

Defensor vs. Atacante: Duas Perspectivas Sobre a Mesma Rede

Uma análise das duas perspectivas essenciais da Segurança da Informação.

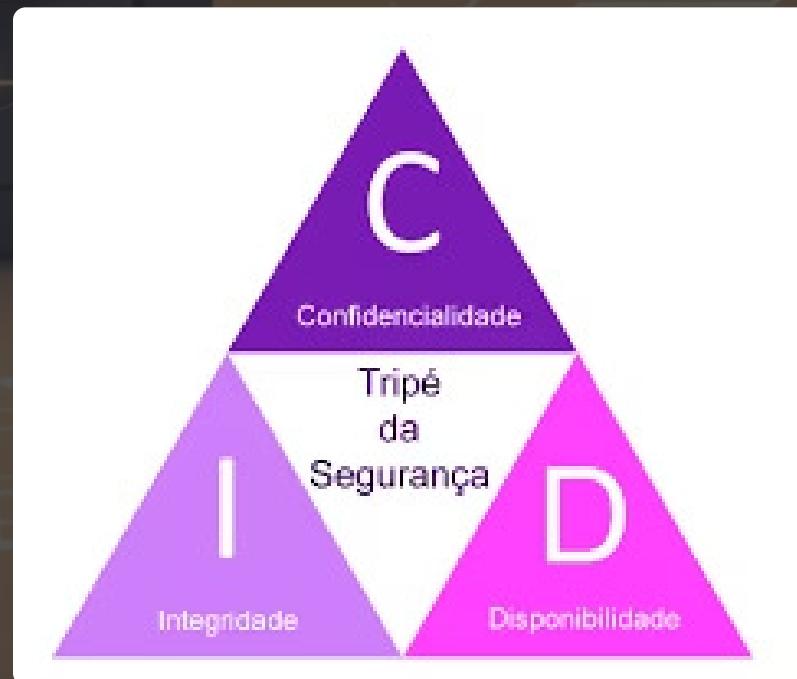
- Luan Garcia, Pentester e Pesquisador de Segurança

O Papel do Profissional de SI



Qual é a missão do profissional de segurança da informação?

- Confidencialidade: Garantir que somente pessoas autorizadas acessem a informação
- Integridade: Manter a informação inteira sempre que a pessoa queira acessá-la
- Disponibilidade: Garantir que a informação esteja lá independente do momento que a pessoa acesse.



Hacker

Lançar um ataque cibernético é uma tarefa complexa. Ele envolve muitos passos e etapas. O atacante precisa entender o sistema que quer invadir, identificar suas vulnerabilidades e encontrar brechas para entrar. Depois disso, ele pode iniciar o ataque, utilizando ferramentas e técnicas avançadas para desestruturar o sistema.

Cadeia de Ataque Cibernético

Como funciona?

O atacante sempre busca entender como funciona o sistema para quebrar o sistema, essa parte guia cada ação do atacante e dá a ele um mapa mental do que deve fazer.

A mentalidade

O atacante sabe que vai lidar com diferentes sistemas de defesa, então antes de atacar, ele busca entender e descobrir quais são os principais métodos de segurança.

Do Reconhecimento a Enumeração

Essas etapas consistem na descoberta de informações e na transformação da informação em um vetor de ataque

O Ataque

O atacante sabe quais são os alvos e quais são os vetores de ataque que ele pode usar, então, ele tem um caminho claro para a invasão.

ATTACK

Um ataque cibernético é uma operação intencionalmente maliciosa contra um sistema informático ou rede. Ele pode ser executado por pessoas ou por computadores. Os ataques podem ser realizados por hackers, terroristas, países ou empresas. Eles podem causar danos físicos ou financeiros, ou simplesmente perturbar o funcionamento de sistemas críticos.

ATTACK

Um ataque cibernético é uma operação intencionalmente maliciosa contra um sistema informático ou rede. Ele pode ser executado por pessoas ou por computadores. Os ataques podem ser realizados por hackers, terroristas, países ou empresas. Eles podem causar danos físicos ou financeiros, ou simplesmente perturbar o funcionamento de sistemas críticos.

O Arsenal do Atacante

1

Negação de Serviço

- DoS (Denial of Service): Sobrecarga de um único ponto de origem.
- DDoS (Distributed Denial of Service): Ataque coordenado de múltiplas fontes, muito mais difícil de mitigar.
- SYN Flood: Envia um avalanche de pedidos de conexão que o servidor tenta manter abertos.

2

Interceptação

- **MitM:** O atacante se posiciona entre a vítima e o serviço.
- **Sniffing:** O atacante usa um software em uma rede para capturar e analisar todos os pacotes de dados que passam entre elas.
- Session Hijacking: O atacante rouba o "cookie de sessão" de um usuário.

3

Spoofing e Poisoning

- IP Spoofing: O atacante altera os cabeçalhos dos pacotes de rede para fazer parecer que eles estão vindo de um endereço ip confiável.
- ARP Poisoning: O atacante envia mensagens ARP falsas em uma rede local.
- DNS Spoofing: O Atacante "envenena" o servidor DNS.

4

Malware

- Worms: Se propagaativamente pela rede, explorando vulnerabilidades para se replicar e infectar novos computadores.
- Trojan: Um ataque pode começar pelo e-mail ou download de um aplicativo que parece legítimo.
- Botnet: Uma rede de dispositivos infectados para execução de ataques.

A Mente do Defensor

1

Negação de Serviço

- Anti-DDoS: Cloudflare, Akamai ou AWS shield colocam-se na frente da sua rede e absorvem o ataque.
- SYN Cookies: O servidor responde ao pedido SYN com um "cookie" especial, mas não aloca recursos.
- Firewall e IPS: Bloqueiam fontes óbvias de ataque e limitam a taxa de conexões de IPs individuais.

2

Interceptação

- Criptografia em Trânsito: Forçar o uso de criptografia em todo tipo de comunicação.
- Cookies Seguros: Configurar os cookies de sessão com as flags HttpOnly e Secure.
- VPNs: Cria um túnel criptografado entre o usuário e a rede da empresa, impedindo que alguém possa obter informações.

3

Spoofing e Poisoning

- Filtragem de Pacotes: Roteadores e Firewalls na borda da rede devem ser configurados (Ingress / Egress Filtering).
- DNSSEC: Usa assinaturas digitais para garantir que a resposta DNS recebida é autêntica e não foi modificada no caminho.
- Dynamic ARP Inspection (DAI): O switch monitora as mensagens ARP e as compara com uma tabela confiável.

4

Malware

- Gestão de Patches: Worms se espalham explorando vulnerabilidades, gerir patches permite que eles não explorem.
- Antivírus e EDR: Escaneiam arquivos, detectam o trojan e o coloca em quarentena.
- Filtro de saída: Bloquear o tráfego de rede suspeito, usando lista de IPs/domínios maliciosos conhecidos.

Os Mecanismos de Defesa



Controle de Perímetro

- **Firewall:** Filtra pacotes, bloqueia portas e soquetes.
- **Servidor Proxy:** Controla o acesso à web e faz cache.
- **VPN:** Cria túneis criptografados para acesso remoto seguro



Proteção de Dados

- **Criptografia:** Proteção de dados em trânsito e em repouso.
- **Assinaturas Digitais:** Garantia de autenticidade de quem enviou o dado.
- **Certificados Digitais:** Validação de identidade de servidores e usuários.



Detecção e Resposta

- **IDS:** Monitora o tráfego e alerta sobre atividades suspeitas.
- **IPS:** Atua ativamente bloqueando as ameaças.
- **SIEM:** Agrega logs de todas as ferramentas.



Controle de Acesso e Endpoints

- **Controle de Acesso:** Permissões de usuário e gerenciamento de senhas
- **Antivírus / EDR:** Proteção contra malwares.
- **NAC:** Verifica se o dispositivo está seguro antes de conectar a rede.

Como um atacante tenta burlar o firewall?

Ataques de Exaustão

O firewall tem recursos limitados. O atacante esgota os recursos do firewall até que ele trave ou pare de filtrar.

Exemplo: DoS/DDoS ou Syn flood até a memória acabar esgotando e o firewall travar/cair.

Serviços Permitidos

O firewall precisa deixar portas abertas. Com base nisso, o atacante envia um ataque dentro de um tráfego permitido.

Exemplo: O atacante envia dados maliciosos para uma aplicação web dentro do tráfego web comum.

Configuração errada

O atacante usa "Ataques Ativos", como varredura de rede, para procurar portas que foram deixadas abertas por engano.

Exemplo: Portas de gerenciamento expostas ao mundo (RDP, SSH ou Telnet)

O que o atacante faz para ser não ser pego por IDS/IPS?

Fragmentando os pacotes

O scan solicitado utiliza pequenos pacotes ip fragmentados. A ideia é dividir o cabeçalho TCP em diversos pacotes.

Exemplo: A opção -f do nmap.

Codificação e ofuscação

O IDS/IPS procura pela assinatura de ataque. O atacante usa alguma codificação para embalar o ataque.

Exemplo: Codificação de URL.

Tunelamento de protocolo

O atacante esconde o tráfego malicioso dentro de um tráfego que é sempre permitido e raramente inspecionado.

Exemplo: Tunelamento DNS

E como protegemos uma rede contra isso?

Análise Profunda de Protocolo (DPI)

Seu firewall ou um sistema de segurança de DNS analisa as próprias consultas DNS, procurando por anomalias com base em parâmetros.

Exemplo: Regra de volume e tamanho da resposta.

Normalização do tráfego e filtragem

Ferramentas modernas, como um WAF ou um IPS avançado normalizam os dados. Além disso, firewalls modernos filtram o tráfego suspeito.

Exemplo: O WAF recebe o ataque e decodifica isso.

Rate limit e Anti-DDoS/flood

O tráfego é roteado primeiramente para o sistema de anti-ddos e o firewall é configurado para limitar conexões de um único IP.

Exemplo: Ataque de 7tbps na Cloudflare.

Como o AV e o EDR detectam um malware?

Baseada em assinatura

O método mais comum. O Software compara arquivos e códigos no sistema com um banco de dados

Análise comportamental

Monitora as atividades e analisa padrões incomuns ou suspeitos que podem identificar algum tipo de ataque.

Detecção heurística

Verificações estáticas e dinâmicas baseado em regras do código, buscando atributos e comportamentos suspeitos

Baseada em Machine Learning

Modelos de treinamento em grandes conjuntos de dados de comportamento benigno e malicioso.

Como o atacante burla o AV/EDR?

Crypters ou packers

Reembalam o vírus, o que muda a impressão digital e faz com que ele pareça ser um arquivo novo e desconhecido.

Entropia

Usamos payloads para reduzir a entropia de um arquivo malicioso, tornando-o semelhante a um arquivo comum.

Fragmentando

Entregamos o Payload em pequenos pacotes com o mínimo de volume de memória em uso fazendo com que pareça comum.

Ruído benígo

Inserimos ruído (como strings falsas ou chamadas de API) no malware para que ele não seja detectado por modelos de Machine Learning.

Como nos proteger quando o ataque vem de dentro?

O erro da Segurança

Ferramentas não bastam: O elo humano é frequentemente o ponto mais fraco. Nenhuma ferramenta é 100% à prova de falhas.

Conscientização constante

A pessoa não precisa saber explorar uma vulnerabilidade ou configurar um firewall, apenas não cair em engenharia social.

O Modelo "Zero Trust"

A estratégia antiga era "Confiar na Rede Interna". A estratégia moderna é "Nunca Confie, Sempre Verifique".

Segurança como processo

O atacante está sempre se adaptando. A defesa também precisa. A segurança não é um produto, é um processo.

Conclusão: O Ciclo infinito da cibersegurança

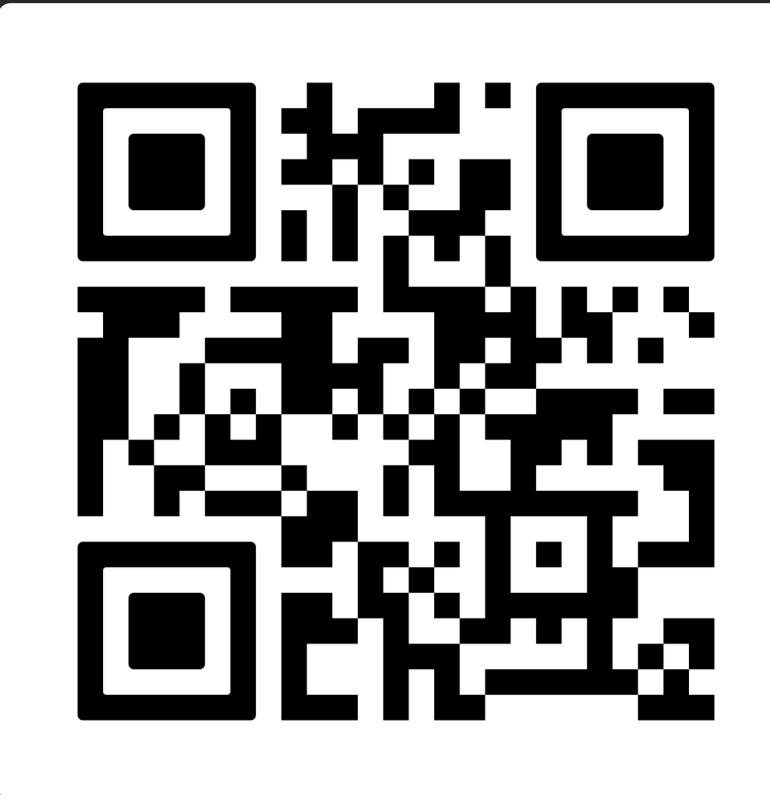
Proteger
manter o
sistema seguro

Melhorar
Aprendizado e
fortalecimento

Detectar
Monitorar o sistema

Responder
Ação imediata a um
ataque

Fim!



https://linktr.ee/luangarcia_23