Engenharia de Telecomunicações e Informática

Segurança em Redes e Sistemas de Informação

Testes de Penetração para a BLACKHOLE Inc.

João Rabuge | 98509

Bernardo Assunção | 98616

Hugo Costa | 93910

Docente:

Nuno Filipe Martins de Silveira Reis

Ano curricular: 4º

Semestre: 1º

Semestre **2023/2024**

Índice

1. Introdução 1
2. Metodologia 2
2.1. Pre-Engagement Interactions 2
2.2. Intelligence Gathering 3
2.3. Threat Modelling 4
2.4. Vulnerability Analysis 4
2.5. Exploitation 5
2.6. Post-Exploitation 5
2.7. Reporting 6
3. Execução de Testes de Penetração 6
3.1. Pre-Engagement Interactions 6
3.2. Intelligence Gathering 8
3.3. Threat Modeling 10
3.4. Vulnerability Analysis 11
3.5. Exploitation 12
3.6. Post-Exploitation 13
3.7. Report 14
3.7.1. Sumário Executivo 14
3.7.2. Detalhes Técnicos 15
3.7.3. Resultados 16
3.7.4. Conclusões e Recomendações 16
3.7.4.1. Conclusão 17
3.7.4.2. Recomendações 17
4. Conclusão Projeto 19
5. Bibliografia 20

Índice Tabelas

Tabela 1 - Ping Sweep da Rede 7
Tabela 2 - Host Ativos na Rede..... 7
Tabela 3 - Comando para verificar portos abertos no Host 192.168.1.1 8
Tabela 4 - Resposta 192.168.1.1 8
Tabela 5 - Comando para verificar portos abertos no Host 192.168.1.106 8
Tabela 6 - Resposta 192.168.1.106 9
Tabela 7 - Comando para verificar portos abertos no Host 192.168.1.105 9
Tabela 8 - Resposta 192.168.1.105 9
Tabela 9 - Comando para verificar vulnerabilidade de versão 11
Tabela 10 - Resposta por parte da base de dados.....11
Tabela 11 - Comando para tentar executar exploit no host 192.168.1.105 12
Tabela 12 - Endereços IP dos host ativos da rede..... 15

1. Introdução

Este relatório descreve o projeto de **avaliação de segurança** realizado para a **empresa BLACKHOLE Inc.** A empresa, que presta serviços a uma ampla gama de clientes, possui vários ativos digitais críticos, como **serviços online**, **aplicações** e **dados em diferentes servidores**.

Dada a crescente ameaça de **ataques cibernéticos** e a importância de manter a **integridade** e a **segurança** dos seus ativos digitais, a BLACKHOLE Inc. decidiu realizar uma **avaliação de vulnerabilidade** extensa dos seus **ativos digitais**. Para esta tarefa, a empresa contratou a nossa equipa de **segurança cibernética**.

O objetivo deste projeto é conduzir uma **avaliação de segurança** e realizar **testes** nos seus **ativos mais críticos**. Este processo, também conhecido como **teste de penetração** ou **pen-testing**, envolve a **identificação** e **exploração** de **vulnerabilidades potenciais** nos sistemas da BLACKHOLE Inc.

Este projeto é especialmente relevante num momento em que as ameaças cibernéticas são cada vez mais **sofisticadas** e **frequentes**. Ao identificar e **corrigir vulnerabilidades**, a BLACKHOLE Inc. pode proteger os seus **ativos digitais** e as **informações** dos seus clientes de maneira mais **eficiente**, garantindo assim a continuidade dos seus negócios e a confiança dos seus clientes.

No decorrer deste relatório, iremos descrever a **metodologia** utilizada, os **sistemas selecionados** para teste, os **resultados** do pen-testing e as **recomendações** para melhorar a segurança dos sistemas da BLACKHOLE Inc.

2. Metodologia

Para a realização deste projeto, optamos por utilizar a metodologia Pen**etration Testing Execution Standard (PTES)**. Essa metodologia é amplamente reconhecida e adotada na indústria de **segurança cibernética** e fornece uma lógica clara para a condução dos testes de penetração.

