Seu LOGO

# RELATÓRIO DE TESTE DE PENETRAÇÃO

## Cliente: JOAS ANTONIO

| | |
|---|---|
| Autor | |
| Encontro | |

| Versão | |
| --- | --- |

## Conteúdo

## Lista de Figuras

Endereço:
Telefone:

# Lista de mesas



.

LOGOTIPO

# 1 Controle de documento

## 1,1 Emissor de Documento

| | |
|---|---|
| Endereço | |
| Telefone | |
| O email | |
| Autor | |

## 1,2 Documento histórico

| Data de Emissão | Versão | Comente | Autor |
|---|---|---|---|
| | | | |

Tabela 1: Histórico de Publicação de Relatório

## 1,3 Declaração de não divulgação

Este documento contém direitos de propriedade intelectual e direitos autorais, que são propriedade da Cyber Security UP. O trabalho e as informações nele contidos são apresentados com o objetivo de fazer uma proposta, cumprir um contrato ou como garantia de marketing. Deve ser tratado como confidencial e não deve ser usado para nenhum outro propósito. Não deve ser copiado ou divulgado a terceiros, no todo ou em parte, sem o consentimento prévio por escrito da Cyber Security UP.

## 1,4 Comentários no relatório

O Cyber Security UP agradece comentários e feedback sobre nossos relatórios. Quaisquer comentários sobre este relatório devem ser encaminhados ao Cyber Security UP no prazo de 10 dias úteis após a emissão do relatório ao cliente. Se nenhum comentário for fornecido dentro deste prazo, será considerado que o cliente aceitou o relatório e suas conclusões na íntegra.

## 1,5 Declaração de Limitação

Este trabalho foi realizado de acordo com os termos e condições de venda do Cyber Security UP. O Cyber Security UP testou os sistemas no momento solicitado e não pode comentar sobre a segurança ou vulnerabilidades que existiam antes ou depois da realização do teste. Todos os testes são limitados no tempo e pode não ser possível investigar totalmente todos os problemas ou encontrar todos os possíveis problemas de segurança. A Cyber Security UP não pode comentar sobre sistemas que estavam fora do escopo deste relatório, indisponíveis no momento do teste ou onde o acesso necessário não foi fornecido. Este relatório não deve ser considerado uma lista de todas as vulnerabilidades ou problemas existentes no sistema ou ambiente. O Cyber Security UP não pode comentar as correções aplicadas aos sistemas após este teste sem avaliá-las tecnicamente.

LOGOTIPO

# 2 Resumo Técnico

O documento a seguir resume os resultados do teste de penetração realizado pelo Cyber Security UP em nome do Cliente.

## 2,1 Escopo do Teste

### 2.1.1 Avaliação

Realizei um teste de penetração nos foophones da organização de telefonia móvel. Isso incluiu os seguintes elementos de teste:

Também a partir de uma perspectiva de aplicativo da Web OWASP

Os aspectos internos da organização também foram testados quando uma máquina foi comprometida, bem como a capacidade de escalar privilégios nas máquinas comprometidas. Finalmente, como é fácil para um invasor pivotar outras redes internas com o objetivo final de explorar o servidor DMZ que foi realizado.

.

### 2.1.2 Alvos

### 2.1.3 Datas de teste

Esta avaliação foi realizada entre DATE.

## 2,2 Equipa de avaliação

Esta avaliação foi realizada pelos seguintes consultores:

## 2,3 IPs de origem

Todos os testes externos foram realizados no ambiente de exame dedicado. O endereço de origem fornecido está listado abaixo.

## 2,4 Recomendações Críticas

Várias vulnerabilidades críticas foram descobertas durante o envolvimento que levou ao comprometimento total da máquina do servidor da web na rede inicial. Foi então possível ligar para a rede corporativa para continuar a exploração de outras máquinas Windows por meio de psexec e uma exploração de estouro de buffer e, em seguida, finalmente, para girar para a rede DMZ final. Onde o comprometimento de máquinas anteriores em sub-redes em andamento permitia a divulgação de credenciais para acessar o servidor DMZ via SSH.

