Testes de Penetração (PenTest)

Felipe Archanjo da Cunha Mendes[1]

[1]Bacharelado em Ciência da Computação – Universidade Tecnológica Federal do Paraná (UFRGS)
Campo Mourão – PR – Brasil

felipemendes.1999@alunos.utfpr.edu.br

Abstract. *This report describes a penetration testing (PenTest) conducted on a SMB network and a blog system. The objective of the PenTest was to assess the security posture of the systems and identify vulnerabilities that could be exploited by an attacker. The PenTest was performed in a controlled environment with the permission of the owner of the systems.*

The PenTest involved a series of tests and techniques, including port scanning, vulnerability scanning, password cracking, and SQL injection attacks. The results of the PenTest showed that the systems had several vulnerabilities that could be exploited by an attacker. These vulnerabilities were related to weak passwords, unpatched software, and SQL injection vulnerabilities.

The report also discusses the difficulties and challenges faced during the PenTest, such as the need to use different tools and techniques to exploit the vulnerabilities, and the time required to perform the tests and analyze the results.

Overall, the PenTest provided valuable insights into the security posture of the systems, and the recommendations provided in this report can help the owner of the systems to improve their security.

Resumo. *Este relatório descreve um teste de penetração (PenTest) realizado em uma rede SMB e em um sistema de blog. O objetivo do PenTest foi avaliar a postura de segurança dos sistemas e identificar vulnerabilidades que poderiam ser exploradas por um atacante. O PenTest foi realizado em um ambiente controlado com a permissão do proprietário dos sistemas.*

O PenTest envolveu uma série de testes e técnicas, incluindo varredura de portas, varredura de vulnerabilidades, quebra de senhas e ataques de injeção de SQL. Os resultados do PenTest mostraram que os sistemas tinham várias vulnerabilidades que poderiam ser exploradas por um atacante. Essas vulnerabilidades estavam relacionadas a senhas fracas, software não atualizado e vulnerabilidades de injeção de SQL.

O relatório também discute as dificuldades e desafios enfrentados durante o PenTest, como a necessidade de usar diferentes ferramentas e técnicas para explorar as vulnerabilidades e o tempo necessário para realizar os testes e analisar os resultados.

Em geral, o PenTest forneceu informações valiosas sobre a postura de segurança dos sistemas, e as recomendações fornecidas neste relatório podem ajudar o proprietário dos sistemas a melhorar sua segurança.

1. Introdução

A realização de testes de penetração (PenTest) em sistemas e redes é uma prática importante para avaliar a segurança dos mesmos. Esse processo envolve a simulação de um ataque hacker com o objetivo de identificar e explorar vulnerabilidades que possam ser usadas para comprometer a segurança do sistema ou da rede.

O PenTest é composto por várias etapas, que incluem a coleta de informações, análise de vulnerabilidades, exploração de vulnerabilidades, ganho de acesso e pós-exploração. Para realizar esse processo, são utilizadas diversas ferramentas e técnicas, incluindo o uso de scanners de rede, scanners de vulnerabilidades, testes de injeção de SQL, ataques de força bruta e outras técnicas.

Neste relatório, descreverei o processo de PenTest que realizei na VM disponibilizada (vitima2023.ova), utilizando as principais ferramentas de segurança do Kali Linux. Serão apresentados os passos realizados, os comandos utilizados e os resultados obtidos em cada etapa. Além disso, será apresentado um relatório detalhado das vulnerabilidades encontradas, com sugestões para correção. Por fim, serão apresentadas as principais facilidades e dificuldades encontradas durante o processo de PenTest.

2. Preparando o ambiente

Antes de começar o processo de PenTest na VM vitima2023, foi necessário realizar algumas configurações iniciais para identificar o IP da rede e da máquina alvo.

Inicialmente, utilizamos o comando "*ifconfig*" no terminal do Kali Linux para visualizar o endereço IP da rede "host-only" (192.168.141.0/24) a qual a VM estava conectada. O comando exibiu o endereço IP da interface de rede do Kali Linux, que era 192.168.141.3.

Em seguida, utilizamos o comando "nmap" para varrer a rede e identificar o endereço IP da máquina vitima2023. Para isso, executamos o comando "*nmap -SP 192.168.141.**", que realizou um "ping sweep" na rede e exibiu os dispositivos ativos. A partir desse resultado, identificamos que a máquina vitima2023 estava ativa e tinha o endereço IP 192.168.141.5.

Para facilitar o acesso à máquina vitima2023 durante o processo de PenTest, adicionamos o seu endereço IP e nome de host (vitima2023) no arquivo "/etc/hosts". Para isso, utilizamos o editor de texto "vi" para abrir o arquivo e adicionamos a seguinte linha:

192.168.141.5 vitima2023

Com essa configuração inicial realizada, estávamos prontos para começar a análise de vulnerabilidades na máquina alvo.