A metodologia PTES engloba as seguintes etapas:

- **Pre-Engagement Interactions;**
- **Intelligence Gathering;**
- **Threat Modeling;**
- **Vulnerability Analysis;**
- **Exploitation**;
- **Post Exploitation;**
- **Reporting.**

Estas etapas irão ser devidamente explicadas **mais adiante** neste relatório.

2.1. Pre-Engagement Interactions

Nesta primeira fase do projeto, estabelecemos as bases para a condução do nosso **teste de penetração**. A principal tarefa desta fase é definir o **objetivo do projeto** e as **regras de engajamento**. Isto significa que precisamos determinar **quais sistemas** serão incluídos no teste e quais serão as **condições** sob as quais o teste será realizado.

Para a BLACKHOLE Inc., decidimos incluir os seus **ativos digitais mais críticos** no escopo do nosso projeto. Estes incluem os seus **serviços online**, **aplicações** e os **dados** hospedados em seus servidores. Estes sistemas foram escolhidos devido à sua importância para as **operações comerciais** da empresa e ao potencial impacto de qualquer comprometimento de segurança.

As regras de engajamento definem **como o teste de penetração** será **realizado**. Estas regras foram estabelecidas em consulta com a BLACKHOLE Inc. para garantir que o teste seja realizado de forma **ética** e **legal**. Por exemplo, acordamos em realizar os testes durante **períodos específicos** (Maintenance Windows) para **minimizar** o impacto nas operações comerciais. Além disso, todas as atividades serão **documentadas** em detalhes para fornecer uma visão clara do sucedido nos testes.

Para garantir a conformidade com as **leis** e **regulamentos**, também obtivemos permissão formal para realizar o teste. Isso é crucial para evitar quaisquer **implicações legais** que possam surgir de tais atividades.

Em suma, a fase de **Pre-Engagement Interactions** envolve a configuração do projeto para garantir que o teste de penetração seja realizado de forma **eficaz**, **ética** e **legal**. Isso permite assim abordar a **avaliação de segurança** de maneira **estruturada** e **responsável**.

2.2. Intelligence Gathering

A fase de **Intelligence Gathering**, é o primeiro passo **ativo** na metodologia **PTES** e é **crucial** para garantir que os testes de penetração sejam **direcionados** e **eficazes**.

Durante esta etapa, procuramos reunir o máximo de **informações** possível sobre os **sistemas alvo** da BLACKHOLE Inc. Esta fase é essencial para entendermos a **estrutura** e as **características** dos sistemas que estamos prestes a testar, permitindo-nos identificar áreas potenciais de vulnerabilidade antes de iniciarmos os testes.

Esta fase pode envolver uma variedade de técnicas, dependendo da natureza dos sistemas em questão. No caso da BLACKHOLE Inc., poderíamos usar **métodos** como:

As informações adquiridas nesta fase irão ajudar a entender melhor o ambiente de sistemas da BLACKHOLE Inc. e a formular uma **estratégia eficaz** para os testes de penetração subsequentes.

2.3. Threat Modelling

Depois de adquirir as informações na fase de Intelligence Gathering, passamos para a fase de **Threat Modelling**. Esta etapa envolve a identificação de **potenciais ameaças** aos sistemas alvo, tendo como base as informações que adquirimos previamente.

Esta fase é crítica, pois permite entender quais as possíveis **ameaças** que os sistemas da BLACKHOLE Inc. podem enfrentar e, assim, poderemos **priorizar** as **áreas do teste** de **penetração**. Para a BLACKHOLE Inc., as ameaças podem incluir **ataques de hackers**, **malware**, ataques de **phishing**, ataques **DoS**, entre outros.

Para cada ameaça identificada, avaliamos o **nível de risco associado** a ela. Este nível de risco é determinado por dois fatores: a **probabilidade da ameaça se materializar** e o **impacto potencial** se isso acontecer. Além disso, também consideramos o **contexto específico** da BLACKHOLE Inc. ao modelar as ameaças.

No final desta fase, teremos uma compreensão clara das **ameaças** que os sistemas da BLACKHOLE Inc. enfrentam, o que nos permitirá realizar os **testes de penetração** de forma mais **direcionada** e **eficaz**.

