ATIVIDADE ENADE - SPRINT 02 - AULA 04

Aluno: Luan Calazans

QUESTÃO 01

Texto-base:
As etapas de um teste de intrusão incluem uma fase de coleta de informações que permite ao pentester levantar os vetores de ataque mais prováveis. Essa fase envolve não apenas varredura de portas e serviços, mas também a correlação com informações de sistemas operacionais, banners, diretórios públicos e registros DNS.

Enunciado:
A partir do cenário abaixo, identifique o vetor de ataque mais provável e relacione-o com a etapa do teste de intrusão onde essa descoberta ocorre.

Cenário:
Durante um reconhecimento em um ambiente corporativo, o analista identificou um serviço FTP na porta 21 com acesso anônimo habilitado. Posteriormente, encontrou arquivos contendo referências a scripts desatualizados de backup que chamam arquivos `.sh` armazenados em `/tmp`.

Considerando o contexto e a metodologia de testes de intrusão, avalie as afirmativas a seguir:

I. A identificação do serviço FTP com acesso anônimo faz parte da fase de varredura e fingerprinting.

II. A exploração de scripts de backup vulneráveis pode indicar um vetor de escalonamento de privilégio local.

III. O reconhecimento de serviços e diretórios como `/tmp` está limitado exclusivamente à fase de pós-exploração.

IV. O acesso anônimo ao FTP deve ser documentado, mas não constitui risco, já que não executa código diretamente.

Assinale a alternativa correta:

a) Apenas as afirmativas I e II estão corretas.

QUESTÃO 02

Texto-base

A equipe de segurança de uma empresa de médio porte está conduzindo um pentest interno autorizado, com o objetivo de avaliar a exposição de seus sistemas à exploração de vulnerabilidades técnicas. O teste será conduzido por um time Red Team devidamente autorizado por LOA (Letter of Authorization), e está em sua fase inicial de **information gathering**. A arquitetura-alvo inclui máquinas com sistemas Windows e Linux, alguns serviços expostos em portas padrão e servidores web em ambiente de teste.

Para uma das primeiras etapas da operação, o time optou por ferramentas nativas do Kali Linux que permitam **coleta ativa**, levantamento de **superfície de ataque**, e **identificação de serviços e banners**, como parte da preparação para exploração futura.

Enunciado:

Considerando as boas práticas de pentest e os conteúdos relacionados à etapa de varredura ativa, assinale a alternativa que apresenta um **conjunto coerente de ferramentas e funcionalidades** para esta fase da operação.

Alternativas

c) **Nmap, Netcat e Enum4linux**, pois possibilitam varredura de portas, obtenção de banners e enumeração de serviços.

QUESTÃO 03

Texto-base:
As fases de um teste de penetração são fundamentais para o sucesso da operação, garantindo que as atividades sejam conduzidas com método, ética e alinhamento aos objetivos de negócio. Desde a fase inicial de coleta de informações até a entrega do relatório final, cada etapa requer ferramentas, técnicas e posturas distintas. Em muitos casos, especialmente em ambientes corporativos, é necessário executar ataques simulados controlados para validar defesas, identificar falhas e mitigar riscos antes que sejam explorados por agentes maliciosos reais.

Nesse contexto, compreende-se que um pentest não é apenas uma atividade técnica, mas também um processo estruturado que exige planejamento, execução controlada e comunicação eficiente com os stakeholders.

Enunciado:
Considerando as fases que compõem um teste de penetração e os

princípios que regem sua execução em ambientes organizacionais, assinale a alternativa que descreve corretamente a relação entre a fase e sua característica principal.

c) A análise pós-exploração tem como objetivo principal o estabelecimento de persistência e movimentação lateral.

QUESTÃO 04

Enunciado

Uma equipe de segurança ofensiva foi contratada para realizar um pentest em um ambiente corporativo utilizando a metodologia de Black Box. Durante a atividade, os profissionais simularam diferentes técnicas conforme as fases do teste. As ações abaixo foram registradas no relatório parcial.

Situações apresentadas:

I) Utilização de ferramentas como *theHarvester* e *whois* para levantamento de informações iniciais sem interação direta com os sistemas do alvo.

II) Envio de pacotes TCP com *flags* específicas para identificar portas abertas e serviços ativos na rede da empresa.

III) Exploração de uma vulnerabilidade crítica no CMS utilizado no portal público da organização.

IV) Uso de uma *web shell* para escalar privilégios, obter persistência e extrair dados sigilosos da rede interna.

