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

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 02: Teste de Penetração e Levantamento de Informações com Whois, Archive e Google

Olá turma, hoje iremos ter a nossa primeira relacionada a teste de penetração. Vocês deverão compreender os princípios básicos do teste de penetração, identificar as etapas envolvidas no processo de teste de penetração e reconhecer as ferramentas comuns usadas em testes de penetração, em especial no levantamento de informações.

Teste de Penetração

O teste de penetração, também conhecido como pentest, é um processo autorizado de avaliação da segurança de um sistema de computador ou rede. O objetivo principal é tenta encontrar e explorar vulnerabilidades simulando de forma controlada um ataque real que normalmente é executado por criminosos. Essencialmente, o teste de penetração simula um ataque real, mas sem causar danos, a fim de identificar e corrigir falhas de segurança antes que sejam exploradas por indivíduos maliciosos.

A importância do teste de penetração em segurança de redes é enorme, pois ajuda a garantir a integridade, confidencialidade e disponibilidade dos sistemas de informação. Além disso, permite que as organizações identifiquem e corrijam vulnerabilidades antes que sejam exploradas por hackers, protegendo assim seus ativos e reputação.

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.

Existem três tipos de pentests, são eles:

- *Blind (black box)*: o profissional de segurança não tem conhecimento prévio da infraestrutura da rede ou do sistema que está sendo testado. Isso simula um ataque de um hacker externo que não possui informações privilegiadas;
- *Non Blind (White-box)*: o profissional possui total conhecimento da infraestrutura da rede ou sistema que está sendo testado. Isso simula um ataque de um funcionário (ou ex-funcionário) mal-intencionado que possui acesso privilegiado. O objetivo é testar a segurança interna da organização.
- *Gray Box*: é uma combinação dos dois tipos anteriores, onde o testador possui algum conhecimento parcial da infraestrutura da rede ou sistema que está sendo testado. Isso simula um ataque de um hacker que conseguiu obter algumas informações privilegiadas.

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."

As etapas do teste de penetração são um conjunto de atividades sequenciais realizadas para identificar e explorar vulnerabilidades em sistemas de computadores ou redes. Aqui estão as principais etapas do teste de penetração são: Coleta de Informações, Análise de Vulnerabilidades, Exploração, Manutenção de Acesso e Geração de Relatórios.

Fase de Coleta de Informações

O profissional reúne informações sobre o alvo do teste, como informações dos funcionários, infrmações das atividades da empresa, endereços IP, topologia da rede, nomes de domínio, servidores, serviços em execução, entre outros. Isso é feito por meio de técnicas passivas, como pesquisa na internet (disponíveis publicamente), e técnicas ativas, como scan de portas.

Fase de Análise de Vulnerabilidades

O pentest identifica e analisa as possíveis vulnerabilidades nos sistemas e serviços identificados na fase de reconhecimento. Isso pode envolver a execução de scanners de vulnerabilidades automatizados, como o Nessus, que usam bancos de dados de vulnerabilidades.

Fase de Exploração

Com base nas vulnerabilidades identificadas, o testador tenta explorar essas vulnerabilidades para obter acesso não autorizado aos sistemas alvo. Isso pode envolver o uso de exploits (Metasploit), que são programas projetados para aproveitar vulnerabilidades específicas. Desta forma, tenta-se ter acessar aos sistemas, descobrir informações confidenciais, obter dados críticos, acessar outros sistemas e assim por diante.

Fase de Manutenção de Acesso

Se o pentest conseguir obter acesso aos sistemas alvo, ele tentará manter esse acesso de forma a persistir mesmo após o término do teste, ou atualizações no sistema. Isso pode envolver a instalação de backdoors. O objetivo de manter o acesso será mostrar o acesso a empresa posteriormente.

Fase de Geração de Relatórios

Finalmente, o profissional documentará todas as atividades realizadas durante o teste, incluindo as vulnerabilidades encontradas, os exploits utilizados, as técnicas de invasão empregadas e as recomendações para corrigir as vulnerabilidades identificadas. Este relatório é essencial para que a organização possa corrigir as vulnerabilidades e melhorar sua segurança.

Na aula de hoje iremos iniciar os estudos referentes a fase de coleta de informações.

Fase de Coleta de Informações

A coleta de informações sobre o alvo é uma etapa crucial em um teste de penetração. Ela envolve a obtenção de informações relevantes sobre o sistema ou rede que está sendo testado, a fim de identificar possíveis vulnerabilidades e pontos de entrada. Aqui estão algumas técnicas comuns de coleta de informações sobre o alvo:

- Pesquisa na Internet: realizar pesquisas sobre a empresa ou organização alvo pode fornecer informações valiosas, como endereços de e-mail, nomes de funcionários, tecnologias utilizadas, entre outros.
- Footprinting: envolve a coleta de informações sobre a infraestrutura de rede da organização, como endereços IP, servidores DNS, subdomínios, etc. Isso pode ser feito usando ferramentas automatizadas de footprinting ou manualmente através de técnicas como DNS lookup, traceroute, etc.
- Engenharia Social: manipulando as pessoas para obter informações confidenciais. Isso pode envolver a realização de telefonemas, envio de e-mails de phishing ou até mesmo visitas pessoais à empresa alvo.
- Análise de E-mail: analisar os cabeçalhos de e-mails recebidos da organização alvo pode revelar informações sobre os servidores de e-mail e possíveis endereços IP associados.
- Redes Sociais: as redes sociais podem ser uma fonte rica de informações sobre uma empresa ou organização, fornecendo detalhes sobre funcionários, parceiros, produtos, 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.