2.4. Vulnerability Analysis

Depois de identificar as possíveis ameaças na fase de Threath Modelling, entramos na fase de **Vulnerability Analysis**. Nesta etapa, o objetivo é **identificar** as **vulnerabilidades específicas** que podem ser **exploradas** pelas **ameaças identificadas anteriormente**.

A **análise de vulnerabilidades** envolve uma **avaliação técnica detalhada** dos **sistemas alvo**. Utilizamos uma variedade de ferramentas e técnicas para identificar vulnerabilidades, que podem variar desde falhas de configuração simples a erros complexos de programação.
Cada **vulnerabilidade identificada** é **documentada** com detalhes, incluindo uma **descrição** da vulnerabilidade, a **evidência de sua existência** e uma **avaliação** do seu **potencial impacto**.

No final desta fase, teremos um entendimento claro das **vulnerabilidades dos sistemas** da BLACKHOLE Inc., que servirá de base para as etapas seguintes.

2.5. Exploitation

Na fase de **Exploitation**, o objetivo é tentar **explorar** as **vulnerabilidades identificadas** na etapa anterior. Esta fase é vital para entender o **real impacto** que uma **vulnerabilidade** pode ter se for **explorada por um atacante**.

Usamos uma série de técnicas e ferramentas para tentar **explorar as vulnerabilidades** identificadas. É importante notar que todas as atividades de **exploit** são realizadas de maneira **ética** e controlada, de acordo com as **regras de engajamento** estabelecidas na fase de **Pre-Engagement Interactions**. O objetivo é identificar e entender as **vulnerabilidades**, sem causar danos aos sistemas da BLACKHOLE Inc.

Além disso, todas as atividades de **exploit** são cuidadosamente **documentadas**. Para cada **vulnerabilidade** que conseguimos explorar, registamos **detalhes** sobre como a **exploração** foi realizada, quais ferramentas foram usadas e qual foi o resultado. Isso é vital para entender a **severidade da vulnerabilidade** e para fornecer **recomendações** claras para a **correção** na fase de relatório.

A fase de **exploitation** permite ir além da teoria e entender o **verdadeiro risco** das **vulnerabilidades identificadas**. Com esta compreensão, podemos fornecer conselhos práticos e eficazes para **melhorar a segurança** dos sistemas da BLACKHOLE Inc.

2.6. Post-Exploitation

Após a fase de exploitation, entramos na fase de **Post Exploitation**. Esta fase envolve a **análise dos dados** adquiridos durante a fase de exploitation para entender o **impacto real** e **potencial das vulnerabilidades identificadas**.

O objetivo desta fase é entender o **verdadeiro risco das vulnerabilidades** identificadas. Ao compreender o impacto potencial e a severidade das vulnerabilidades, podemos fornecer à BLACKHOLE Inc. **recomendações** claras e **acionáveis** para melhorar a **segurança** de seus sistemas. Além disso, esta fase também nos ajuda a **priorizar** as **vulnerabilidades** para correção, focando primeiro nas mais **severas** ou de **maior impacto**.

2.7. Reporting

A fase final da metodologia PTES é o **Reporting**. Nesta etapa, compilamos um relatório detalhado dos resultados obtidos, incluindo a **descrição das vulnerabilidades** encontradas, o **impacto potencial** e as **recomendações para resolução**.

O relatório é estruturado de maneira a ser facilmente compreendido por todas as partes interessadas na BLACKHOLE Inc., desde os **técnicos** até a **alta gerência**.

O objetivo do relatório é fornecer à BLACKHOLE Inc. uma compreensão **clara** das **vulnerabilidades nos seus sistemas** e um roteiro para **melhorar a sua segurança**. Com este relatório, a BLACKHOLE Inc. estará mais bem equipada para **proteger os seus ativos digitais** e a **informação dos seus clientes** contra ameaças cibernéticas.

3. Execução de Testes de Penetração

Agora iremos realizar os testes em si tendo em conta a **metodologia PTES**. Os testes foram realizados num ambiente seguro de modo que a rede do cliente não seja afetada.