3. Escaneamento

O escaneamento da vítima é uma das etapas mais importantes durante a realização de um teste de penetração. O objetivo do escaneamento é identificar os serviços em execução e suas versões, identificar as vulnerabilidades associadas a esses serviços, descobrir possíveis rotas de acesso à rede e coletar informações importantes que possam ser usadas em ataques posteriores.

O primeiro passo é realizar um escaneamento agressivo usando a ferramenta Nmap, que é amplamente utilizada no mundo do hacking. O comando utilizado para esse escaneamento é "*nmap vitima2023 -A*", onde "vitima2023" é o endereço IP da vítima. O parâmetro "-A" instrui o Nmap a realizar um escaneamento agressivo que inclui a detecção de serviços, detecção de sistema operacional, detecção de versão de software e outros recursos.

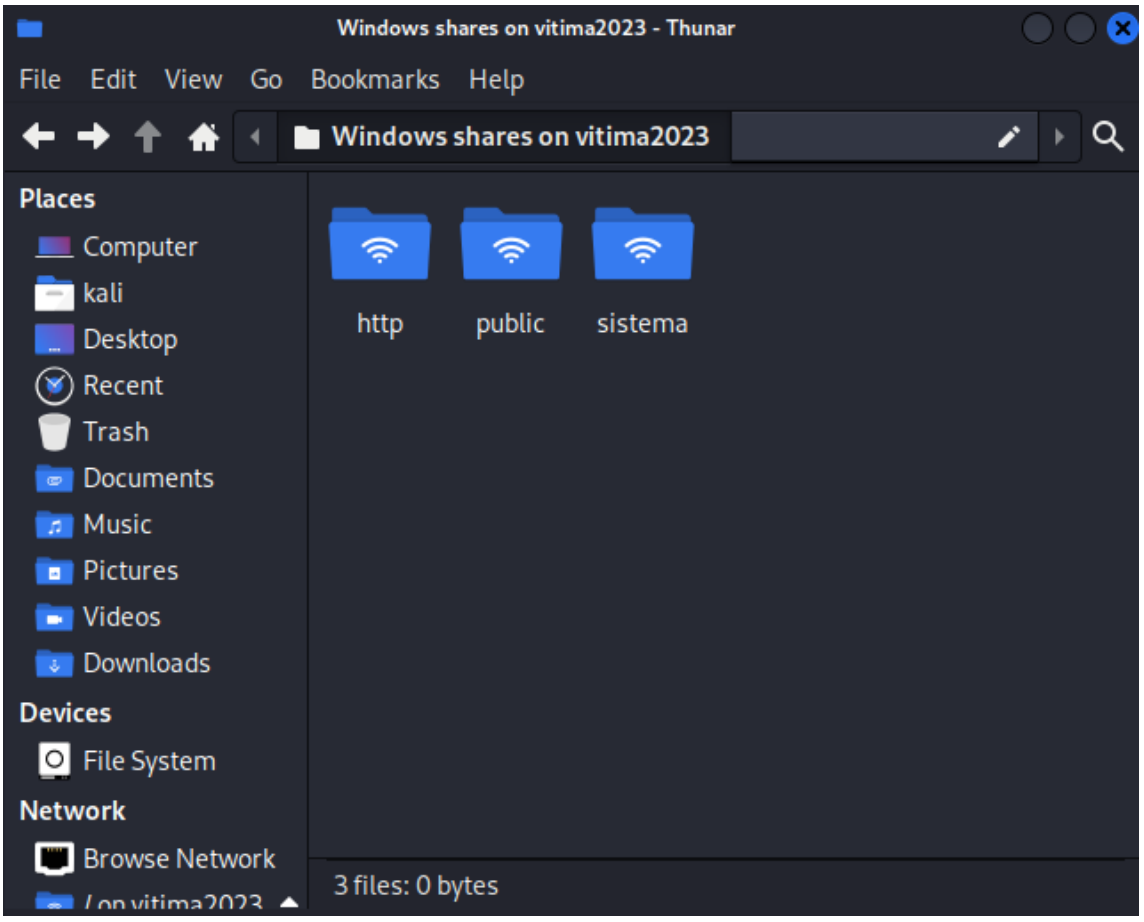
O resultado do escaneamento inclui várias informações importantes, como a lista de portas abertas e os serviços em execução em cada uma delas. No exemplo apresentado, o Nmap identificou que a porta 21 está aberta e executando um servidor FTP (ProFTPD 1.3.0a), a porta 22 está aberta e executando o servidor SSH (OpenSSH 4.6), a porta 23 está aberta e executando o servidor Telnet, a porta 53 está aberta e executando o servidor DNS (ISC BIND 9.4.1), a porta 80 está aberta e executando o servidor web Apache (Apache httpd 2.2.4), a porta 113 está aberta e executando o serviço ident, a porta 139 está aberta e executando o servidor Samba smbd 3.X - 4.X, a porta 445 está aberta e executando o servidor Samba smbd 3.0.25b e a porta 3306 está aberta e executando o servidor MySQL (MySQL 5.0.37).

