INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 02: Teste de Penetração - Levantamento de Informações

---

Olá turma, hoje iremos ter a nossa primeira relacionada a teste de penetração. Para isso, inicialmente iremos conhecer os conceitos relacionados. Posteriormente, iremos conhecer algumas ferramentas que podem nos auxiliar a obtermos informações sobre determinadas empresas no levantamento de informações.

Teste de Penetração

O Teste de Invasão, também chamado de teste de intrusão ou pentest, é um método que **avalia** a segurança de um sistema de computador ou de uma rede, **simulando um ataque** de uma fonte maliciosa com a **autorização do responsável pelo computador/rede**. O objetivo principal é **simular de forma controlada** um ataque real que normalmente é executado por criminosos. Esta prática é recomendada de forma periódica em redes institucionais para **medir o grau de vulnerabilidade e corrigir problemas** antes que sejam explorados por agentes externos.

Em um teste de invasão (em oposição a uma avaliação de vulnerabilidades), os pentesters não só identificam vulnerabilidades que poderiam ser usadas pelos invasores, mas também exploram essas vulnerabilidades, sempre que possível, para avaliar o que os invasores poderiam obter após uma exploração bem-sucedida das falhas.

Existem quatro tipos de pentests, são eles:

- *Blind (black box)*: o profissional de segurança executa o teste sem a empresa fornecer qualquer informação da rede;
- *Non Blind (White-box)*: a execução é feita com conhecimento da rede, tais como servidores, firewalls, roteadores, sistemas operacionais, etc;
- Externo: a execução é feita a partir da rede externa;
- Interno: a execução é feita a partir da rede interna (LAN).

O teste de penetração **explora as falhas específicas através de uma invasão controlada**. Desta forma, para evitar causar situações que gerem algum tipo de comprometimento nos serviços do cliente, deve-se criar imagens dos servidores críticos que serão testados e realizar os testes em máquinas virtuais.

Atenção, no Código Penal Brasileiro (Art. 154-A.) informa que:

> " Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa."

Logo, antes de realizar o teste de penetração, prepare o contrato de serviço especificando de forma clara os alvos, objetivos, tipos de ataques que podem ser realizados, prazos, limites, confidencialidade e autorização da organização.

As fases de um teste de invasão são:

- Fase de preparação: que envolve conversar com o cliente a respeito de seus objetivos para o teste de invasão, o mapeamento do escopo (a extensão e os parâmetros do teste) e assim por diante. Faça perguntas sobre os negócios de seu cliente. O que é mais importante para eles? O que os levou a procurar um pentester? Quais as exposições que eles mais temem? Eles têm algum dispositivo frágil com o qual você deverá ter cuidado ao efetuar os testes?
- Fase de coleta de informações: o pentester procura informações disponíveis publicamente sobre o cliente e identifica maneiras em potencial de conectar-se com seus sistemas. Você também começará a usar ferramentas como scanners de porta para ter uma ideia de quais sistemas estão presentes na Internet ou na rede interna, bem como quais softwares estão executando

- Fase de análise de vulnerabilidades: procura-se descobrir vulnerabilidades nos sistemas que poderão ser exploradas. Durante essa fase, os pentesters executam scanners de vulnerabilidades, que usam bancos de dados de vulnerabilidades e uma série de verificações ativas para obter um palpite melhor a respeito de quais vulnerabilidades estão presentes no sistema de um cliente.

- Fase de exploração de falhas: executa-se exploits contra as vulnerabilidades descobertas (às vezes, usando uma ferramenta como o Metasploit) em uma tentativa de acessar os sistemas de um cliente, descobrir informações adicionais, obter dados críticos, acessar outros sistemas e assim por diante.

- Fase de geração de relatórios: informa-se as nossas descobertas ao cliente de maneira significativa. Dizemos o que eles estão fazendo corretamente, os pontos em que devem melhorar sua postura quanto à segurança, como você conseguiu invadir, o que você descobriu, como corrigir os problemas e assim por diante.

Fase de Coleta de Informações

Podemos aprender bastante sobre a organização e a infraestrutura de nossos clientes antes de lhes enviar um único pacote sequer, basta pesquisarmos em banco de dados públicos, tais como redes sociais, DNS, site da empresa, etc.

Com estas informações poderemos tentar descobrir senhas ou softwares utilizados pela empresa. Por exemplo, se o seu cliente tiver postagens de ofertas de emprego online para uma vaga de administrador de sistemas que seja especialista em determinado software, existe uma boa chance de essas plataformas terem sido implantadas na infraestrutura do cliente.

Podemos coletar estas informações em sites de empregos (determinar funcionário, tecnologias, equipamentos, softwares e serviços utilizados na empresa), Engenharia Social (obter informações confidenciais através da persuasão) e Redes Sociais (Facebook, Twitter, Instagram, etc..).

Nesta disciplina, iremos focar em coletar informações através de banco de dados públicos e ferramentas disponíveis.

Ferramenta Whois

Todos os registradores de domínio mantêm registros dos domínios que eles hospedam. Esses registros contêm informações sobre o proprietário, incluindo informações de contato.