Associe cada situação à fase correspondente de um teste de penetração:

1. Coleta de informações passiva
2. Varredura e enumeração

3. Exploração
4. Pós-exploração

Em seguida, assinale a alternativa que apresenta a sequência correta de associação:

A) I–1 II–2 III–3 IV–4

QUESTÃO 05

Texto-base:

O reconhecimento (ou *recon*) é a primeira fase crítica de um teste de penetração e envolve a coleta de informações sobre o alvo antes de qualquer tentativa de exploração. Essa fase pode ser dividida em **reconhecimento passivo**, no qual o atacante obtém dados sem interagir diretamente com os sistemas da vítima, e **reconhecimento ativo**, onde há interação direta com os ativos-alvo, com o risco de gerar alertas nos sistemas de defesa. A distinção entre esses métodos está ligada não apenas à técnica, mas à postura estratégica do atacante, ao contexto do teste (ex: escopo legal), e à capacidade de disfarçar intenções maliciosas. Enquanto o passivo é ideal para manter o sigilo da operação, o ativo oferece maior profundidade, permitindo mapeamento preciso de serviços, portas, sistemas operacionais e vulnerabilidades potenciais. No entanto, ambos são complementares e, quando aplicados de forma inteligente, aumentam a eficácia e a discrição do pentest.

Enunciado:

Com base no texto-base e nos conceitos relacionados à fase de reconhecimento em testes de penetração, discorra sobre a importância da distinção e aplicação estratégica do reconhecimento ativo e passivo no contexto da segurança ofensiva. Em sua resposta, aborde:

(i) as principais diferenças técnicas e operacionais entre os dois métodos;

(ii) os riscos e benefícios da aplicação de cada tipo de reconhecimento durante a etapa inicial de um pentest; e
(iii) por que a combinação dessas abordagens pode potencializar a eficácia do processo de coleta de informações e preparação para a exploração.

(Limite: 20 linhas – Valor: 10,0 pontos)

Fazer o reconhecimento e a enumeração é a parte mais importante no pentest,
porque é com ela que você adquire dados, informações, versões, banners, tecnologia
e tudo isso é essencial lá na frente para executar, por exemplo, um shell reverse,
mas isso é outra história, por enquanto.

Existem tipos de enumeração, como passiva e ativa:
A passiva você pode usar docs do próprio Google, navegador, websites (whois etc.),
e na passiva você coleta dados sem fazer "barulho", sem deixar rastros nos arquivos de logs do servidor.
Porém, você não consegue tantas informações privilegiadas, mas não deixa de ser importante!

E a ativa: você já utiliza ferramentas para coletar melhor informações e dados, como Nmap, Enum4linux, Burp, Netcat.
O lado negativo é que elas fazem "barulho", deixando rastros nos arquivos de logs do servidor.

Usar ambas as enumerações garante um melhor entendimento.
É claro que você tem que estar fazendo suas anotações também. Com a análise passiva,
você pode descobrir uma aba de "equipe"; ali você já consegue possíveis usuários de login,
que você pode usar em uma análise ativa, como entrar em um SSH.

QUESTÃO 06

Texto-base:

O Nmap é uma das ferramentas mais utilizadas por analistas de

segurança ofensiva durante a fase de reconhecimento ativo em testes de penetração. Por meio de técnicas de varredura de portas e detecção de serviços, o Nmap permite não apenas identificar hosts ativos e suas respectivas portas abertas, mas também realizar *banner grabbing*, que é a extração de informações

`--script=banner`

`--script=banner`

textuais enviadas por serviços, como servidores web ou FTP, quando se conectam. Entretanto, esse tipo de ação pode levantar alertas em sistemas de detecção, além de depender da forma como os serviços foram configurados para responder a requisições. Há opções no Nmap, como `-sV` para detecção

de versão e para coleta específica, que podem ou não

retornar dados úteis, dependendo do alvo e do contexto de segurança.

Enunciado:

Durante a execução de uma etapa de reconhecimento ativo em um teste de penetração autorizado, um analista utiliza o Nmap com a intenção de obter informações detalhadas sobre os serviços em execução, incluindo banners e versões. Contudo, ao aplicar as opções `-sV` e `--script=banner` , o resultado não apresenta os banners esperados em determinados serviços identificados

como abertos.

I – O parâmetro do Nmap pode falhar em retornar dados se

o serviço estiver configurado para ocultar ou filtrar respostas iniciais a conexões. PORQUE

II – O reconhecimento ativo sempre consegue extrair banners dos

serviços detectados, desde que as portas estejam abertas e acessíveis.

C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

QUESTÃO 07

Texto-base:
O Nmap é uma ferramenta essencial para analistas de cibersegurança durante a fase de varredura e enumeração em um teste de intrusão. Com ela, é possível mapear hosts ativos, identificar portas abertas e descobrir serviços e versões rodando nos alvos. No entanto, para utilizar o Nmap de forma eficaz, é
imprescindível que o operador tenha sólidos conhecimentos sobre redes de computadores, especialmente os protocolos da pilha TCP/IP.