Na sequência, iremos focar em coletar informações através de banco de dados públicos e ferramentas disponíveis.

Ferramenta Whois

Whois é uma ferramenta de linha de comando usado para consultar bancos de dados que armazenam informações sobre registros de domínios. Essas informações incluem detalhes sobre o proprietário do domínio, o registrador do domínio, os servidores de nomes associados ao domínio, informações de contato, bem como sua localização geográfica.

Ela é amplamente utilizada por administradores de rede, profissionais de segurança e pesquisadores para obter informações sobre um determinado domínio.

A sintaxe básica para usar a ferramenta é:

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

É importante observar que algumas organizações e provedores de registro de domínios podem restringir o acesso às informações do Whois por motivos de privacidade.

Exemplos de Uso

1. Site do IFRN:

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

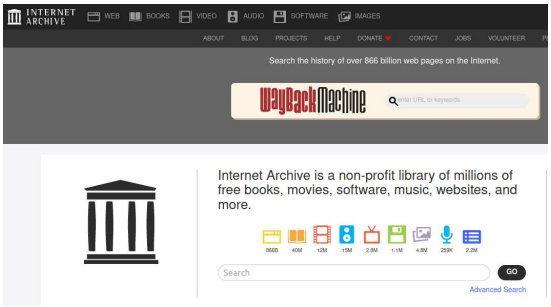
```
domain:      ifrn.edu.br
owner:       Instituto Federal de Educação do RN
ownerid:     24.370.371/0001-23
responsible: Jose Arnobio de Araujo Filho
country:     BR
owner-c:     CEGEG2
tech-c:      WERME22
nserver:     ns1.ifrn.edu.br 200.137.1.167
nsstat:      20240303 AA
nslastaa:    20240303
nserver:     ns2.ifrn.edu.br 200.137.1.168
nsstat:      20240303 AA
nslastaa:    20240303
created:     20081013 #4887132
```

Atividade

1. Obtenha informações sobre o domínio da Prefeitura de São Gonçalo do Amarantes (`www.saogoncalo.rn.gov.br`).

Archive.org

O Archive.org, também conhecido como Internet Archive, é um site dedicado a preservar e oferecer acesso público a uma ampla variedade de conteúdos digitais, incluindo websites, vídeos, músicas, livros e imagens. O principal objetivo do Archive.org é servir como um repositório de recursos digitais de valor histórico, cultural e educacional, garantindo que esses recursos estejam disponíveis para as gerações futuras.



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*;

O Internet Archive pode ser uma ferramenta útil em testes de penetração de várias maneiras:

- Reconhecimento de Alvos: usar para pesquisar versões antigas de um site pode revelar informações sobre a infraestrutura e possíveis vulnerabilidades que foram corrigidas em versões mais recentes.
- Engenharia Social: ao analisar versões antigas de um site, um profissional de penetração pode obter informações sobre funcionários, estrutura organizacional, informações administrativas, antigos funcionários, trabalhos realizados, descobrir tecnologias, telefones antigos e outras informações sensíveis que podem ser exploradas em ataques de engenharia social.
- Avaliação da Segurança de Aplicações Web: ao analisar versões antigas de um site, o profissional pode identificar mudanças na aplicação web que podem indicar a adição de novos recursos e tentar identificar vulnerabilidades na mesma.

Exemplos de Uso

1. Site do IFRN:

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.

Google Hacking refere-se ao uso de técnicas avançadas de pesquisa no Google para encontrar informações sensíveis ou vulnerabilidades de segurança em sites e sistemas online. O Google Hacking geralmente envolve o uso de operadores de pesquisa avançados, como operadores booleanos, aspas, wildcards e operadores de exclusão, para refinar os resultados da pesquisa e encontrar informações específicas que normalmente não seriam acessíveis por meio de uma pesquisa convencional.

Os principais parâmetros para coleta de informações são:

- site: utilizado para especificar um determinado site. Por exemplo,

```
macedo firmino site:ifrn.edu.br
```

- filetype: utilizado para especificar um determinado tipo de arquivo. Por exemplo,

```
macedo firmino site:ifrn.edu.br filetype:pdf
```

- intext: utilizado para fazer buscas por uma palavra ou por múltiplas palavras, respectivamente, no corpo do texto. Por exemplo,

```
site:ifrn.edu.br intext:macedofirmino
```

- inurl: restringir os resultados da busca no Google a páginas que contenham uma ou várias palavras na URL. Por exemplo,

```
site:ifrn.edu.br inurl:login
```

- Encontrar câmeras IP desprotegidas:

```
inurl:view/index.shtml
```

- Descobrir diretórios expostos:

```
intitle:“index of” “backup”
```

- Acesso a base de dados disponibilizadas na Web:

```
fitetype:sql
```

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.