SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Segurança de Redes

- A segurança de redes pode ser considerada um subconjunto da segurança da informação. Uma das diferenças fundamentais entre a segurança de redes e a segurança da informação é o seu escopo de aplicação.
- A segurança da informação trata de todas as formas de informação, enquanto a segurança de redes foca o meio digital.

- Uma forma de entender a segurança de redes é a sua aplicação na suíte de protocolos TCP/IP (Transmission Control Protocol/Internet Protocol), que é o coração da internet.

Portas ou serviços

- Uma porta TCP está associada diretamente a um serviço da camada de aplicação e representa pontos de conexão de rede para aquele serviço específico. Um exemplo é o serviço Telnet, que possui como porta padrão a 23 do TCP.

- O conceito de porta é importante porque é por meio dela que as conexões são realizadas para os ataques, de modo que devemos utilizar os controles de segurança adequados.

- Uma porta aberta significa um serviço disponível, que pode ser conectado e, consequentemente, pode ser atacado.

Aplicação e protocolos

- Cada aplicação ou serviço utiliza um protocolo específico e funciona em uma porta específica para poder receber as conexões. Alguns exemplos são:
  - Comunicação colaborativa: Skype (SIP, Session Initiation Protocol)
  - Servidor de arquivos: Windows (NTFS, New Technology File System).
  - E-mail: SMTP (Simple Mail Transfer Protocol).
  - RH: SAP (SNC, Secure Network Communications), na camada de aplicação para segurança fim a fim, e SSL (Secure Sockets Layer) nas conexões HTTP (Hypertext Transfer Protocol)

Aplicação e protocolos

- Cada aplicação ou serviço utiliza um protocolo específico e funciona em uma porta específica para poder receber as conexões. Alguns exemplos são:
  - Financeiro: SAP (SNC, Secure Network Communications), na camada de aplicação para segurança fim a fim, e SSL (Secure Sockets Layer) nas conexões HTTP (Hypertext Transfer Protocol)
  - Projeto colaborativo: softwares baseados na nuvem e na web, que utilizam o HTTP (Hypertext Transfer Protocol), devendo usar o TLS (Transport Layer Security) ou o SSL (Secure Sockets Layer), o que resulta no HTTPS (Hypertext Transfer Protocol Secure). O TLS, SSL e o HTTPS são protocolos de segurança que garantem confidencialidade, integridade e autenticidade das comunicações, o que não acontece com o HTTP tradicional.

Varredura de portas

- Uma das principais técnicas para iniciar a identificação de vulnerabilidades é a varredura de portas, ou port scanning. Uma porta aberta, em um computador, corresponde a um serviço que está disponível e que, portanto, pode ser acessado. Uma vez acessada essa porta aberta, podem ser enviados comandos e realizados ataques. Uma pichação de um sítio web, por exemplo, ocorre com ataques à porta 80, que corresponde à porta padrão de funcionamento de um servidor web. Já um ataque a um servidor de e-mail ocorre na porta 25, que é a porta padrão do serviço SMTP (Simple Mail Transfer Protocol) do correio eletrônico.

EXERCITANDO...

- Imagine uma empresa qualquer que possui um firewall (será abordado mais à frente em detalhes). O mesmo deve bloquear acessos indevidos.
- Essa mesma empresa provê serviços de e-mail e possui um sítio web. O firewall deve, portanto, ser configurado para liberar conexões nas portas 25 e 80, respectivamente.

- A pergunta é: o firewall protege contra ataques ao servidor Web?

Exemplos

- Uma das principais ferramentas de varredura de portas é o Nmap, que pode ser utilizada para verificar os serviços que estão rodando em determinado equipamento.
- Instale o nmap em seu computador e teste o seguinte comando:

nmap –v localhost

nmap –T5 –sV –O localhost

-v -> Faz um scan de TODAS as portas TCP que estejam reservadas no host scaneado.