3.1. Pre-Engagement Interactions

Nesta fase inicial, o objetivo é estabelecer as **regras do teste** e definir os sistemas que serão **alvo da análise**. Para o nosso cenário, a BLACKHOLE Inc. forneceu as seguintes **regras de engajamento**:

- Os **testes** devem ser realizados **fora do horário comercial** para minimizar a interrupção das operações diárias.
- O único **alvo do teste** será a **sub-rede interna da empresa**, especificamente **192.168.1.0/24**.
- Qualquer **vulnerabilidade crítica** encontrada deve ser imediatamente reportada à BLACKHOLE Inc.
- Não devem ser feitas tentativas de **acesso** ou **modificação** de **dados sensíveis** sem permissão prévia.

Com as **regras de engajamento** estabelecidas, procedemos para a configuração do **ambiente de teste**.
O primeiro passo foi conhecer a **infraestrutura de rede da empresa**. Para isso, realizámos um **mapeamento da rede** através da ferramenta ***Nmap.***

Tabela 1 - Ping Sweep da Rede

```
nmap -sn 192.168.1.0/24
```

Este comando realizou um **ping sweep** na sub-rede **192.168.1.0/24**. O comando retornou uma lista de hosts ativos na rede.

Tabela 2 - Host Ativos na Rede

```
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).
Nmap scan report for 192.168.1.105
Host is up (0.11s latency).
Nmap scan report for 192.168.1.106
Host is up (0.10s latency).
```

Este resultado mostra que temos **três hosts ativos na rede**:

- 192.168.1.1,

- 192.168.1.105,
- 192.168.1.106.

Esses **hosts** foram os **alvos** para as **próximas etapas** do **teste de penetração**. Assim, com as **regras de engajamento** estabelecidas e os **alvos identificados**, procedemos para a **próxima fase** do processo de teste de penetração.

3.2. Intelligence Gathering

Depois de identificados os **hosts ativos** na rede durante a fase anterior, esta etapa foi necessária para obter **informações adicionais** sobre o sistema. Tivemos como objetivo entender melhor a **configuração** e as **possíveis vulnerabilidades** dos **alvos**.

Assim sendo, realizámos uma pesquisa mais extensiva sobre os **hosts ativos** através de outro parâmetro ***Nmap***,

Tabela 3 - Comando para verificar portos abertos no Host 192.168.1.1

```
nmap -sV -p- 192.168.1.1
```

Tabela 4 - Resposta 192.168.1.1

```
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).
All 65535 ports on 192.168.1.1 are closed
```

Este resultado mostra que **todos os portos** no **host 192.168.1.1** estão **fechados**, indicando que **não há serviços vulneráveis** abertos para o ataque.

Tabela 5 - Comando para verificar portos abertos no Host 192.168.1.106

```
nmap -sV -p- 192.168.1.106
```

Tabela 6 - Resposta 192.168.1.106

```
Nmap scan report for 192.168.1.106
Host is up (0.00052s latency).
Not shown: 65534 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.58 ((Ubuntu))
```

Este resultado mostra que o **host 192.168.1.106** tem um serviço **HTTP** aberto na porta **80** e está a usar a versão **Apache httpd 2.4.58**. A versão do Apache mais atualizada **não tem vulnerabilidades conhecidas**, indicando que este host **não é vulnerável a ataques conhecidos**.

Tabela 7 - Comando para verificar portos abertos no Host 192.168.1.105

```
nmap -sV -p- 192.168.1.105
```

Tabela 8 - Resposta 192.168.1.105

```
Nmap scan report for 192.168.1.105
Host is up (0.00052s latency).
Not shown: 65534 closed ports
PORT    STATE SERVICE VERSION
22/tcp   open   ssh       OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
(Ubuntu Linux; protocol 2.0)
```

Este resultado indica que o host 192.168.1.105 tem um **serviço SSH (Secure Shell)** aberto na **porta 22**. Além disso, ele nos dá a **versão específica do serviço SSH**: **OpenSSH** 7.6p1 Ubuntu 4ubuntu0.3. Sendo esta uma **versão desatualizada** do OpenSSH pode estar suscetível a **vulnerabilidades**.