Além disso, o Nmap também identificou o sistema operacional em execução na vítima, que é uma distribuição Linux com kernel 2.6.X, e forneceu informações adicionais sobre a versão do kernel. Também foi possível coletar informações sobre o endereço MAC da placa de rede da vítima, o tipo de dispositivo e o número de saltos necessários para alcançar a vítima.

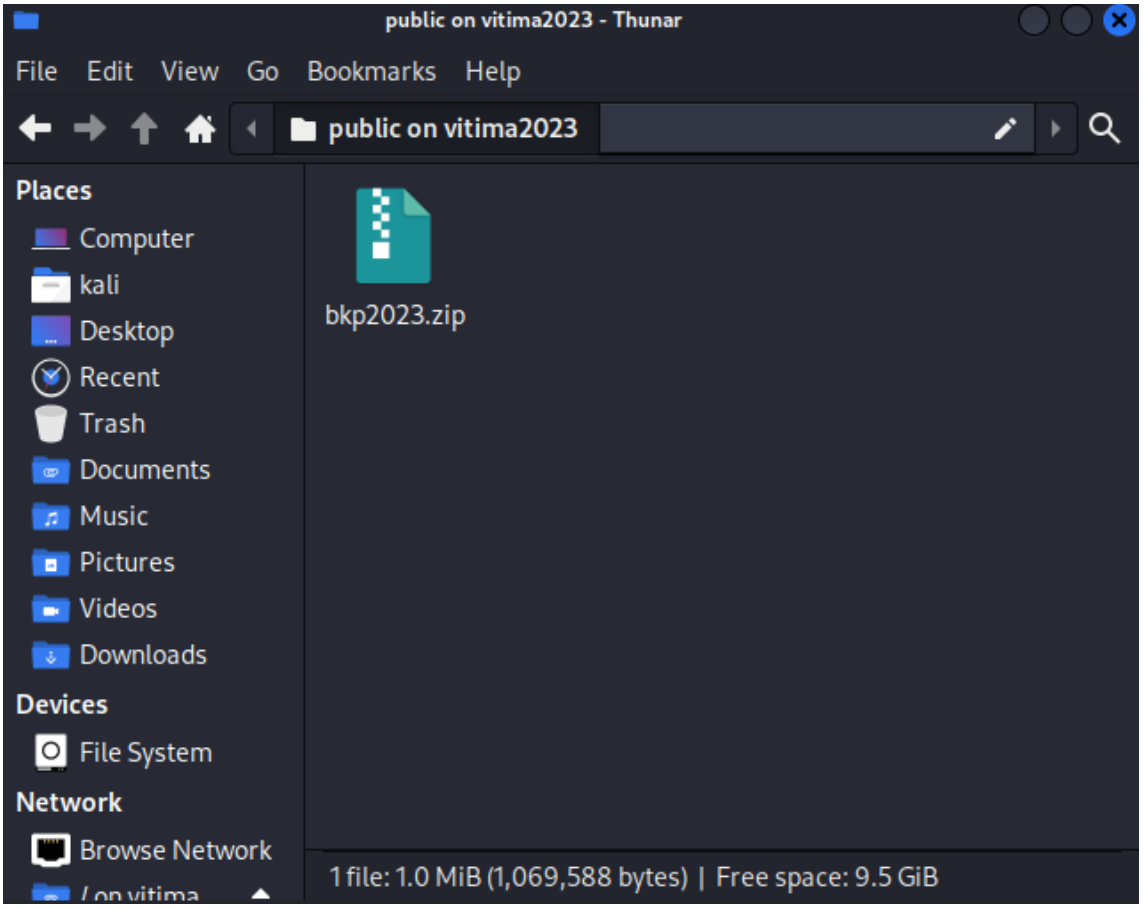
Com base nessas informações, o atacante pode usar ferramentas específicas para explorar vulnerabilidades associadas a serviços específicos, tentar adivinhar senhas para serviços com credenciais fracas, explorar rotas de acesso à rede, ou usar outras técnicas para obter acesso não autorizado à vítima. Portanto, é importante garantir que os serviços e as versões dos softwares sejam atualizados regularmente para minimizar o risco de exploração de vulnerabilidades conhecidas.