## 2,5 Recomendações Gerais

Vários sistemas operacionais sem suporte foram descobertos em execução em todos os hosts em toda a infra-estrutura de rede, bem como software sem patch que deve ser corrigido imediatamente. Isso ajudaria a mitigar muitas das vulnerabilidades mais críticas descobertas nesses hosts.

Conforme mencionado anteriormente no relatório, várias vulnerabilidades de tipo estão presentes no aplicativo da web inicial. A higienização de todas as entradas do usuário, bem como a implantação de um WAF, ajudaria a mitigar muitos desses problemas encontrados. O antivírus deve ser implantado em todas as máquinas da organização para interromper a execução de executáveis mal-intencionados, como o Mimikatz, por exemplo, que pode ser usado em um host Windows comprometido para extrair credenciais da memória.

Nos ambientes Windows, os módulos psexec devem ser desabilitados para impedir a autenticação remota dos usuários

com outros dispositivos de compartilhamento de arquivos do Windows por meio de apenas um nome de usuário e hash da senha. A assinatura SMB também deve ser habilitada em todos os hosts Windows. Todos os hosts devem ser verificados para pontos de escalonamento de privilégios fáceis, como binários SUID e se os privilégios sudo foram configurados incorretamente. As versões do kernel em todos os hosts devem ser verificadas quanto a exploits de escalonamento de privilégios disponíveis.

O aplicativo do Portal de Gerenciamento do Cliente em execução em um dos hosts foi descoberto como vulnerável a uma exploração de estouro de buffer e deve ser imediatamente desativado e seu código-fonte do aplicativo completamente reescrito, pois no momento é possível aproveitar esse estouro de buffer para obter a execução remota de código e no final das contas gerou um shell que é o que eu consegui fazer durante o noivado.

Todos os softwares e aplicativos em execução nos hosts da rede devem estar na versão mais recente e também totalmente corrigidos. Faço referência particular a uma instância em execução do WINSCP que me permitiu executar um módulo de pós-exploração dentro do Metasploit para obter credenciais de trabalho para o servidor final na rede DMZ.

## 2,6 Estatisticas

### 2.6.1 Gravidade do Problema vs. Mapa de Probabilidade

A tabela a seguir exibe o número de problemas de acordo com a gravidade e a probabilidade.

| | | Gravidade | | | |
|---|---|---|---|---|---|
| | | Crítico | Alto | Médio | Baixo |
| ade | Alto | 0 | 0 | 0 | 0 |
| | Médio | 0 | 0 | 0 | 0 |
| | Baixo | 0 | 0 | 0 | 0 |

### 2.6.2 Médias de gravidade do problema

| | |
|---|---|
| Não. Hosts testados | 5 |
| Número médio de problemas por host | 3,60 |
| Número médio de problemas críticos por host | 1,40 |
| Número médio de problemas elevados por host | 1,60 |
| Número médio de problemas médios por host | 0,40 |
| Número médio de problemas baixos por host | 0,20 |

## 2,7 Conclusão Geral

Em comparação com compromissos de escopo semelhante de uma perspectiva de caixa preta, o nível de segurança interno e de aplicação dos foofones externos foi considerado incrivelmente pobre. Ganhar uma posição na rede por meio do aplicativo Web inicial é uma tarefa trivial para qualquer ator de ameaça potencial. Com o aplicativo sendo vulnerável a várias vulnerabilidades de tipo críticas, levando à aquisição completa.

Uma vez que um dispositivo foi comprometido, o escalonamento de privilégios, bem como a rotação para alcançar outras partes da infraestrutura interna também foi possível, conforme mencionado no relatório, nenhuma solução antivírus apareceu presente em qualquer um desses dispositivos, permitindo o upload irrestrito, download e execução de cargas maliciosas . Sistemas operacionais desatualizados e software sem correção pareciam constituir a maior parte do ambiente encontrado durante o contrato.