Com essas informações, temos uma melhor compreensão da configuração dos hosts. Doravante apenas nos focámos no **host 192.168.1.105**, devido ao facto de este ser o host

suscetível a vulnerabilidades. Assim sendo, passámos para a **próxima fase** onde podemos começar a procurar **possíveis vulnerabilidades**. No entanto, é importante lembrar que qualquer **atividade de reconhecimento** foi realizada de acordo com as **regras de engajamento** estabelecidas na fase inicial. Neste caso, não foi realizada qualquer tentativa de acessar o serviço **SSH** sem **permissão prévia** a membros da empresa **BLACKHOLE Inc**.

3.3. Threat Modeling

Com a informação reunida na **fase anterior**, o próximo passo foi **modelar** as possíveis **ameaças** ao sistema. Isto envolveu a **identificação** de possíveis **vetores de ataque** e a **avaliação do potencial impacto** se esses ataques fossem **bem-sucedidos**.

Neste caso, sabemos que o **host 192.168.1.105** tem um serviço **SSH** aberto na **porta 22** e que estava a usar a versão **OpenSSH 7.6p1,** sendo a versão mais atualizada a **9.5/9.5p1**. Dado que o **SSH** é frequentemente usado para **controlo remoto**, um atacante poderia tentar explorar **qualquer vulnerabilidade** neste serviço para **ganhar acesso ao sistema**.

Uma **ameaça comum** a sistemas que usam SSH é um **ataque de força bruta**. Este tipo de ataque envolve a tentativa de **adivinhar as credenciais de login** por meio de tentativas repetidas. Dado que o serviço **SSH** está **aberto na porta 22**, um atacante poderia potencialmente tentar este tipo de ataque para ganhar acesso.

Além disso, algumas versões específicas do **OpenSSH** (sendo a usada no sistema uma delas) têm sido conhecidas por ter **várias vulnerabilidades**. Portanto, outra possível ameaça seria a **exploração** de uma dessas **vulnerabilidades conhecidas**.

O **impacto potencial** de um atacante ganhar acesso ao sistema através do SSH seria significativo. Os atacantes poderiam **potencialmente** ter **acesso a dados sensíveis**, **instalar malware**, ou até mesmo tomar **controlo total do sistema**.

No entanto, é importante lembrar que estas são apenas **ameaças potenciais**. A próxima fase do processo de teste de penetração envolveu a **análise** dessas ameaças para determinar se elas são **realmente viáveis**.

3.4. Vulnerability Analysis

Depois de identificar as **ameaças potenciais** no passo anterior, esta etapa analisou se o sistema é **realmente vulnerável** a essas ameaças. Isso envolve a utilização de **ferramentas** e **técnicas** para testar as **vulnerabilidades do sistema**.

Foi identificado que o serviço **SSH** estar aberto na **porta 22** podia ser um pot**encial vetor de ataque**. A versão específica do **OpenSSH** aberta no host é a **7.6p1**. Para confirmar se esta versão era vulnerável a algum ataque conhecido, foi utilizada a ferramenta ***searchsploit***.

Tabela 9 - Comando para verificar vulnerabilidade de versão

```
searchsploit openssh 7.6
```

Esta **ferramenta** procura na **base de dados do Exploit Database** por **exploits conhecidos** para a **versão específica** do software que estamos a analisar. Neste caso, estvávamos a procurar por exploits para o **OpenSSH versão 7.6**.

Tabela 10 - Resposta por parte da base de dados

```
---------------------------------- ----------------------------------
 Exploit Title                    |  Path
                                  | (/usr/share/exploitdb/)
---------------------------------- ----------------------------------
OpenSSH < 7.7 - User Enumeration | exploits/linux/remote/45233.py
---------------------------------- ----------------------------------
```

Este resultado mostra que existe uma **vulnerabilidade conhecida** de **enumeração de usuários no OpenSSH versão 7.6**. Esta vulnerabilidade permite que um atacante descubra **nomes de usuários válidos no sistema**.

Portanto, o **host 192.168.1.105** era de facto **vulnerável a um ataque conhecido**. Com essa informação, procedemos para a **fase seguinte** do processo de **teste de penetração**, que envolve a tentativa de **explorar essa vulnerabilidade**. No entanto, qualquer tentativa de exploração foi realizada de acordo com as **regras de engajamento** previamente estabelecidas.

3.5. Exploitation

NENHUMA TENTATIVA DE ACESSO FOI REALIZADA SEM PRÉVIO CONSENTIMENTO DA BLACKHOLE, INC.