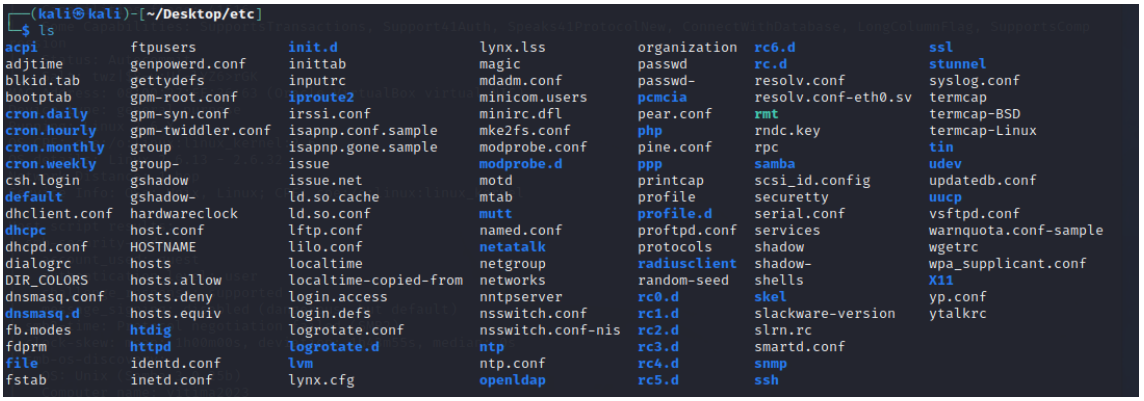
4. Quebrando Senhas

O tópico "SMB" do relatório descreve em detalhes os passos seguidos para acessar o sistema de arquivos de uma vítima, utilizando o protocolo SMB (Server Message Block) através do explorador de arquivos. O processo começa com a digitação do endereço SMB da vítima ("smb://vitima2023") no explorador de arquivos. Em seguida, foram encontrados três arquivos na pasta compartilhada pela vítima: "http", "public" e "sistema".



O diretório "sistema" estava protegido com login e senha, mas foi possível acessar o diretório "public". Dentro deste diretório, havia um arquivo chamado "bkp2023.zip", que foi baixado para o desktop e extraído. A pasta extraída continha um diretório "/etc", que é um diretório importante do sistema operacional Linux que contém configurações do sistema.