O aplicativo da web deve ser completamente revisado para começar, pois esse é atualmente o ponto de entrada inicial disponível publicamente para os agentes de ameaças em potencial para a rede interna. A entrada do usuário deve ser limpa conforme mencionado anteriormente pelo servidor com tags e caracteres maliciosos sendo removidos. A codificação também deve ser adicionada quando a entrada do usuário é processada pelo servidor e um Web Application Firewall deve ser implantado e ajustado para capturar cargas maliciosas, o que ajudará a mitigar as múltiplas vulnerabilidades de tipo que encontrei no aplicativo. Uma solução antivírus também deve ser implantada nos dispositivos descobertos.

# 3 Resumo do problema

A tabela nesta seção oferece um resumo técnico das vulnerabilidades que foram descobertas durante o teste.

## 3,1 Tabela de vulnerabilidades descobertas

| Título do Problema | Gravidade | Probabilidade | Vulnerabilidade de tipo | Hosts |
|---|---|---|---|---|
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Crítico | Alto | | |
| Vulnerabilidade (1 host afetado) | Alto | Alto | | |
| Vulnerabilidade (1 host afetado) | Alto | Alto | | |
| Vulnerabilidade | Alto | Alto | | |

| Título do Problema | Gravidade | Probabilidade | Modelo | Hosts |
|---|---|---|---|---|
| (1 host afetado) | | | | |
| Vulnerabilidade<br><br>(1 host afetado) | Alto | Alto | | 10.185.11.127 |
| Vulnerabilidade<br><br>(1 host afetado) | Médio | Alto | | 10.185.10.34 |
| Vulnerabilidade<br>(1 host afetado) | Médio | Alto | | foophonesels |
| Vulnerabilidade<br>(1 host afetado) | Médio | Alto | | foophonesels |
| Vulnerabilidade<br>(1 host afetado) | Médio | Alto | | 10.185.10.34 |
| Vulnerabilidade<br>(1 host afetado) | Médio | Alto | | 10.185.10.34 |
| Vulnerabilidade<br>(1 host afetado) | Médio | Alto | | foophonesels |
| Vulnerabilidade<br>(1 host afetado) | Baixo | Baixo | | 10.185.10.27 |

Tabela: Tabela de Resumo do Problema

# 4 Problemas de segurança identificados

## 4,1 Vulnerabilidade

| Não. Hosts afetado | | 0 | Gravidade: | | Crítico | Probab | | Vulnerabilidade de tipo |
|---|---|---|---|---|---|---|---|---|

**Explicação do problema**

Figura 1:

**Lista de hosts identificados**

**Recomendação**

.

Endereço:
Telefone:

**Sistema de pontuação de vulnerabilidade comum (CVSS)**

| | | | |
|---|---|---|---|
| Pontuação B | | 7,1 | AV: L / AC: L / Au: N / C: C / I: C / A: C |
| Pontuação ge | | 7,1 | |

.

Endereço:
Telefone:

# UMA Definições

## A.1 Gravidade da vulnerabilidade

As vulnerabilidades são fornecidas com uma escala de gravidade que foi determinada individualmente pelo CNS Tester levando em consideração os resultados do teste realizado dentro do ambiente exclusivo do cliente.

Nenhuma ferramenta automatizada é usada para determinar essa escala de gravidade.

| Gravidade | Descrição |
|---|---|
| Crítico | Uma vulnerabilidade crítica é aquela que foi executada pelo CNS e levou ao comprometimento do alvo por a vulnerabilidade. |
| Alto | Uma vulnerabilidade alta é aquela que é confirmada como uma vulnerabilidade positiva e pode levar a uma violação de rede ou host e pode levar ao comprometimento do alvo. |
| Médio | Uma vulnerabilidade média é aquela que pode revelar mais informações que podem levar a um ataque ou onde detalhes essenciais foram encontrados que podem diminuir a segurança do alvo, por exemplo, portas abertas desnecessárias. |
| Baixo | Uma vulnerabilidade baixa diz respeito às informações encontradas durante o teste que podem não ser uma ameaça imediata para o computador. pany. No entanto, a empresa deve revisar as informações e determinar o curso de ação correto. |

Tabela: Definição de Gravidades

## A.2 Probabilidade de vulnerabilidade

Também pode ser útil determinar o risco da probabilidade de uma vulnerabilidade específica ocorrer no host de destino. Portanto, a vulnerabilidade é avaliada individualmente para determinar esse risco.