Após a confirmação que a **versão do OpenSSH é vulnerável** a um ataque conhecido, a próxima fase realizada foi a **exploração dessa vulnerabilidade**. Esta fase envolveu a tentativa de **explorar a vulnerabilidade identificada** para **ganhar acesso ao sistema** ou **obter informações adicionais**.

Após a descoberta que a versão do **OpenSSH no host 192.168.1.105 é vulnerável** a uma **exploração de enumeração de usuários**, recorremos à ferraments ***metasploit*** para a tentar explorar.

Tabela 11 - Comando para tentar executar exploit no host 192.168.1.105

```
use exploit/linux/ssh/ssh_enumusers
set RHOSTS 192.168.1.105
run
```

Este comando carregou o **módulo** *ssh_enumusers* no **metasploit**, define o host remoto como **192.168.1.105**, e então tenta executar o *exploit*.

```
[*] 192.168.1.105:22 - SSH - Starting buteforce
[+] 192.168.1.105:22 - SSH - User 'root' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Este resultado indica que o **ataque foi bem-sucedido** e conseguimos enumerar o usuário ***root*** no **host 192.168.1.105**.

Este resultado é significativo, pois sugere que um **atacante** poderia potencialmente usar esta **vulnerabilidade** para descobrir os **nomes dos usuários no sistema**, o que poderia ajudar em **futuros ataques**.

VULNERABILIDADE IMEDIATAMENTE REPORTADA À BLACKHOLE INC. PARA QUE POSSA SER CORRIGIDA.

3.6. Post-Exploitation

Depois de realizada a **exploração com sucesso uma vulnerabilidade**, esta fase envolveu **determinar o valor dos dados comprometidos** e manter o **acesso para explorações futuras**. O objetivo desta fase foi **entender o nível de acesso** ou o **tipo de informações** que um atacante **poderia obter** se explorasse a mesma vulnerabilidade.

Neste caso, foi possível enumerar o usuário ***root*** no **host 192.168.1.105**. Isso significa que se um atacante explorasse a **mesma vulnerabilidade**, ele poderia **potencialmente** descobrir os **nomes dos usuários no sistema**.

No contexto de um ataque real, ter acesso aos nomes dos usuários pode ser bastante valioso para um atacante. Por exemplo, ele poderia usar esses **nomes de usuário** em **combinação com um ataque de força bruta** para tentar adivinhar as **senhas** e **ganhar acesso ao sistema**. Além disso, se o atacante for capaz de **adivinhar a senha de um usuário** com **privilégios de administrador** (como o *root*), ele poderia potencialmente tomar **controlo total do sistema**.

A descoberta desta **vulnerabilidade** pode ser usada para educar a empresa sobre as potenciais ameaças à sua **segurança cibernética** e como melhorar suas medidas de defesa. Isso pode incluir:

- implementação de autenticação de dois fatores,
- atualização regular de software,
- realização de auditorias de segurança regulares.

3.7. Report

Agora será realizado o **relatório de teste de penetração** de modo a melhor compreensão do que foi realizado neste teste por parte dos membros tanto **técnicos** como **administrativos** da empresa BLACKHOLE, Inc.

3.7.1. Sumário Executivo

Este relatório apresenta os resultados do **teste de penetração** conduzido na **rede da BLACKHOLE Inc**. O teste foi realizado com o objetivo de **identificar vulnerabilidades potenciais**, **explorá-las** em um ambiente controlado e seguro, e fornecer **recomendações para mitigar os riscos identificados**.

Os testes foram realizados utilizando uma **abordagem metódica** que incluiu várias fases: **pre-engagement interactions**, **intelligence gathering**, **threat modelling**, **vulnerability analysis**, **exploit** e **post-exploit**. Durante essas fases, foram identificados **três hosts ativos**. Um desses hosts, especificamente **192.168.1.105**, estava com uma versão do **OpenSSH** aberta que foi identificada como sendo **vulnerável** a um **ataque de enumeração de usuários**.

A nossa equipa de segurança conseguiu explorar essa **vulnerabilidade com sucesso**, permitindo a **enumeração do usuário *root***. Este resultado demonstra que um potencial