-T5

-O -> Retorna o sistema operacional

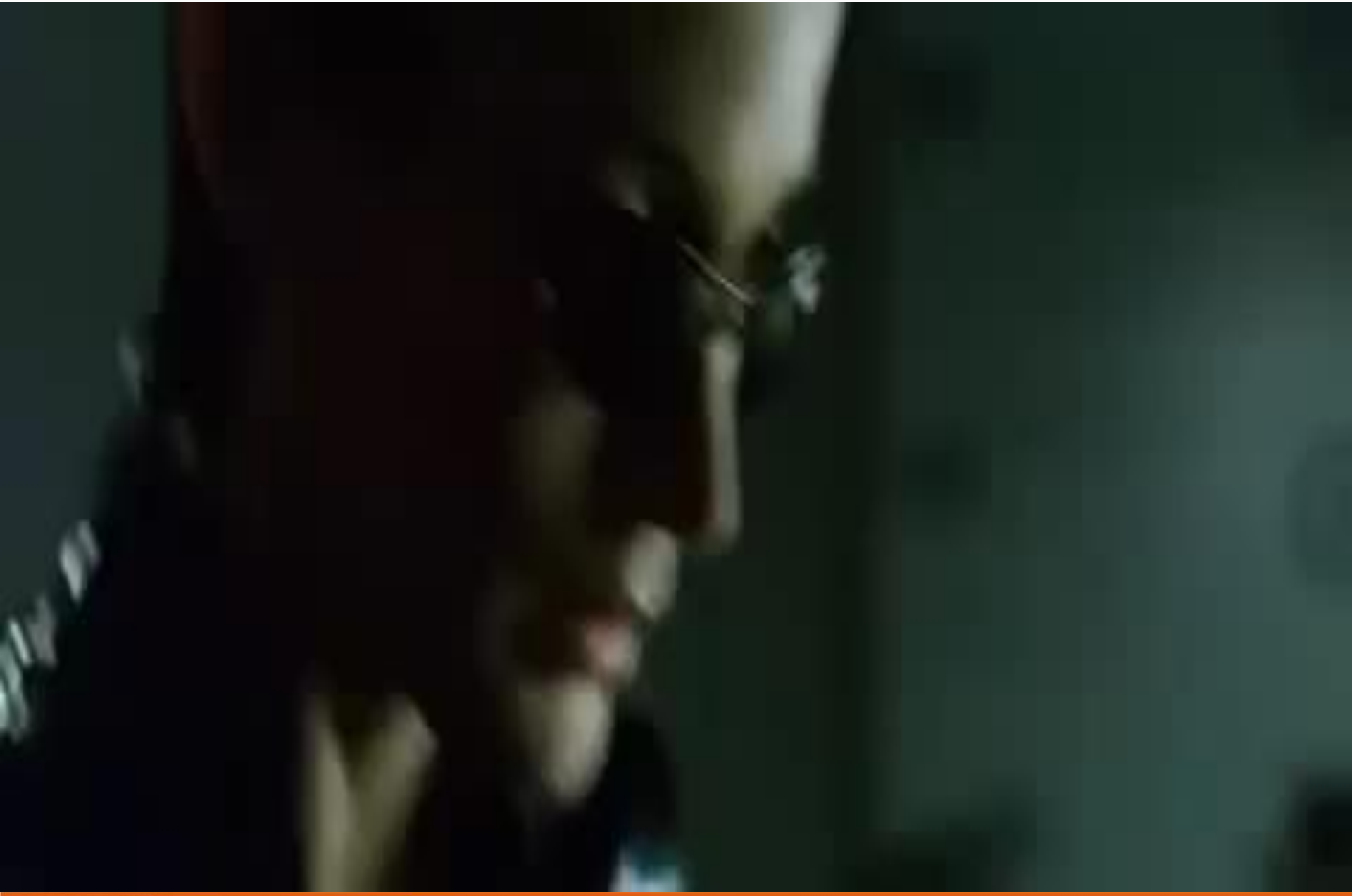
-sV -> Identifica a versão de um serviço rodando em determinada porta

Exemplos

- Matrix é um dos clássicos dos filmes de ficção científica. Nele, a personagem Trinity utiliza a ferramenta nmap para mapear um servidor e identificar serviços a serem atacados.
- O ataque é feito com a exploração de uma vulnerabilidade do serviço SSH.

- https://www.youtube.com/watch?v=0PxTAn4g20U

SEGURANÇA DE REDES DE COMPUTADORES



Varredura de vulnerabilidades

- A busca por vulnerabilidades de um ativo pode ser realizada nos serviços identificados pela varredura de portas. Caso uma porta 80, por exemplo, seja identificada, uma varredura de vulnerabilidades correspondentes ao servidor web poderá ser realizada.

- Além dos conhecimentos sobre vulnerabilidades em servidores web, há uma série de ferramentas que podem ser utilizadas para o scan (varredura) de vulnerabilidades.

Sniffing

- Também conhecida como passive eavesdropping (espionagem ou escuta passiva), essa técnica de ataque no nível de rede consiste na captura de informações valiosas diretamente pelo fluxo de pacotes na rede. As informações que podem ser capturadas pelos sniffers são referentes aos pacotes que trafegam no mesmo segmento de rede em que o software funciona.

- Como o fluxo de dados trafegam por meio de uma rede, o sniffer captura cada pacote e, se necessário, decodifica os dados brutos do pacote, mostrando os valores de vários campos no pacote, e analisa seus conteúdos.

Sniffing

- O uso do IPv6 é uma das formas de proteção contra o sniffing, já que utilizada o protocolo IPSec, que provê, dentre vários mecanismos de segurança, a criptografia dos dados, tornando as comunicações protegidas com a garantia da confidencialidade.

- PESQUISE sobre o IPv6.