NOTA: A tabela abaixo deve ser usada apenas como uma indicação da probabilidade da ameaça.

| Probabilidade | Descrição |
|---|---|
| Alto | Uma vulnerabilidade com alta probabilidade está disponível publicamente e é muito comum ou é relativamente exploit fácil de executar. Qualquer um dos casos deve ser revisto o mais rápido possível. Vírus, worms, cavalos de Tróia, padrão configurações etc. são todos exemplos de alta probabilidade. |
| Médio | Uma vulnerabilidade que tem uma probabilidade média é aquela que requer uma certa habilidade para ser executada ou isso é difícil de encontrar, a menos que o host de destino seja especificamente direcionado. Para realmente realizar o exploit pode exigir várias etapas ou conhecimento do aplicativo ou serviço para ser bem-sucedido. Aplicação específica vulnerabilidades como injeção de SQL e ataques XSS são exemplos de probabilidades médias. |
| Baixo | Uma vulnerabilidade de baixa probabilidade é extremamente difícil de executar ou não é publicamente conhecido ou disponível. Se uma vulnerabilidade tem baixa probabilidade, não significa necessariamente que terá uma baixa gravidade. |

Tabela: Definição de Probabilidades

## A.3 Tipos de vulnerabilidade

As vulnerabilidades são categorizadas em tipos específicos para ajudar o cliente a avaliar a ameaça. A tabela a seguir detalha ainda mais os tipos de vulnerabilidade:

| Modelo | Descrição |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Continua na próxima página...

| Modelo | Descrição |
| --- | --- |
| | |

Tabela: Definição de Tipos de Vulnerabilidade

# B Enumeração de host

Após a fase de descoberta de rede, cada host foi examinado por sua vez em busca de sinais de vulnerabilidades ou configurações incorretas que poderiam fornecer a um invasor uma rota para a rede. Cada host foi enumerado para ver quais portas estavam abertas para o mundo externo. Cada uma dessas portas foi examinada posteriormente para determinar os aplicativos em execução nas portas e as maneiras pelas quais esses aplicativos podem ser subvertidos.

## B.1 Detecção de sistema operacional

Este teste tenta obter a impressão digital dos sistemas operacionais de cada host. Conhecer o sistema operacional é uma vantagem distinta para localizar vulnerabilidades. A varredura geralmente fornece uma porcentagem do sucesso ao adivinhar o sistema operacional.

| Hospedeiro | SO detectado |
|---|---|
| | |
| | |
| | |
| | |
| | |

Tabela: Tabela de detecção de sistema operacional

## B.2 Enumeração de porta

As portas TCP / IP podem estar em um dos 3 estados: -

- Aberto = o host de destino aceitará conexões com essa porta
- Filtrado = Um firewall ou filtro está em vigor, interrompendo a varredura de porta
- Não filtrado ou fechado = Nenhum firewall ou filtro interferiu na varredura, o que determinou que a porta está fechada para conexões.

Portas abertas são geralmente as portas de destino a serem exploradas. No entanto, para um hacker dedicado, as portas filtradas também podem ser um alvo. Este teste investigará em que estado as portas estão para cada host.

| Hospedeiro | Porta | Protocolo | Descrição | Status |
|---|---|---|---|---|
| | | | | |
| | | | | |

Continua na próxima página...

| Hospedeiro | Porta | Protocolo | Descrição | Status |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

Tabela: Tabela de resumo de digitalização de porta

# C Graph Pack

## C.1 Número de vulnerabilidades por tipo

Figura: Número de vulnerabilidades por tipo

## C.2 Número de vulnerabilidades por gravidade

Figura: Número de vulnerabilidades por gravidade

.