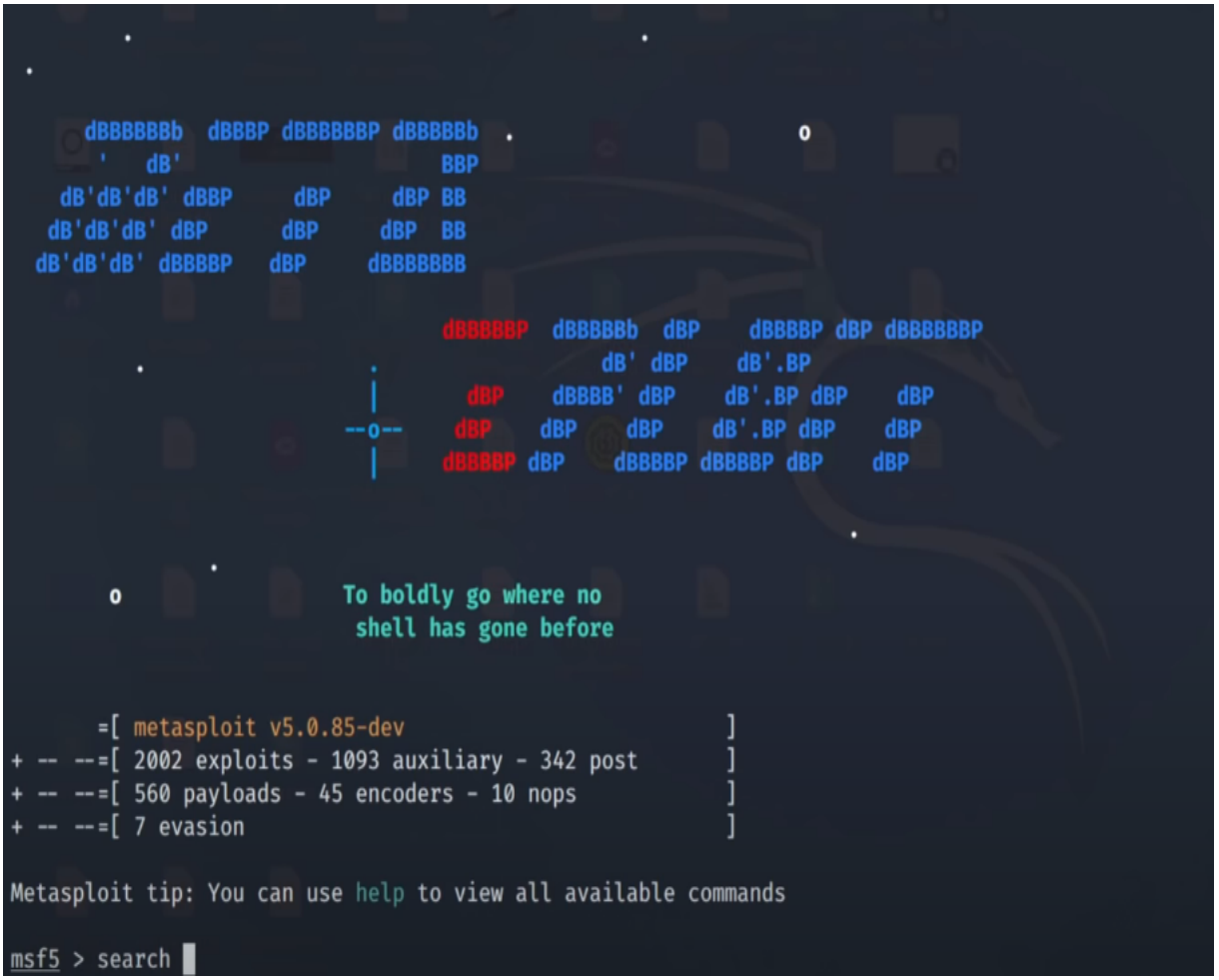
Kali Linux e Black Arch Linux oferecem uma gama abrangente de ferramentas para profissionais de segurança cibernética. Essas ferramentas cobrem vários aspectos de *hacking* e testes de penetração. Ambas as distribuições fornecem ferramentas conhecidas e disponíveis gratuitamente.

