SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

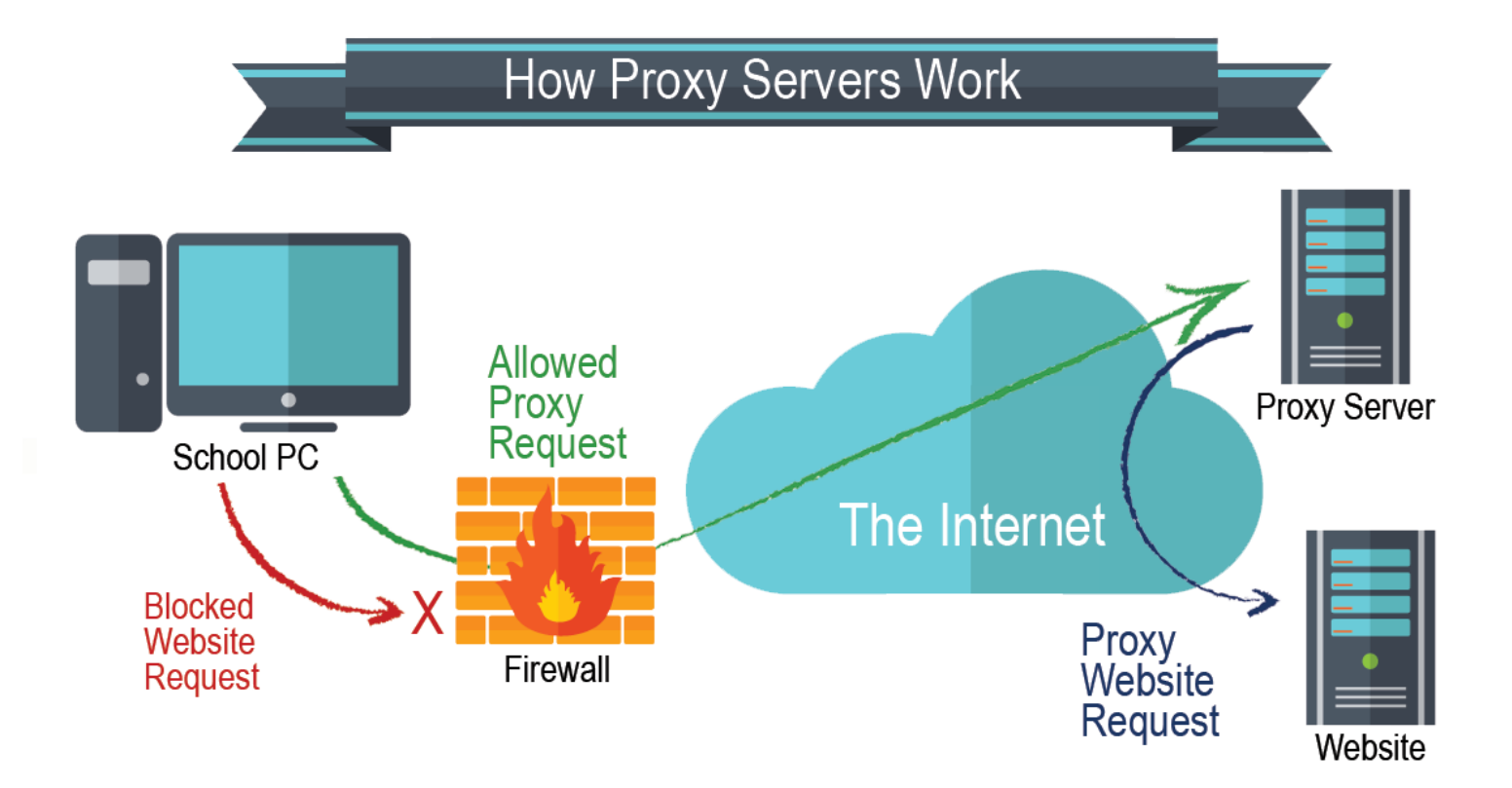
Firewall

- Os firewalls podem atuar ainda no nível de aplicação, o que permite que dados de protocolos como o HTTP, utilizado na web, possam ser analisados. A partir dessa análise, é possível realizar algumas tarefas, como a filtragem de conteúdo, por exemplo. Outra funcionalidade de um firewall que atua no nível de aplicação é o proxy.

- O Proxy é um servidor intermediário que atende a requisições repassando os dados do cliente à frente: um usuário (cliente) conecta-se a um servidor *proxy*, requisitando algum serviço, como um arquivo, conexão, página *web*, ou qualquer outro recurso disponível no outro servidor.

Firewall

- Um servidor proxy geralmente trabalha junto ou no mesmo equipamento que um firewall, sua função além intermediar a conexão também é definir quais sites as máquinas ou usuários podem acessar.



Firewall

- Os proxies ajudam também na aceleração do acesso à internet no caso de empresas que precisam de velocidade na hora de navegar. O registro da página acessada fica guardado na sua cache. Com este arquivo já gravado, o próximo acesso fica muito mais rápido uma vez que não será necessário refazer o primeiro reconhecimento do destino.

IDS

- Os Sistemas de Detecção de Intrusão (Intrusion Detection Systems, IDS) possuem um papel importante para a segurança da informação e de redes porque permitem a detecção de ataques em andamento, principalmente contra serviços legítimos, que passam pelas regras do firewall. Essa importância está relacionada ao monitoramento e à detecção, já que o IDS não pode prevenir um ataque em andamento.
- Algumas das principais funcionalidades do IDS são:
  - Monitoramento e análise das atividades dos usuários e dos sistemas.
  - Avaliação da integridade de arquivos importantes do sistema e de dados.
  - Análise estatística do padrão de atividade.

IDS

- Algumas das principais funcionalidades do IDS são:
  - Análise baseada em assinaturas de ataques conhecidos.
  - Análise de atividades anormais.
  - Análise de protocolos.
  - Detecção de erros de configuração do sistema.
  - Identificação do destino do ataque.
  - Registro para investigações

IDS

- Um dos principais tipos de IDS é o baseado em host (Host-Based IDS, HIDS), que realiza a detecção de:
  - Acessos a arquivos.
  - Alteração de arquivos.
  - Modificação de privilégio de usuários.
  - Acesso a processos do sistema.
  - Execução de programas.
  - Uso de CPU. • Conexões.

IDS

- Outro tipo de IDS é o tradicional baseado em rede (Network IDS, NIDS), que atua analisando cabeçalhos e conteúdos dos pacotes em trânsito, com comparações baseadas em assinaturas. Os pontos fracos do NIDS estão relacionados com a dificuldade de detecção de ataques que usam técnicas para driblar os mecanismos implementados e também com a dificuldade de ação em caso de detecção de atividades suspeitas, pois há muitos alarmes falsos.

- Consiste em um conjunto de sensores que trabalha detectando atividades maliciosas na rede, como ataques baseados em serviço, portscans, etc.

IDS – Formas de detecção de um intruso

- **Detecção por assinatura -** A Detecção por assinatura analisa as atividades do sistema procurando por eventos que correspondam a padrões pré-definidos de ataques e outras atividades maliciosas. Estes padrões são conhecidos como assinaturas e geralmente cada assinatura corresponde a um ataque.

- **Detecção por anomalias -** A detecção por anomalias parte do princípio que os ataques são ações diferentes das atividades normais de sistemas. IDS baseado em anomalias monta um perfil que representa o comportamento rotineiro de um usuário, Host e/ou conexão de rede.

- A desvantagem da primeira é que as intrusões são detectadas somente se estiverem dentro de um padrão, enquanto a segunda pode gerar um alto número de alarmes falsos.

IDS – Modos de utilização

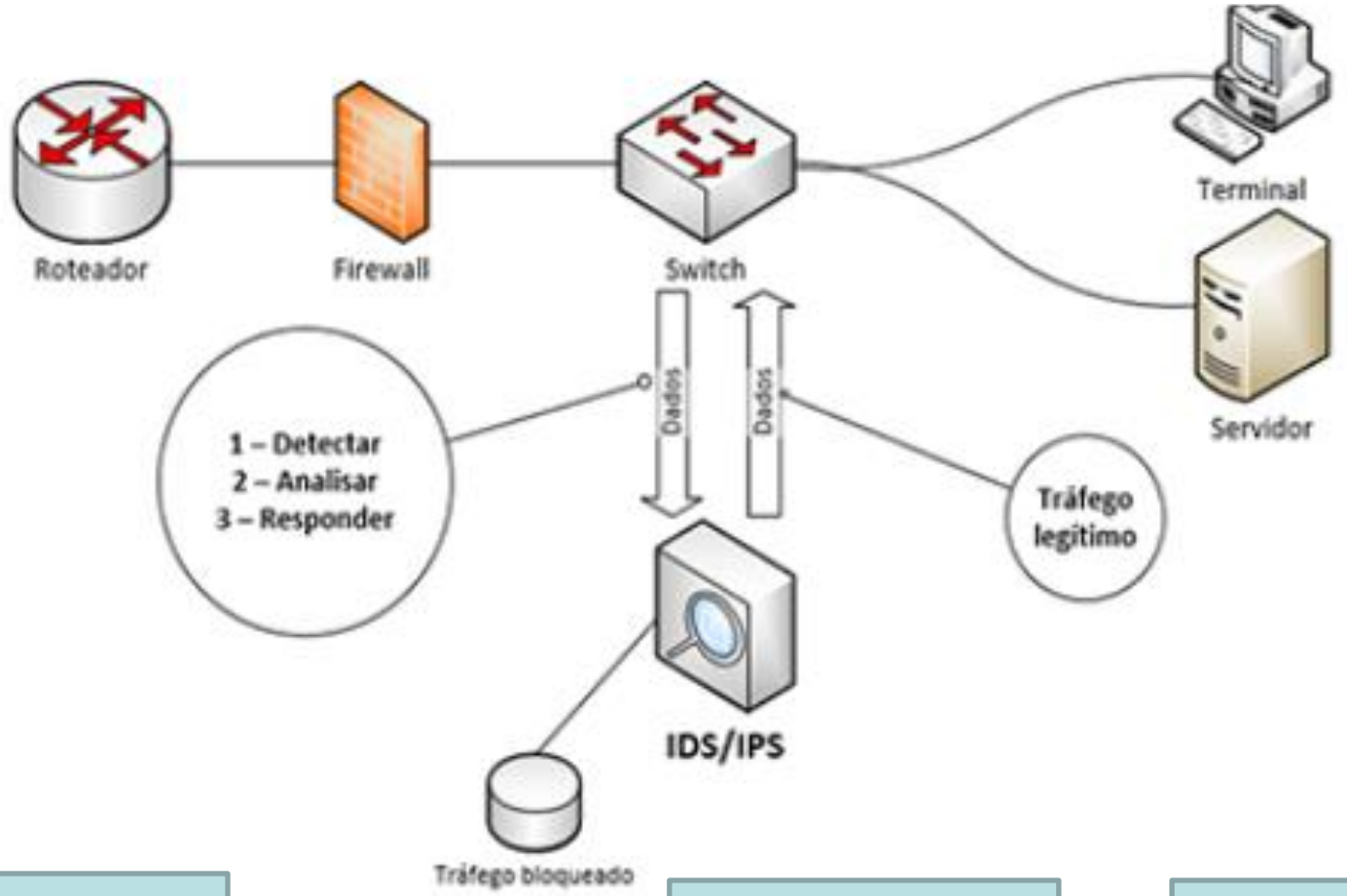
- **Modo Passivo -** Um IDS passivo quando detecta um tráfego suspeito ou malicioso gera um alerta e envia para o administrador. Não toma nenhum atitude em relação ao ataque em si.

- **Modo Reativo -** Um IDS reativo não só detecta o tráfego suspeito ou malicioso e alerta o administrador, como também possuí ações pré-definidas para responder as ameaça. Normalmente, isso significa bloquear todo o tráfego do IP suspeito ou do usuário mal-intencionado.

IPS

- Sistemas de Prevenção de Intrusão (Intrusion Prevention System, IPS) possuem grande similaridade com o IDS, porém funcionam de uma forma mais ativa após a detecção de atividades suspeitas, tomando ações diretas, como o término daquela conexão. A diferença fundamental é que o IPS atua de uma forma in-line, ou seja, todo o tráfego passa pelo IPS, diferentemente do IDS, que opera passivamente. Com esse posicionamento na rede, o IPS atua de modo similar ao firewall no que tange à análise de todos os pacotes que entram na rede protegida.

IPS e IDS



O switch encaminha o tráfego para o IDS;IPS

O tráfego legítimo é encaminhado ao destino

O tráfego nocivo é bloqueado

Antivirus e antimalware

- Os malwares incluem códigos maliciosos, como vírus, worms, cavalos de Troia, spyware, bots, keyloggers e rootkits. As primeiras ferramentas de segurança eram voltadas para os vírus, códigos maliciosos que dominavam o cenário de segurança no início. Essas ferramentas, os antivírus, fizeram fama desde essa época e continuam evoluindo. Atualmente, muitos antivírus atuam também sobre outros tipos de malwares, apesar de conservarem o nome de “antivírus”.

- Assim, os antimalwares podem indicar que se tratam de controles que vão além dos do antivírus, porém eles são similares. As ferramentas que se declaram antimalwares geralmente são mais novas, já nasceram quando o termo malware estava mais disseminado, o que era diferente na época dos “vírus”.

Antivirus e antimalware

- Há ainda ferramentas antimalwares mais avançadas, normalmente direcionadas a malwares específicos, como é o caso dos que atacam transações financeiras. Geralmente disponibilizadas pelas próprias instituições financeiras, essas ferramentas buscam dificultar o funcionamento dos malwares que trazem prejuízos aos bancos.

- Assim, os antimalwares podem indicar que se tratam de controles que vão além dos do antivírus, porém eles são similares. As ferramentas que se declaram antimalwares geralmente são mais novas, já nasceram quando o termo malware estava mais disseminado, o que era diferente na época dos “vírus”.

EXERCÍCIOS

Questões 1, 2 e 3 Unidade 2 Seção 3.

EXERCÍCIO PARA ENTREGA

Pesquisa sobre o SNORT

- **O que é?**
- **Para que serve?**
- **Configuração básica**

DATA: 06/05

Efetividade dos controles de segurança

- Um controle de segurança não é capaz de resolver todos os problemas de segurança isoladamente. Um firewall deixa portas abertas para serviços legítimos. Um IDS pode detectar ataques em andamento nessas portas abertas pelo firewall, porém uma ação ainda é esperada. O IPS dá uma resposta, agindo preventivamente contra os ataques em andamento, porém técnicas de evasão podem ser utilizadas. Já os antimalwares atuam no endpoint, ou no equipamento do usuário, mas mesmo assim ataques que partem de usuários contaminados causam grandes prejuízos às empresas.

- Exemplo: malware de boleto. Os números são alterados e o pagamento acaba caindo em contas de fraudadores.

Efetividade dos controles de segurança

- Além dos ataques que partem de usuários contaminados com malware, há problemas ainda mais complexos de serem resolvidos, como aqueles em que crackers roubam credenciais de usuários, passando a ter acesso a sistemas e informações críticas de uma forma direta, como se fossem os usuários legítimos. Nesse caso, os ataques não visam à exploração de vulnerabilidades de sistemas, mas sim o roubo de identidades desses usuários, normalmente com a descoberta da senha, que é o método de autenticação mais comum.

Efetividade dos controles de segurança

- Outras ameaças devem ser ainda consideradas, como o vazamento de informações confidenciais através de métodos de comunicação seguros, por exemplo, o envio de documentos de projetos para concorrentes a partir de um funcionário, por e-mail. Nesse caso, a comunicação acontece de dentro da empresa para fora, de modo legítimo e, portanto, mecanismos de segurança como firewall, IDS, IPS ou antimalware não são efetivos, já que eles visam proteger a empresa contra ataques vindos do exterior.

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