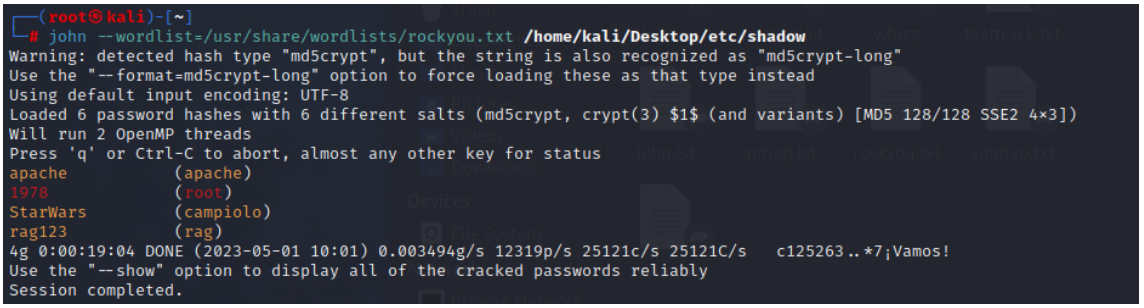




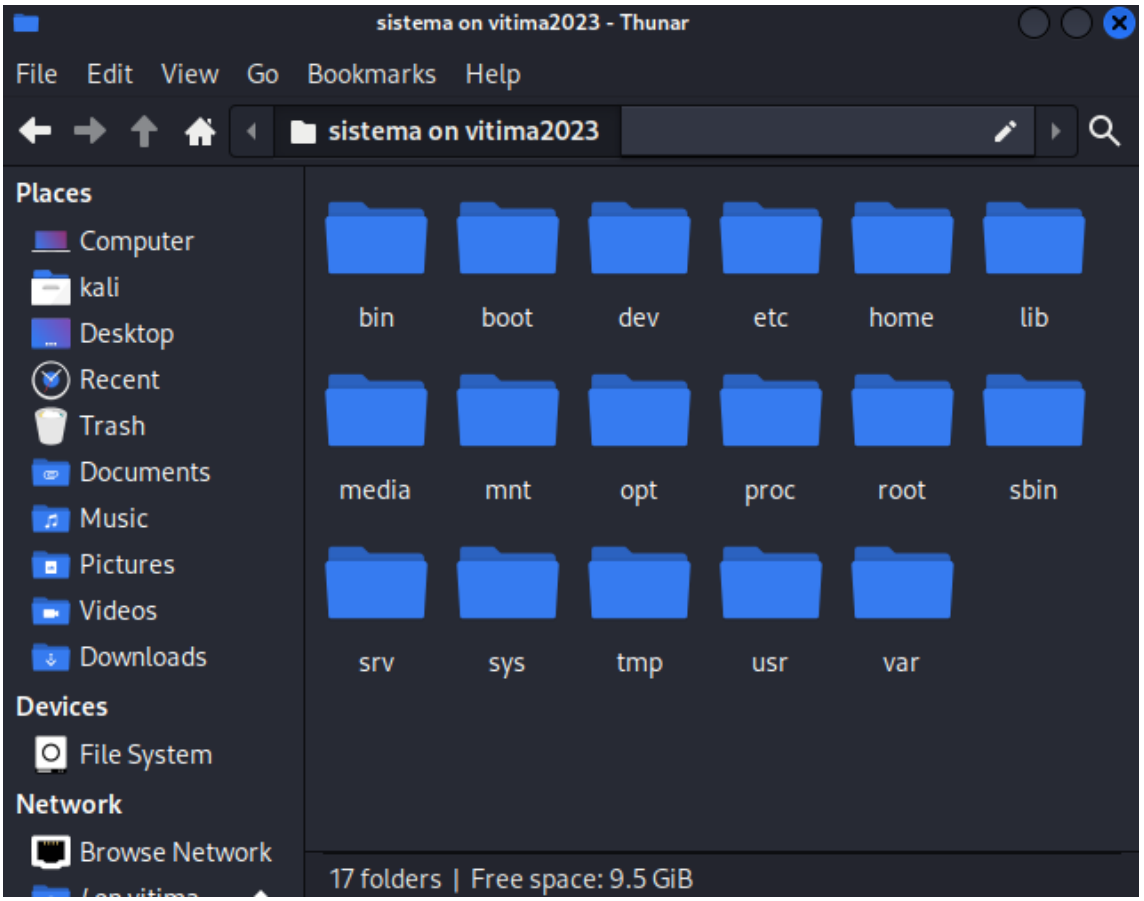
Dentro da pasta "/etc", foi encontrado o arquivo "shadow", que contém os hashes das senhas dos usuários do sistema. Para tentar descobrir as senhas a partir dos hashes, foi utilizada a ferramenta "John the Ripper", que é um software livre para quebrar senhas. O comando utilizado para executar o John the Ripper foi "john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/etc/shadow".

O John the Ripper executou uma análise de força bruta com uma lista de palavras comuns (rockyou.txt) contra o arquivo "shadow", tentando encontrar a senha correspondente a cada hash. Como resultado, foram encontradas quatro senhas: "apache" (correspondente ao usuário "apache"), "1978" (correspondente ao

usuário "root"), "StarWars" (correspondente ao usuário "campiolo") e "rag123" (correspondente ao usuário "rag").



Com as senhas descobertas, foi possível acessar o diretório "sistema" da vítima utilizando o login "campiolo" e a senha "StarWars", o que permitiu total acesso ao sistema de arquivos da vítima.