Metasploit

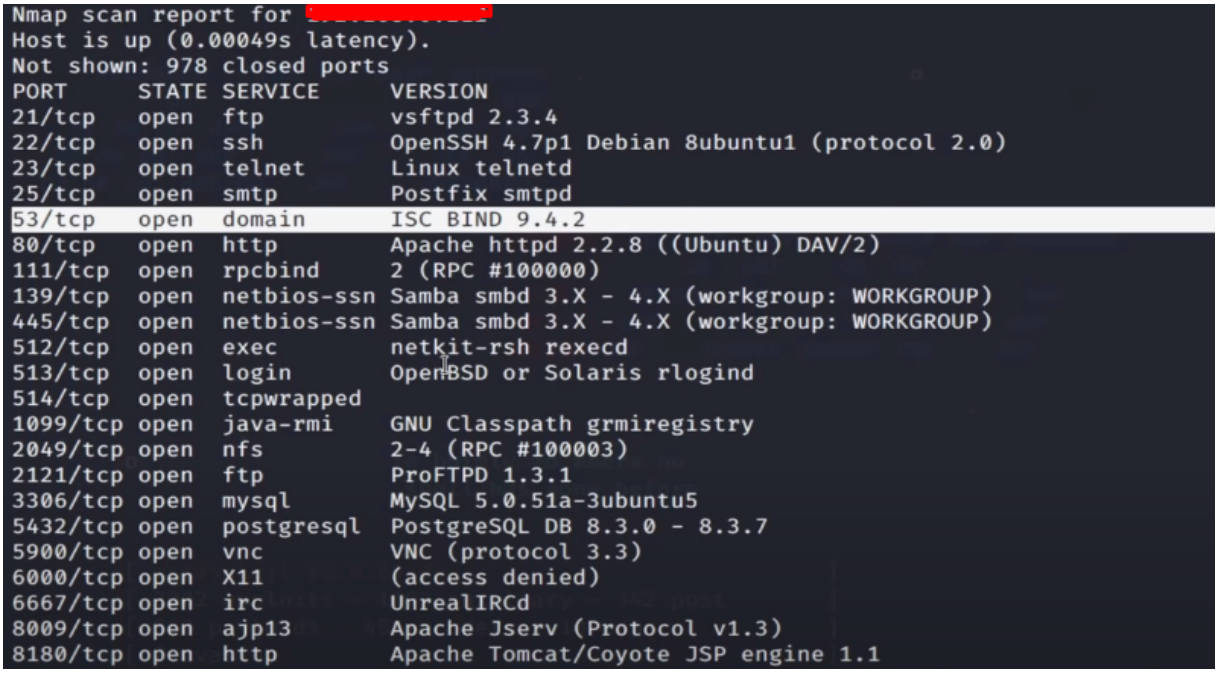
Metasploit é uma ferramenta para desenvolvimento e lançamento de *exploits* amplamente utilizada em auditorias e testes de penetração. O *framework* consiste em uma série de ferramentas, *exploits* e códigos que podem ser usados através de diferentes interfaces.

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.

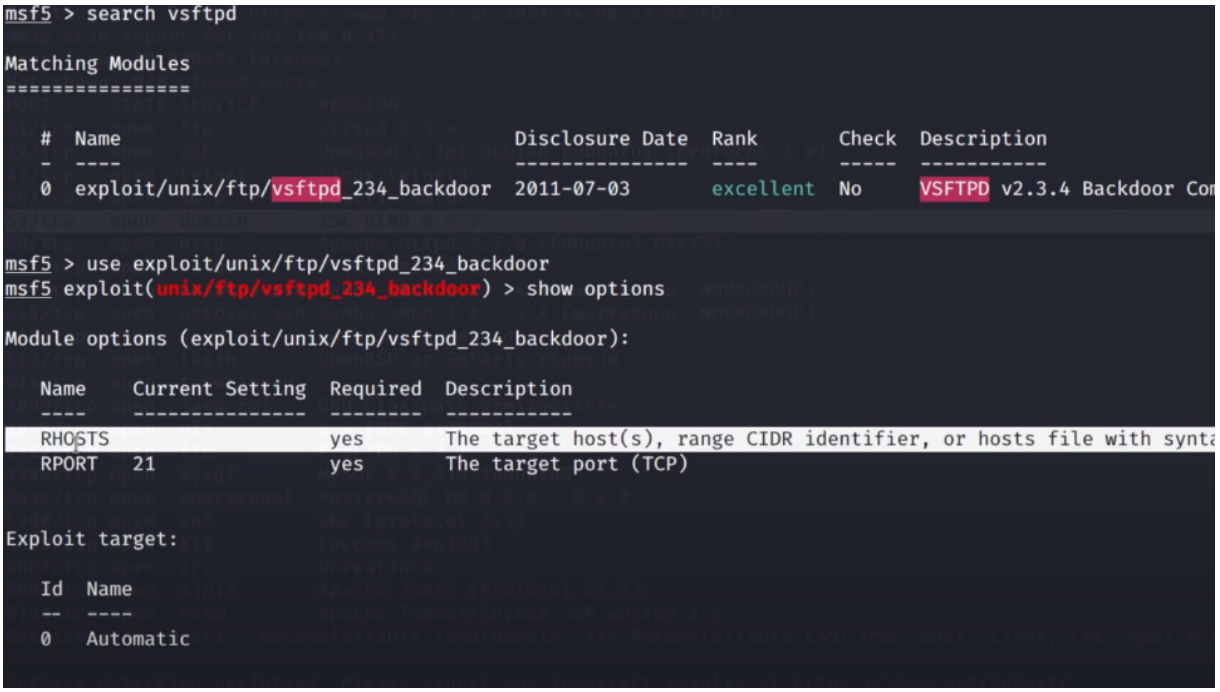
Inicialização do Metasploit:



Uso do Nmap como auxiliar:



Verificação de existência de exploit no Metasploit:



NMap

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

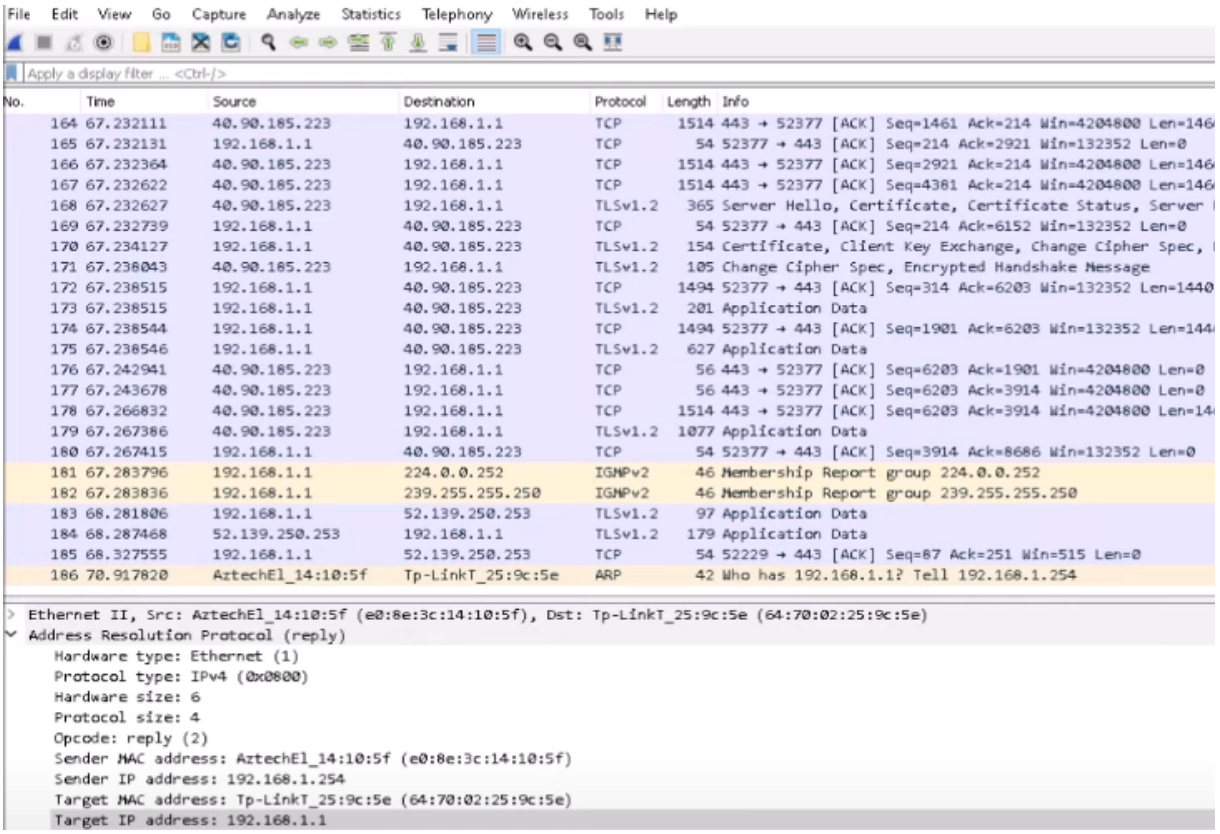
Exemplos de casos de uso do Nmap incluem mapeamento de arquiteturas de rede, identificação de portas e serviços abertos, detecção de vulnerabilidades potenciais em dispositivos de rede e realização de reconhecimento de rede.