A ferramenta whois permite coletar estas informações através de uma consulta a um banco de dados pública do domínio DNS, que nos fornece informações pessoais sobre o proprietário, por exemplo, seus detalhes de contato, sua organização e seu IP, bem como sua localização geográfica.

```
whois <endereço IP/nome do site>
```

Exemplos de Uso

1. Site do IFRN:

```
whois www.ifrn.edu.br
```

2. Site da Prefeitura de São Gonçalo do Amarantes:

```
whois www.saogoncalo.rn.gov.br
```

3. Site do Google:

```
whois www.google.com.br
whois 74.125.68.106
```

Dependendo da consulta é possível obtermos informações de endereços, números de telefone, CNPJ da empresa, reponsáveis.

Dnsenum

A ferramenta dnsenum é um script em perl que obtem informações de DNS de um domínio. Como ele podemos obter o endereço do host (registro A), obter os servidores de nomes, obter o registro MX.

```
dnsenum ifrn.edu.br
```

Archive.org

O Internet Archive é uma organização sem fins lucrativos que disponibiliza uma biblioteca digital de sites da Internet e outros artefatos culturais em formato digital. Atualmente, já possui mais de:

- 330 bilhões de páginas da web;
- 20 milhões de livros e textos;
- 4,5 milhões de áudio;
- 4 milhões de vídeos;
- 3 milhões de imagens;
- 200.000 programas de *software*;

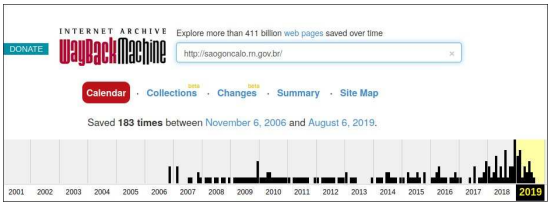
No teste de penetração podemos obter versões antigas de sites para coletarmos informações. Por exemplo, a página do IFRN possui, atualmente, 214 versões entre 23/01/2009 a 20/08/2019. Dessa forma, é possível determinarmos no que a empresa divulgou em todo esse período, informações administrativas, antigos funcionários, trabalhos realizados, descobrir tecnologias, telefones antigos e utilizar os mesmos para montar um ataque de engenharia social.

Exemplos de Uso

1. Site do IFRN:

2. Site da Prefeitura de São Gonçalo do Amarantes:

A base de dados possui 183 versões do site da prefeitura entre os períodos de between 6/11/2006 a 6/08/2019.



Google Hacking

O google é uma excelente buscador e permite obtermos informações sobre muita coisa. Dessa forma, ele também é muito utilizado por hackers e pentesters como uma técnica para coletar informações de empresas e detectar vulnerabilidades. O Google Hacking é a utilização da plataforma Google para nos ajuda a encontrar vulnerabilidades usando alguns parâmetros na hora de realizar as pesquisas.

Além disso, um servidor mal configurado pode expor diversas informações da empresa no Google.

Os principais parâmetros para coleta de informações são:

- site: utilizado para especificar um determinado site. Por exemplo, site:ifrn.edu.br;
- filetype: utilizado para especificar um determinado tipo de arquivo. Por exemplo, site:ifrn.edu.br filetype:pdf edital;
- intext e allintext: utilizado para fazer buscas por uma palavra ou por múltiplas palavras, respectivamente, no corpo do texto. Por exemplo, site:ifrn.edu.br intext:macedo;
- inurl e allinurl: restringir os resultados da busca no Google a páginas que contenham uma ou várias palavras na URL. Por exemplo, site:ifrn.edu.br inurl:concurso;
- cache: mostra a última versão do site salva pelo Google. Por exemplo, cache:ifrn.edu.br;

Existem ainda alguns parâmetros que auxiliam a encontrarmos vulnerabilidade em sites. Por exemplo:

- intitle:index.of: são sites que disponibilizam a vizualização e obtenção de arquivos no servidor. Por exemplo, intitle:index.of inurl:gov.br;
- Acesso a base de dados disponibilizadas na Web através do comando "fitetype:sql". Por exemplo, fitetype:sql site:gov.br.
- Acessar sites que disponibilizam acesso remoto pelo navegador através do comando inurl:connectcomputer/precheck.html | inurl:remote:logon.aspx

Contramedidas

Para minimizar a coleta de informações dos funcionários ou das empresas, devemos tomar os seguintes cuidados:

- Possuir uma boa política referente à publicações de informações na internet e sempre analisar as informações disponíveis sobre a empresa em sites de busca e mídias sociais.
- Não deixar configurações padrão em servidores web, de email e outros serviços de rede.
- Alertar e treinar os funcionários da empresa com relação a maneira com que um ataque de engenharia social pode acontecer, e as possíveis informações que o atacante poderá usar nesse ataque.

Atividade

01. Descubra o máximo de informações sobre o IFRN São Gonçalo do Amarante. Funcionários, estrutura, tecnologia, organograma, etc.

02. Procure outros sites ou ferramentas de coleta de informações sobre empresas e redes.