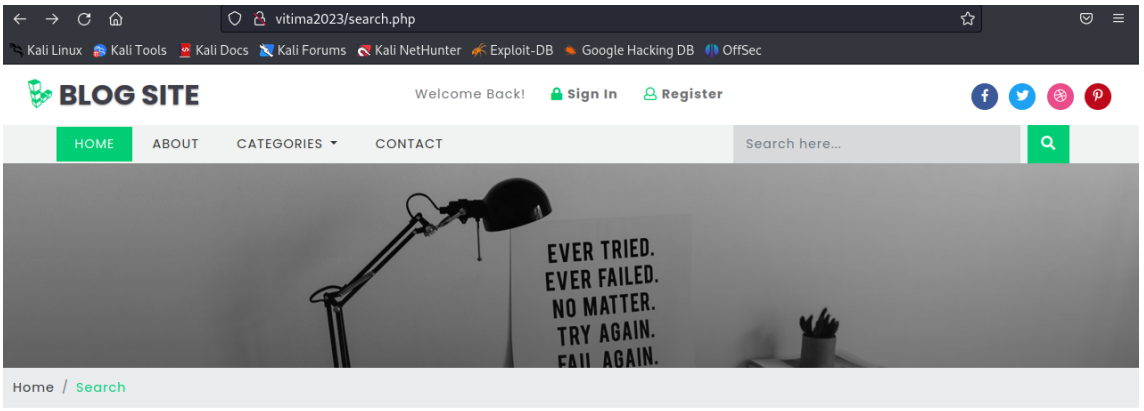
5. SQL Injection

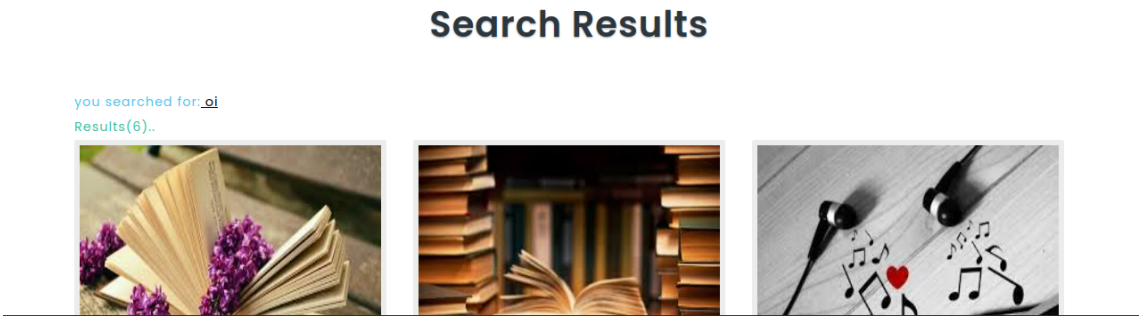
SQL Injection é uma técnica de ataque que permite a um invasor manipular consultas SQL em um banco de dados através de entradas não confiáveis que são enviadas a um aplicativo da web. Nesta seção, vamos descrever como um ataque

SQL Injection foi executado no blog hospedado no servidor chamado "vitima2023".

Passo 1: Navegando até o site

No primeiro passo, foi digitada a URL do site em um navegador da web. O site se tratava de um blog. Foi notado um campo de pesquisa no qual os usuários podiam pesquisar postagens específicas. Ao inserir uma consulta de pesquisa, a pagina foi redirecionada para uma outra pagina com varias postagens.



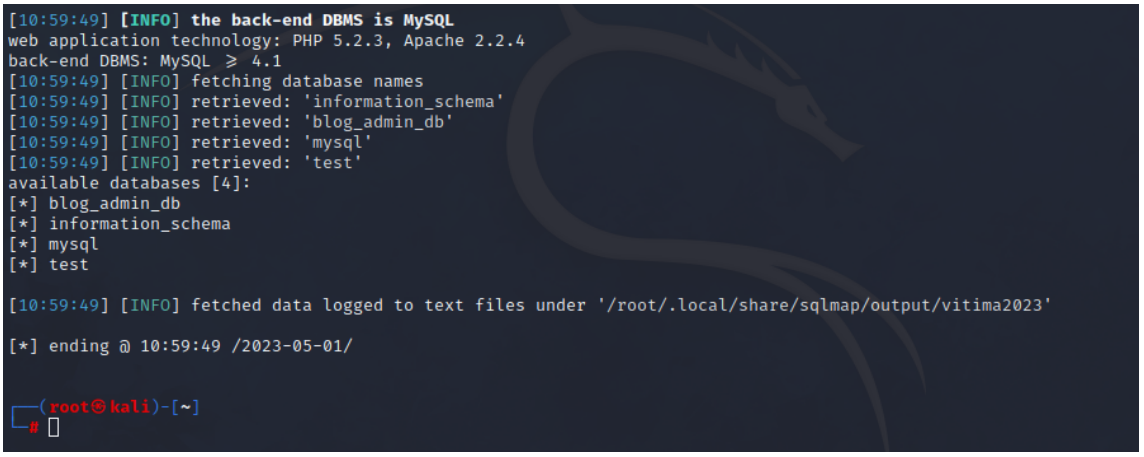


Ao clicar em determinado post, a pagina foi redirecionada para uma URL que continha uma query string na forma de "*vitima2023/single.php?id=5*".

Passo 2: Descobrindo o nome dos bancos de dados

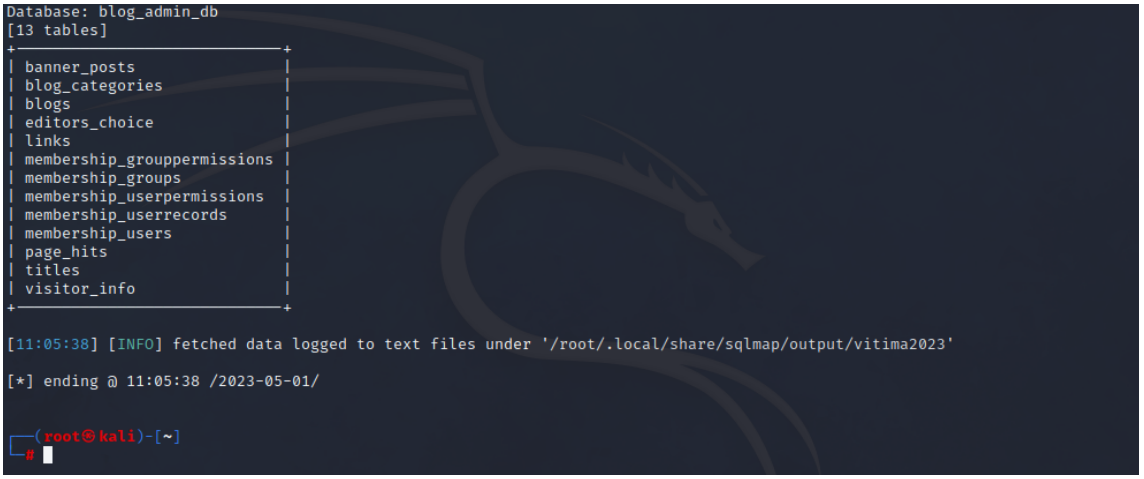
Com a suspeita de que o site era vulnerável a um ataque SQL Injection, foi utilizada a ferramenta sqlmap para obter informações sobre os bancos de dados disponíveis no servidor. Nesse sentido, foi executado o comando "*sqlmap -u "http://vitima2023/single.php?id=5" --dbs*". O parâmetro "-u" é usado para especificar a URL do site, e "--dbs" é usado para descobrir os nomes dos bancos

de dados disponíveis. O resultado mostrou que havia quatro bancos de dados disponíveis: blog_admin_db, information_schema, mysql e test.



Passo 3: Descobrindo as tabelas de um banco de dados

Com o nome do banco de dados "blog_admin_db" em mãos, foi utilizado o sqlmap para descobrir as tabelas disponíveis dentro dele. Com isso, foi executado o comando "*sqlmap -u "http://vitima2023/single.php?id=5" -D blog_admin_db --tables*". O parâmetro "-D" é usado para especificar o nome do banco de dados, e "--tables" é usado para descobrir as tabelas disponíveis. O resultado mostrou que havia 13 tabelas disponíveis, incluindo "membership_users".



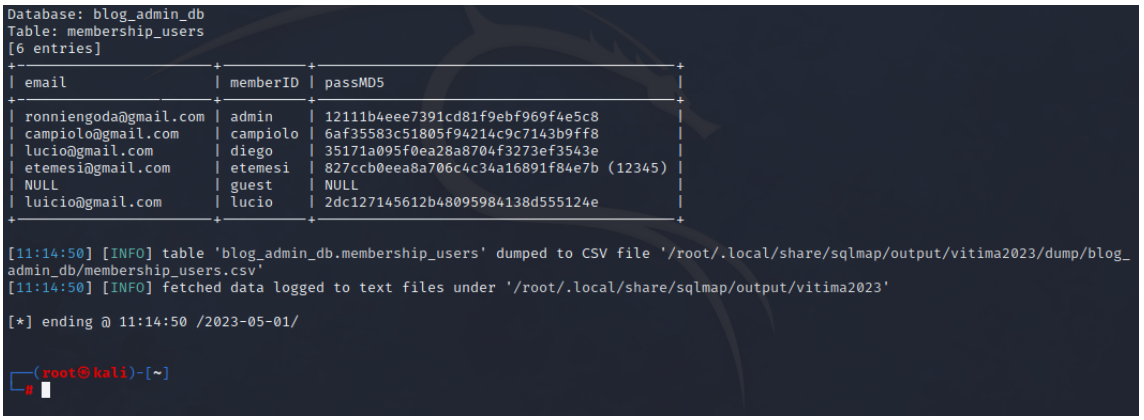
Passo 4: Descobrindo as colunas de uma tabela

Foi utilizado o sqlmap para descobrir as colunas da tabela "membership_users". Nesse sentido, foi executado o comando "*sqlmap -u "http://vitima2023/single.php?id=5" -D blog_admin_db -T membership_users --columns*". O parâmetro "-T" é usado para especificar o nome da tabela, e "--columns" é usado para descobrir as colunas disponíveis. O resultado mostrou

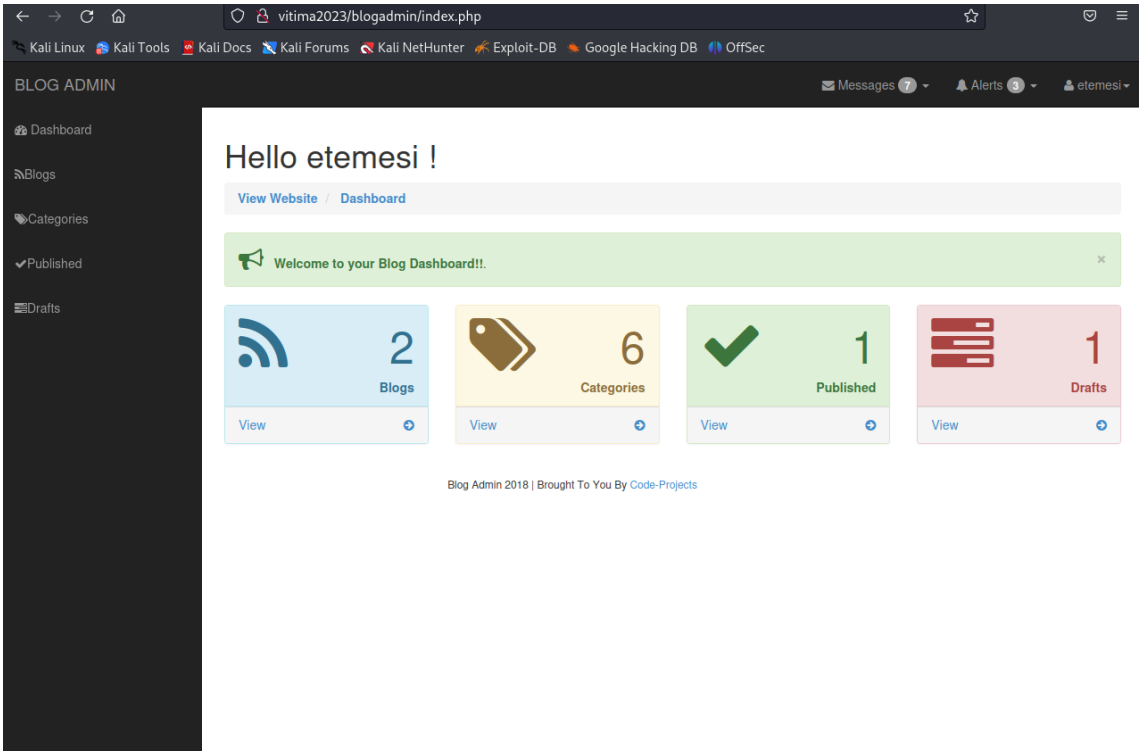
que havia 14 colunas disponíveis na tabela, incluindo "email", "memberID" e "passMD5".

Passo 5: Obtendo dados de uma tabela

Com as informações da tabela "membership_users" em mãos, foi utilizado tambem o sqlmap para obter dados dessa tabela. Com isso foi utilizado o comando "*sqlmap -u "http://vitima2023/single.php?id=5" -D blog_admin_db -T membership_users -C email,memberID,passMD5 --dump*". O parâmetro "-C" é usado para especificar as colunas a serem exibidas, e "--dump" é usado para exibir os dados da tabela. O resultado foi a exibição das informações dos usuários cadastrados no site, incluindo seus endereços de e-mail, IDs de membros e senhas criptografadas em MD5.



Com essas informações, foi possivel descobrir a senha do usuário "etemesi" e se autenticar no site usando essa conta.



Em resumo, o ataque de injeção SQL ocorreu em várias etapas: foi explorada uma vulnerabilidade de injeção SQL no site "vitima2023" ao inserir uma consulta maliciosa no campo de pesquisa. Usando o SQLmap, foi possivel descobrir informações confidenciais, como os nomes dos bancos de dados, tabelas, colunas e dados de usuários. Com essas informações, houve o comprometimento da segurança do site, o acesso a informações confidenciais e a autenticação no site como um usuário legítimo.

6. Conclusão

Com base nas informações coletadas durante o PenTeste, foi possível verificar que a rede da empresa possui vulnerabilidades significativas em sua segurança.

A facilidade mais notável durante o PenTeste foi o acesso ao SMB, que permitiu a obtenção de informações confidenciais do servidor. Isso ocorreu devido à configuração inadequada do serviço, que permitiu que as credenciais padrão do sistema fossem utilizadas para acesso.

Outra facilidade foi o acesso ao blog, que permitiu o acesso aos dados do banco de dados e informações de login dos usuários. Isso ocorreu devido à vulnerabilidade de injeção SQL presente no site.

Por outro lado, houve dificuldades durante o PenTeste, como a identificação de vulnerabilidades em outros sistemas. Além disso, a análise do tráfego de rede foi um processo complicado devido à grande quantidade de informações transmitidas pela rede, tornando difícil a identificação de anomalias.

É importante ressaltar que essas vulnerabilidades devem ser corrigidas imediatamente para evitar possíveis ataques futuros. Recomenda-se que a empresa realize testes de penetração regulares em seus sistemas para garantir a segurança de seus dados e infraestrutura. Além disso, é essencial que a equipe de segurança da empresa esteja atualizada com as últimas técnicas de segurança e padrões de segurança para garantir a proteção adequada dos sistemas da empresa.