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:



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.

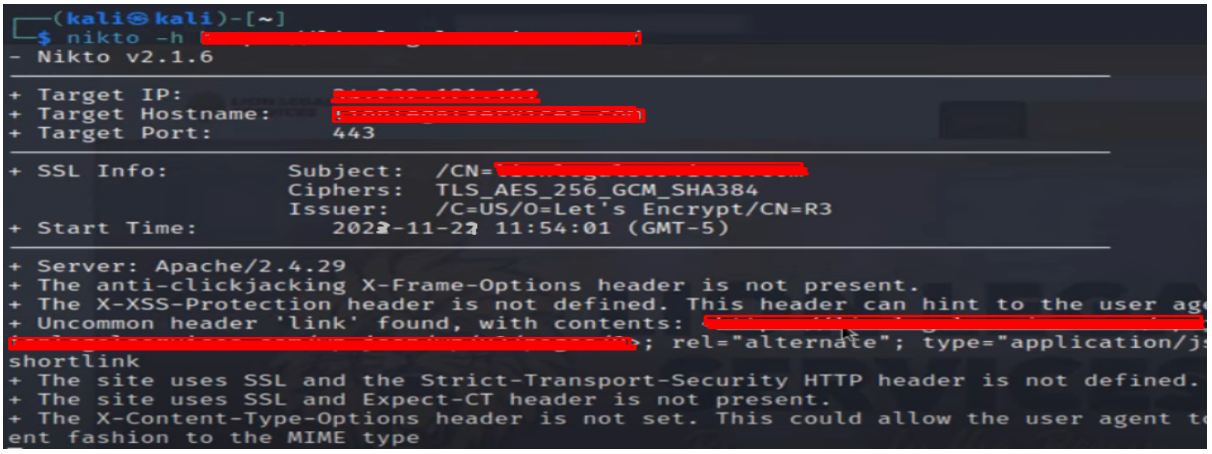
Exemplos de casos de uso do Hydra incluem teste de segurança de credenciais de login, realização de ataques de quebra de senha e realização de testes de penetração em sistemas com senhas fracas ou padrão.

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:



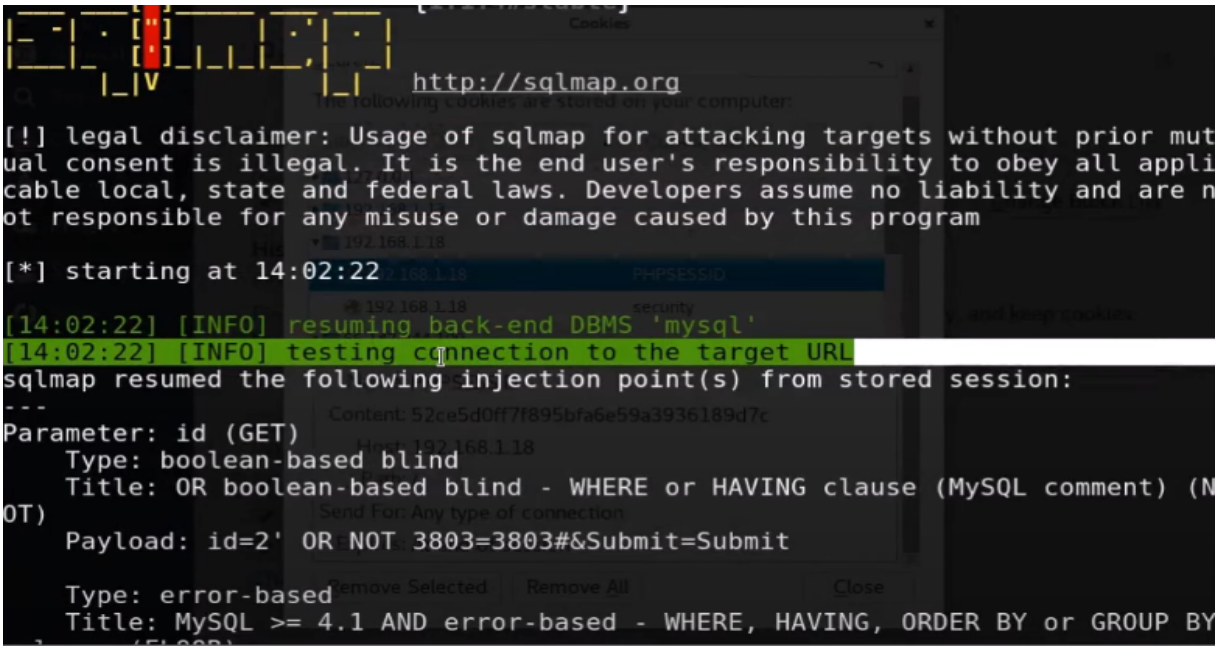
SQLMap

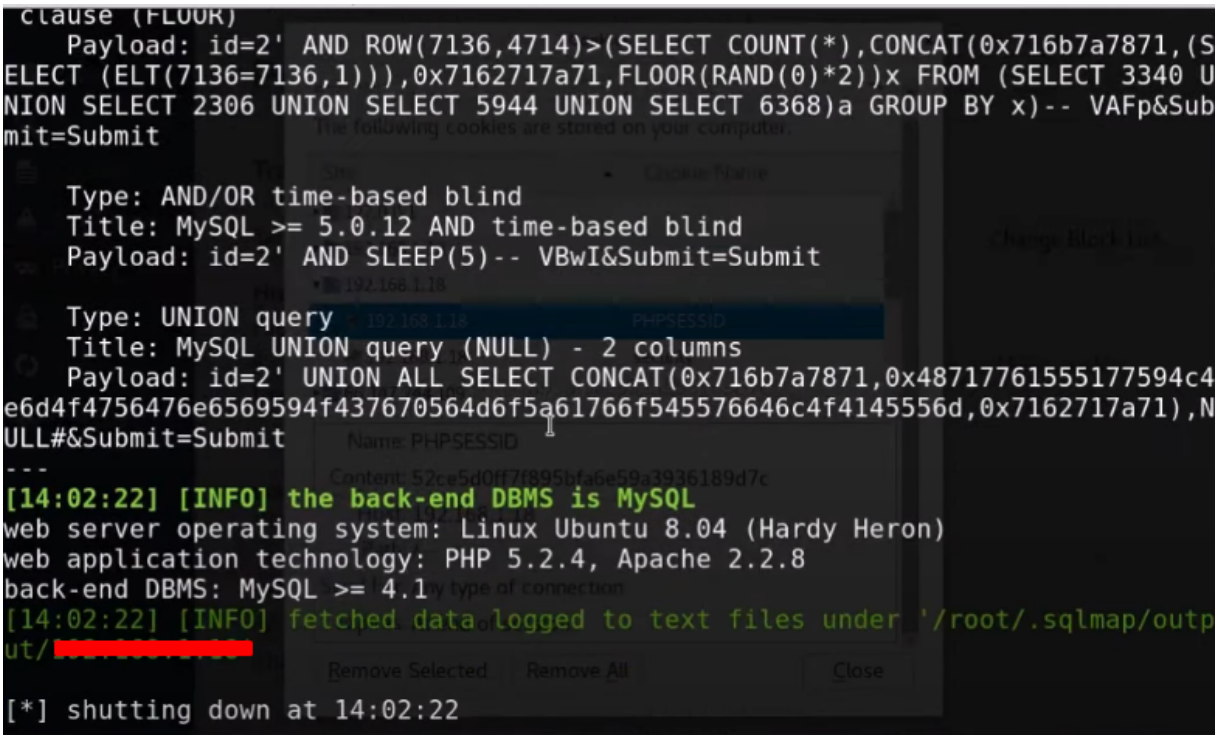
SQLMap é uma ferramenta usada para detecção e exploração automatizada de vulnerabilidades de injeção SQL em aplicações *web*.