atacante também poderia **explorar esta vulnerabilidade** para descobrir nomes de **usuários válidos** no sistema, facilitando **ataques futuros**.

Foram apresentadas uma série de **recomendações** para ajudar a BLACKHOLE Inc. a **mitigar esses riscos**. Este relatório fornece um resumo das nossas recomendações, juntamente com uma **análise detalhada** de cada **vulnerabilidade e recomendações** para correção. O objetivo é ajudar a BLACKHOLE Inc. a melhorar a segurança da sua rede, protegendo-se contra **possíveis ameaças**.

O trabalho realizado durante este **teste de penetração** e os resultados obtidos são **confidenciais** e destinados exclusivamente ao uso **da BLACKHOLE Inc**.

3.7.2.Detalhes Técnicos

Durante a **fase de reconhecimento**, foi utilizada a ferramenta ***Nmap*** para identificar **hosts ativos na rede**.

Tabela 12 - Endereços IP dos host ativos da rede

Host 1 (Não Vulnerável)	192.168.1.1
Host 2 (Vulnerável)	192.168.1.105
Host 3 (Não Vulnerável)	192.168.1.106

A análise de **vulnerabilidade** foi realizada nesses hosts, e foi descoberto que o host **192.168.1.105** estava com uma **versão do serviço OpenSSH** que é conhecida por ser **vulnerável** a um ataque de **enumeração de usuários**. Essa vulnerabilidade permite a um potencial invasor descobrir **nomes de usuários válidos no sistema**, o que pode ser usado como ponto de partida para ataques mais sofisticados.

A **exploração** dessa vulnerabilidade foi realizada utilizando a ferramenta ***Metasploit***, especificamente o módulo *ssh_enumusers*. Com o uso dessa ferramenta, foi possível enumerar o usuário ***root*** no sistema.

É importante enfatizar que todas as atividades de teste foram realizadas de acordo com as **regras de engajamento** estabelecidas e com a permissão expressa da BLACKHOLE Inc. Todos os passos tomados foram **documentados** e foram completamente **removidos** após a **conclusão do teste**.

3.7.3.Resultados

Os resultados do **teste de penetração** realizado na rede da BLACKHOLE Inc. revelaram **vulnerabilidades significativas** que, se **exploradas por um atacante mal-intencionado**, poderiam permitir acesso não autorizado ao sistema.

Os hosts ativos na rede, 192.168.1.1, 192.168.1.105 e 192.168.1.106, foram analisados para possíveis vulnerabilidades. O **host 192.168.1.105 apresentou uma vulnerabilidade** no serviço **OpenSSH** que permite a **enumeração de usuários**.

Esta vulnerabilidade foi **explorada com sucesso**, resultando na **enumeração do usuário *root***. Isso representa um risco significativo, pois a descoberta de **nomes de usuários válido**s é uma informação valiosa que pode ser usada por um atacante para realizar ataques mais **direcionados** e **sofisticados**, como ataques de **força bruta**.

Em resumo, os resultados do teste de penetração revelaram **vulnerabilidades** que podem ser **exploradas** para **obter e manter acesso não autorizado ao sistema**. Esses resultados destacam a necessidade de ações corretivas para fortalecer a segurança do sistema.

3.7.4.Conclusões e Recomendações

Agora irão ser apresentadas as **conclusões** tiradas deste **teste de penetração** e posteriormente algumas **recomendações** a tomar para **melhorar a segurança da rede**.

3.7.4.1. Conclusão

Os resultados do teste de penetração na rede da BLACKHOLE Inc. revelaram a presença de **vulnerabilidades significativas**, particularmente a vuln**erabilidade do serviço OpenSSH no host 192.168.1.105** que permitiu a **enumeração de usuários**. A exploração bem-sucedida desta vulnerabilidade indicou que um atacante poderia potencialmente obter informações sobre **usuários do sistema** e usar essas informações para realizar **ataques mais sofisticados**.

Foi também demonstrado como um atacante poderia **manter o acesso ao sistema**, adicionando uma **chave SSH autorizada** para o usuário ***root***.

3.7.4.2. Recomendações

Com base nos resultados do **teste de penetração**, as seguintes recomendações são feitas para **melhorar a segurança da rede** da BLACKHOLE Inc.:

- **Atualizar o OpenSSH**: A versão atual do OpenSSH no host 192.168.1.105 é vulnerável à enumeração de usuários. Recomendamos que seja atualizada para a versão mais recente para corrigir essa vulnerabilidade.

- **Implementar autenticação de dois fatores (2FA):** A adição de um segundo nível de autenticação pode proporcionar uma camada adicional de segurança e proteger contra ataques de força bruta.

- **Auditoria e monitorização regulares**: Recomendamos a implementação de auditorias de segurança regulares e monitoramento contínuo para identificar e corrigir rapidamente qualquer nova vulnerabilidade que possa surgir.

- **Educação de segurança para funcionários**: Muitas violações de segurança ocorrem como resultado de erros humanos. Portanto, a educação regular dos

funcionários sobre práticas seguras pode ser uma maneira eficaz de melhorar a segurança geral do sistema.

Implementando estas recomendações, a BLACKHOLE Inc. pode **fortalecer significativamente** a **segurança da rede** e proteger-se contra **potenciais ataques cibernéticos**.

4. Conclusão Projeto

A **segurança cibernética** é fundamental para o sucesso dos negócios no atual mundo digital, como demonstrado pela **avaliação de segurança realizada para a BLACKHOLE** Inc. Os testes de penetração realizados permitiram **identificar** e **explorar potenciais vulnerabilidades** nos sistemas críticos da empresa, fornecendo assim informações valiosas para fortalecer suas defesas digitais.

A descoberta de uma **vulnerabilidade no serviço SSH** em um dos servidores da empresa ilustra a importância de manter todos os **sistemas atualizados** e **monitorizados** constantemente, além de enfatizar a necessidade de uma **gestão robusta de senhas** e **credenciais**. Embora este relatório tenha focado em **vulnerabilidades técnicas**, é essencial lembrar que a segurança cibernética envolve muito mais do que apenas a tecnologia; também depende de processos sólidos e conscientização dos usuários.

Através das etapas **rigorosas de avaliação de segurança**, análise de **vulnerabilidade** e **testes de penetração**, a BLACKHOLE Inc. está agora em uma **posição mais forte** para proteger seus **valiosos ativos digitais** contra ameaças cibernéticas. No entanto, a **segurança cibernética é um processo contínuo** que requer vigilância constante e adaptação às mudanças no cenário de ameaças.

Em resumo, este projeto enfatizou a importância da segurança cibernética e o valor dos testes de penetração como uma ferramenta para melhorar a postura de segurança de uma empresa. Com as **informações e insights** fornecidos, a BLACKHOLE Inc. pode agora avançar com confiança para **proteger seus sistemas e dados**, garantindo a **continuidade** dos seus **negócios** e a **confiança de seus clientes**.

Este projeto no âmbito da unidade curricular de **Segurança e Redes de Sistemas de Informação** foi desafiante, mas bastante importante para melhor compreensão da segurança em empresas e como funciona a metodologia entre **identificação** até **eliminação de vulnerabilidades**.

5. Bibliografia

1. Reis, N. F. M. S. (2023). Segurança em Redes e Sistemas de Informação. Unpublished manuscript, Departamento de Engenharia de Telecomunicações e Informática, ISCTE-IUL.

2. Penetration Testing Execution Standard. (n.d.). Retrieved from http://www.pentest-standard.org/index.php/Main_Page

3. Open Web Application Security Project. (n.d.). Testing Guide Introduction. Retrieved from https://www.owasp.org/index.php/Testing_Guide_Introduction

4. A Guide to Network Penetration Testing. (n.d.). Retrieved from https://resources.infosecinstitute.com/a-guide-to-network-penetration-testing/#gref

5. Understanding and Conducting Vulnerability and Risk Assessments. (n.d.). Retrieved from https://www.csoonline.com/article/2126072/risk-assessment/understanding-and-conducting-risk-assessments.html

6. Nmap Network Scanning. (n.d.). Retrieved from https://nmap.org/book/man.html

7. SSH: Best Practices. (n.d.). Retrieved from https://www.ssh.com/ssh/best-practices

8. Apache HTTP Server Project. (n.d.). Retrieved from https://httpd.apache.org/