PARA CONHECIMENTO

- A ferramenta WIRESHARK é muito utilizada para análise de protocolos de rede e pode ser utilizada para captura de pacotes também.

- PESQUISE sobre essa ferramenta, instale em sua máquina e realize alguns testes.

IP Spoofing

- Essa é uma técnica na qual o endereço real do atacante é mascarado, de forma a evitar que ele seja encontrado. É muito utilizada em tentativas de acesso a sistemas nos quais a autenticação tem como base endereços IP, como a utilizada nas relações de confiança em uma rede interna. Essa técnica é também bastante usada em ataques do tipo DoS, nos quais pacotes de resposta não são necessários.

Sequestro de Conexões

- É um ataque ativo que explora o redirecionamento de conexões de TCP para determinada máquina, caracterizando um ataque man-in-the-middle, conhecido também como session hijacking.

- Com o sequestro de uma conexão, um agente de ameaça passa a ter o controle dessa conexão, comprometendo a confidencialidade (tendo acesso às informações em trânsito), a integridade (alterando ou injetando informações na conexão) e mesmo a disponibilidade (descartando informações, que deixam de chegar ao seu destino).

Vulnerabilidades em aplicações

- Os ataques no nível de rede evoluíram para os ataques na camada de aplicação, que possuem uma vasta gama de vulnerabilidades disponíveis para serem exploradas. Um exemplo é o ataque de SQL Injection, em que comandos de ataques são executados a partir da inserção de dados não convencionais em formulários de sites.

- Uma vez realizada a varredura de portas, vulnerabilidades específicas de serviços identificados podem ser testadas e exploradas.

- Uma vulnerabilidade clássica é o buffer overflow, uma violação da memória que permite a escrita de dados em localizações específicas desta, levando à execução arbitrária de códigos que resultam em ataques.

Vulnerabilidades em aplicações

- Outras vulnerabilidades em aplicações, incluindo aplicações móveis:
  - Controles fracos no lado servidor, podendo ser utilizados em ataques XSS (Crosssite scripting), que é uma injeção de códigos maliciosos em clientes via servidores web vulneráveis.

- https://www.youtube.com/watch?v=sZiBZBASHFM

Vulnerabilidades em aplicações

- Outras vulnerabilidades em aplicações, incluindo aplicações móveis:
  - Armazenamento inseguro de dados.
  - Proteção insuficiente na camada de transporte.
  - Vazamento de dados não intencional.
  - Autenticação fraca.
  - Criptografia falha.
  - Injeção de dados no lado cliente.
  - Entrada de dados não confiáveis.
  - Manipulação inadequada de sessões.
  - Falta de proteção de binários.

Vulnerabilidades em Hardware

- Apesar de serem mais raras, há situações que despertam bastante a atenção da comunidade, como o caso do backdoor (porta aberta sem conhecimento do usuário) em firewall.

- Além disso, o avanço da internet faz com que a segurança de informação e de redes deva tratar com bastante cuidado os novos dispositivos, que serão alvos de ataques, como já está ocorrendo, por exemplo, no caso do ataque a um veículo da Jeep.

EXERCÍCIOS

1) A segurança da informação e de redes possui como propriedade básica a confidencialidade, a integridade e a disponibilidade. Controles de segurança devem ser aplicados em ativos. Por quê?

a) Porque ativos possuem vulnerabilidades.

b) Porque ativos possuem ameaças.

c) Porque ativos possuem impactos.

d) Porque controles agem contra hardware.

e) Porque controles agem contra software.

EXERCÍCIOS

2) A segurança da informação e de redes possui como propriedade básica a confidencialidade, a integridade e a disponibilidade. Há alguma diferença entre segurança da informação e segurança de redes?

a) Não há diferença alguma.

b) A segurança da informação é mais importante do que a segurança de redes.

c) A segurança de redes é mais importante do que a segurança da informação.

d) A segurança de redes foca os meios digitais.

e) A segurança de redes foca as informações que estão na cabeça das pessoas e em meios físicos.

EXERCÍCIOS

3) Vulnerabilidades em redes de computadores podem ser identificadas com o uso de ferramentas como o Nmap, que realiza a varredura de portas de um ativo. Essa afirmação está correta? Por quê?

a) Sim, porque portas abertas representam vulnerabilidades.

b) Sim, porque cada porta aberta é uma vulnerabilidade.

c) Sim, porque o mapeamento das portas indica as vulnerabilidades do ativo.

d) Não, porque uma porta aberta indica apenas que há um serviço disponível no ativo.

e) Não, porque serviços podem ser atacados independentemente de portas abertas.

RESOLUÇÃO

1)

2)

3)

EXERCÍCIOS

Pesquise sobre Sniffing, IP Spoofing, SQL Injection e XSS. Explique cada um desses ataques e cite casos de ataques realizados conhecidos através desses tipos de ataques.

DATA DE ENTREGA: 15/04

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

REFERÊNCIAS

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera