Lista de Exercícios: Aula 07

Aluno: João Victor de Souza Costa

RA:825150259

1) Um pentest, é uma simulação controlada de um ataque cibernético contra um sistema, rede ou aplicação com o objetivo de identificar vulnerabilidades de segurança que poderiam ser exploradas por invasores reais.

Etapas: Planejamento e reconhecimento, enumeração, ganho de acesso, escalada de privilégios, manutenção de Acesso, cobertura de Rastros, relatório.

2) Ataque DoS: o ataque vem de vários dispositivos comprometidos, dificultando a defesa, com objetivo de sobrecarregar os recursos (CPU, memória), fazendo com que o serviço fique lento, indisponível ou caia completamente.

Ransomware: Pode tornar sistemas inteiros indisponíveis, afetando hospitais, empresas, governos, etc. O atacante exige resgate ($) para liberar o acesso.

infraestrutura de rede (como DNS spoofing): Visam comprometer serviços essenciais de rede, como DNS (que traduz domínios para IPs) ou BGP (que controla o tráfego entre roteadores da internet). Podem redirecionar tráfego ou simplesmente tornar sites e serviços inacessíveis.

3) Conformidade, em inglês é conhecido como compliance.

4)

| **Recurso** | **Firewall** | **IDS (Intrusion Detection System)** | **IPS (Intrusion Prevention System)** |
| --- | --- | --- | --- |
| **Função** | Controla o tráfego de rede, permitindo ou bloqueando com base em regras definidas. | Detecta atividades suspeitas ou anômalas na rede. | Detecta e impede ataques em tempo real, bloqueando o tráfego malicioso. |
| **Atuação** | Filtra pacotes e controla acessos (entrada/saída). | Apenas detecta e alerta sobre possíveis intrusões. | Detecta e age preventivamente, interrompendo as intrusões. |
| **Modo de Ação** | Passivo ou ativo, com bloqueio baseado em regras. | Passivo, com emissão de alertas e relatórios. | Ativo, interrompe ou bloqueia ataques em tempo real. |
| **Objetivo** | Proteger a rede e evitar acessos não autorizados. | Monitorar e identificar comportamentos anormais ou maliciosos. | Prevenir ataques em tempo real e proteger a rede ativamente. |
| **Exemplo** | Firewall de rede ou de aplicação. | Sistema que verifica tráfego e gera alertas quando detecta atividades suspeitas. | Sistema que além de alertar, pode bloquear pacotes ou sessões suspeitas. |

**Resumo:**

* **Firewalls**: Controlam o tráfego com base em regras, filtrando ou bloqueando acessos.
* **IDS**: Apenas detecta e alerta sobre possíveis ameaças ou comportamentos anormais.
* **IPS**: Vai além do IDS, bloqueando ativamente as ameaças detectadas.

5- Criar senhas fortes, com letras, números e símbolos.

Evitar usar a mesma senha em vários sites.

Ativar a verificação em duas etapas sempre que possível.

6 - a) O uso de um sistema operacional não original (pirata), isso pode ter falhas de segurança, ausência de atualizações e deixar o computador exposto a riscos.

b) Possibilidade de ataques, como vírus, malwares ou roubo de dados, justamente por causa da falta de proteção em um sistema pirata.

c) Instalar uma versão original do Windows e manter o sistema sempre atualizado, além de usar antivírus confiável.

7 - a) Uso de nome de usuário padrão (admin), que é fácil de adivinhar.

b) Invasores podem acessar o sistema usando essas credenciais conhecidas.

c) Trocar o nome de usuário e senha padrão por credenciais fortes e personalizadas.

8 - a) Ana utiliza a chave pública de Bob para criptografar a mensagem, garantindo que somente ele, com a chave privada correspondente, consiga decifrá-la

b) Bob utiliza sua chave privada para decifrar a mensagem que foi cifrada com sua chave pública.

c)Ana criptografa a mensagem (ou o hash dela) com sua chave privada, criando uma assinatura digital que garante que a mensagem é realmente dela e que não foi alterada.

d) Carlos usa a chave pública da Ana pra verificar a assinatura digital e, com isso, confirmar se a mensagem é mesmo dela e se não foi modificada.

9 - a) O certificado digital assegura que apenas as partes envolvidas na transação (o cliente e o banco) possam acessar e ler os dados trocados. Isso acontece porque a mensagem é criptografada com a chave pública do destino (o banco) e só pode ser decifrada pela chave privada correspondente do banco.

b) O certificado digital também garante que a transação tenha origem confiável (como o Banco do Brasil, no exemplo). Além disso, assegura que a mensagem não foi alterada durante o envio. O uso de assinaturas digitais garante que qualquer modificação nos dados seja detectada, pois, caso os dados sejam alterados, a assinatura se torna inválida. E a data de validade no certificado digital dificulta a falsificação, pois limita o período em que ele pode ser usado, sendo automaticamente rejeitado após o vencimento. Isso garante que qualquer tentativa de fraude no certificado seja detectada, evitando o uso de certificados expirados ou comprometidos e garantindo a verificação de sua autenticidade e integridade.

10) Registros de autenticação (login/logout) – Registram quando os usuários fazem login e logout, incluindo informações sobre o horário e o dispositivo de acesso. Isso ajuda a identificar acessos fora do comum ou por usuários não autorizados.

Tentativas de acesso não autorizado – Capturam falhas de login ou tentativas de acesso a sistemas restritos, que podem indicar tentativas de ataques como força bruta ou invasões.

Alterações em dados e configurações – Monitoram mudanças em arquivos importantes ou configurações de segurança, como a modificação de permissões, instalação de software, ou exclusão de dados, ajudando a rastrear ações suspeitas ou mal-intencionadas.

Esses logs são cruciais para auditorias, identificação de incidentes e resposta rápida a possíveis falhas de segurança.