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:



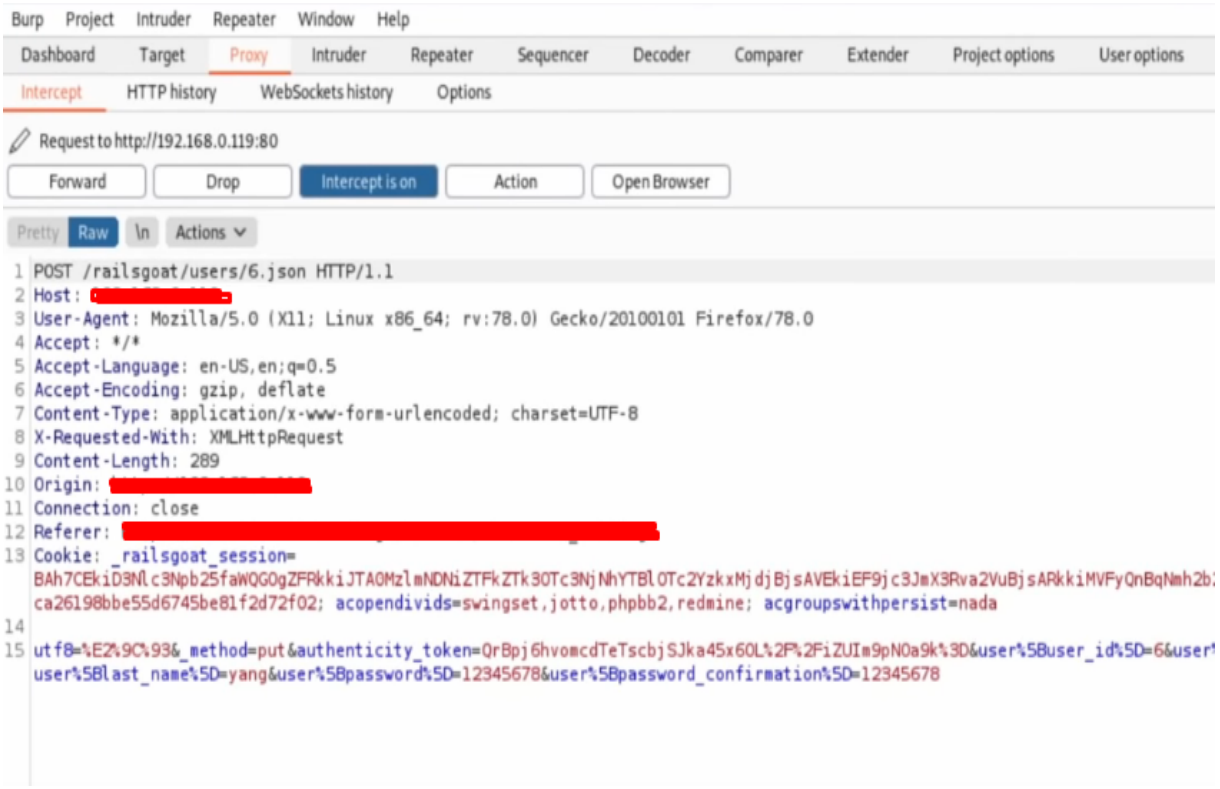


Burp Suite

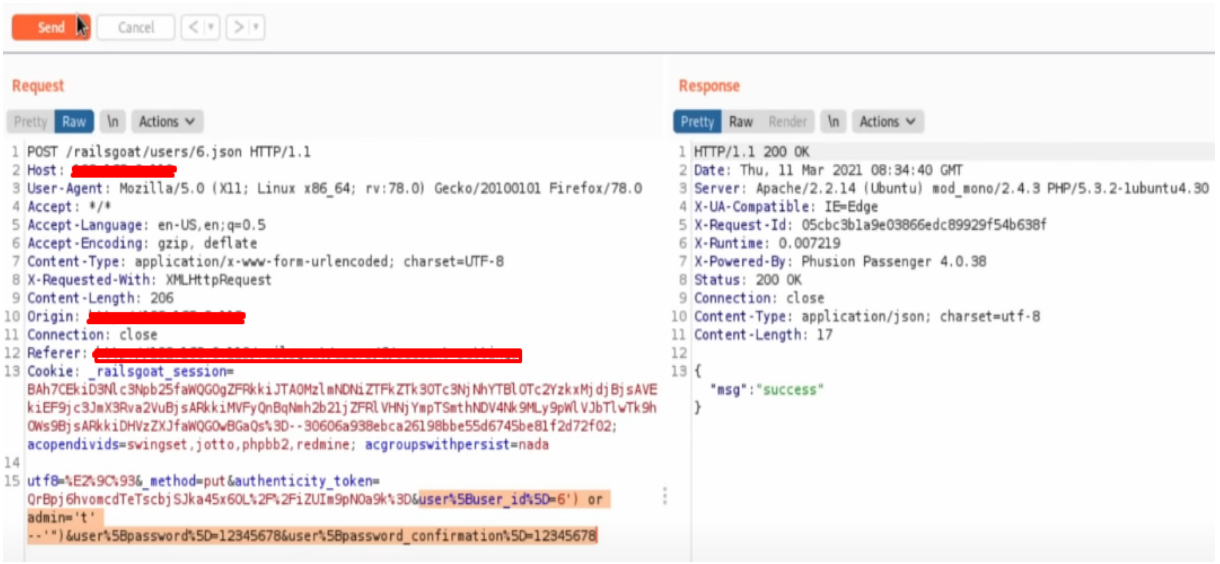
Burp Suite é uma ferramenta de teste de segurança de aplicativos da *web* que permite aos usuários interceptar, modificar e analisar solicitações e respostas HTTP/S.

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:



Exemplo de requisição modificada no Burp Suite com resposta de sucesso:



Exploit DB

ExploitDB é um banco de dados abrangente de explorações e vulnerabilidades que pode ser usado para fins de testes de penetração.

Exemplos de casos de uso do ExploitDB incluem pesquisar e encontrar explorações relevantes para vulnerabilidades específicas, testar a eficácia de estratégias de correção e gerenciamento de vulnerabilidades, compreender o impacto e a gravidade de vulnerabilidades conhecidas e conduzir exercícios de exploração direcionados em um ambiente controlado.

Reaver

Reaver é uma ferramenta especializada para ataques a redes sem fio, particularmente focada na exploração de vulnerabilidades em WPS.

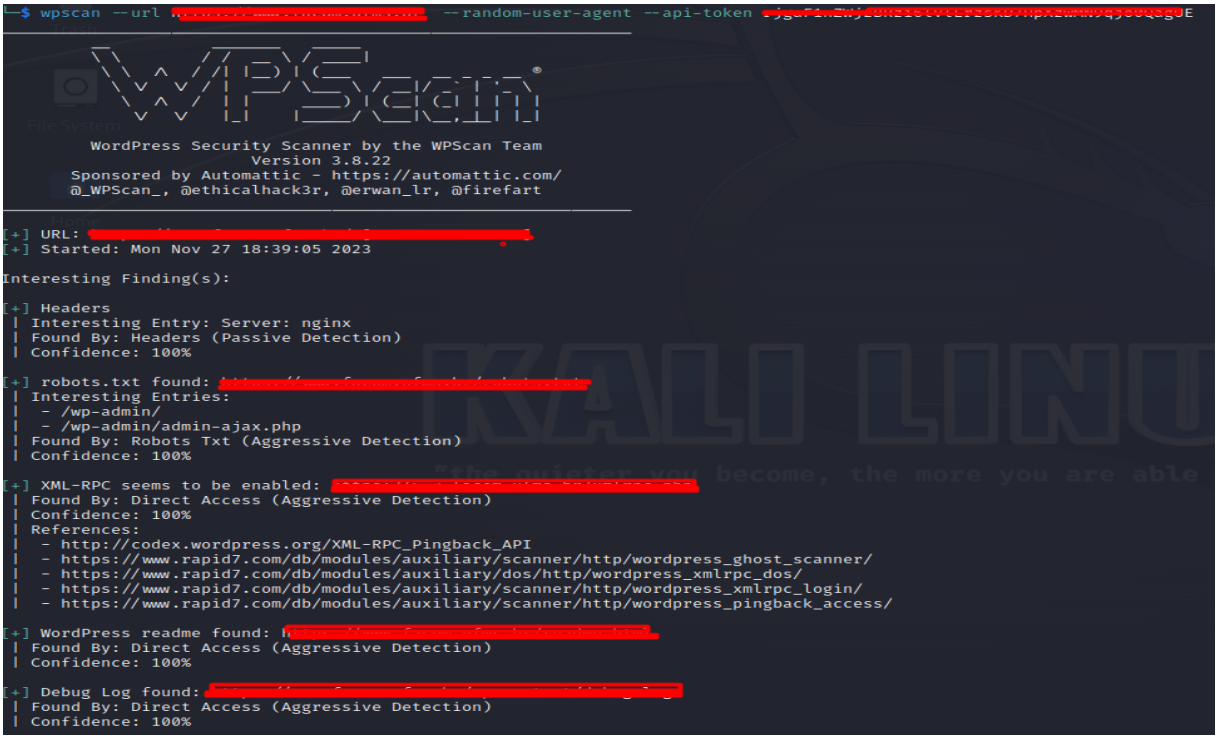
Exemplos de casos de uso do Reaver incluem testar a segurança de redes sem fio tentando quebrar o PIN WPS, avaliando a vulnerabilidade de roteadores e pontos de acesso a ataques WPS, avaliando a eficácia das medidas de segurança de dispositivos habilitados para WPS e conduzindo testes de penetração em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

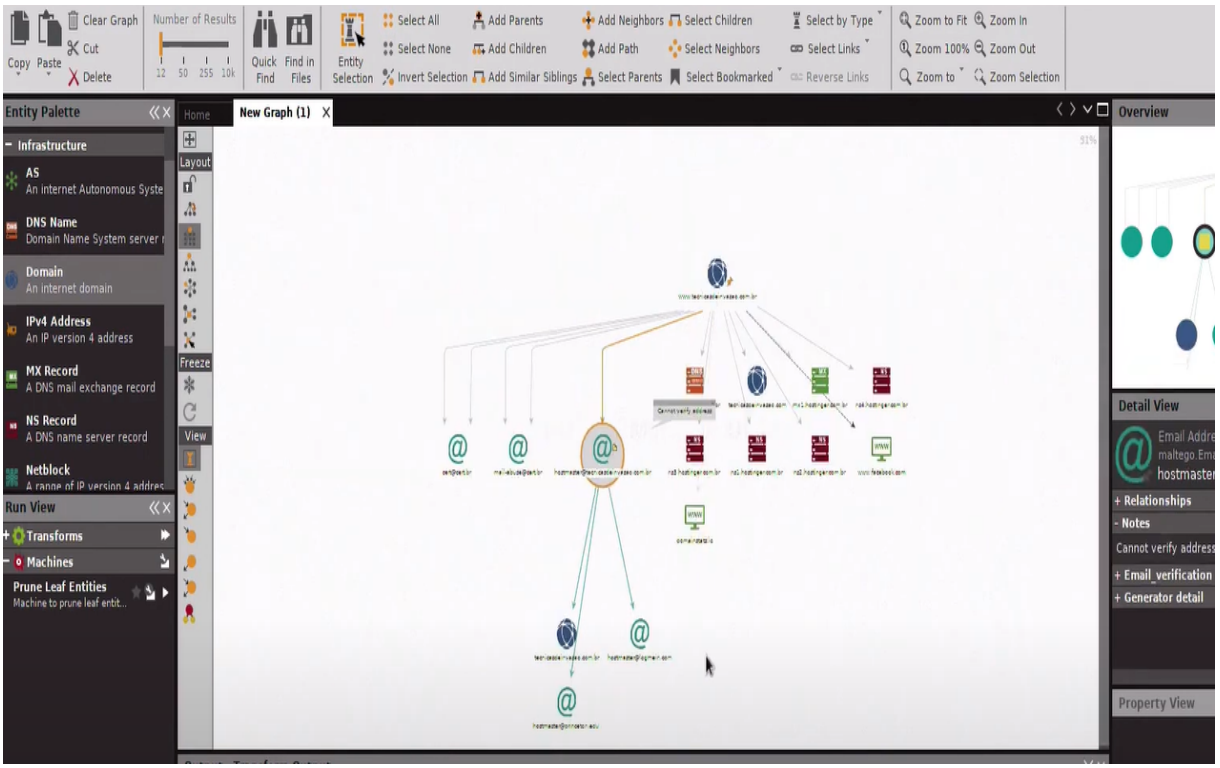


Maltego

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:



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 criptografía, 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.

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.

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.

gov.br
Documento assinado digitalmente
GABRIEL PASTORELLO DE OLIVEIRA
Data: 27/11/2023 21:00:45-0300
Verifique em https://validar.iti.gov.br

Gabriel Pastorello