Ao compreender como o TCP estabelece conexões com handshake e como o UDP funciona sem esse mecanismo, o analista consegue interpretar resultados corretamente e ajustar os parâmetros de varredura para minimizar falsos positivos e negativos. Por exemplo, uma porta UDP pode parecer "fechada" por simplesmente não responder, enquanto o TCP tende a dar respostas mais claras. Essa diferença impacta diretamente o sucesso da identificação de vulnerabilidades e o planejamento do ataque.

Enunciado:
Com base na importância da compreensão dos fundamentos de redes para o uso eficaz do Nmap, explique **como o funcionamento distinto dos protocolos TCP e UDP pode influenciar a coleta de informações**

durante um pentest. Em sua resposta, destaque: (i) **um exemplo prático de varredura que demonstre essa diferença**, (ii) **um risco associado à má interpretação de resultados UDP**, e (iii) **uma recomendação técnica para reduzir a chance de erro durante a varredura com o Nmap**.

(Limite: 20 linhas – Valor: 10,0 pontos)

TCP = garante a entrega ,e te retorna o status se foi entregue o não de acordo com um calculo de bytes
se os numeros baterem esta tudo certo.
UDP = ele garante a entrega porém não garante a integridade do que está sendo entregue, assim você não tem retorno.

exemplo pratico : vc vai fazer uma varredura UDP em um server ,como u UDP não garante a resposta ,
pode ter um serviço rodando
na porta 5096 mas como ele é UDP o nmap pode reconhecer que nao tem nenhum serviço rodando naquela porta,
compromentendo a coleta

recomendação: Utilizar opções que aumentem a confiabilidade da detecção de portas ,
--max-retries <n> ,
--host-timeout <tempo> ,
-sV,
-Pn (Para varreduras em servidor win)

QUESTÃO 08

Texto-base:

Antes de qualquer tentativa de exploração de vulnerabilidades, a fase de coleta de informações, também conhecida como *reconhecimento*, é fundamental em qualquer operação de pentest. É nesse momento que o analista mapeia a superfície de ataque, identifica portas e serviços,

descobre versões de softwares em uso e analisa o comportamento do alvo no contexto da rede. Essa etapa, quando bem executada, aumenta significativamente a eficácia dos testes subsequentes, reduz o risco de causar interrupções indesejadas e permite que o profissional escolha vetores de ataque mais precisos e silenciosos.

Ignorar ou subestimar o *information gathering* pode levar a decisões equivocadas, exploração ineficaz ou, em casos extremos, à detecção prematura
da atividade ofensiva.

Com base nas situações descritas a seguir, identifique **a ação que mais representa uma falha na etapa de levantamento de informações** e que, por consequência, compromete diretamente a fase de exploração:

I) Utilização de scripts automatizados sem análise prévia do escopo do alvo.
II) Enumeração de serviços web com coleta de banners e fingerprints.
III) Escaneamento de rede com definição clara de ranges IP e técnicas de evasão.
IV) Correlação de informações públicas (OSINT) sobre domínios e subdomínios.
V) Testes de exploração iniciados sem mapear previamente os serviços rodando no alvo.

E) V–ação incorreta, pois iniciar testes sem reconhecimento adequado compromete o pentest.

QUESTÃO 09

Texto-base:

O Sistema de Nomes de Domínio (DNS) é um dos pilares da arquitetura da internet moderna. Ele permite que nomes legíveis por humanos, como `www.empresa.com` , sejam traduzidos em endereços IP utilizados pelas máquinas, como `192.0.2.1` . Essa estrutura distribuída de resolução é composta por zonas autoritativas, registros de recursos (como A, AAAA, CNAME, MX, TXT) e servidores responsáveis, organizando a navegação de forma transparente ao usuário final.

Apesar de sua utilidade, o DNS também é vetor de múltiplas ameaças cibernéticas, incluindo ataques de envenenamento de cache (DNS poisoning), tunneling, amplificação e, mais recentemente, o **Subdomain Takeover** — uma
técnica sofisticada que explora configurações incorretas ou registros órfãos em subdomínios.

No ataque de Subdomain Takeover, um subdomínio aponta para um serviço externo (como GitHub Pages, Heroku, AWS S3, entre outros), mas esse recurso externo não está mais alocado (por exemplo, a bucket foi deletada ou o app removido). Quando o DNS ainda mantém o apontamento (ex: via CNAME), um atacante pode registrar o serviço anteriormente utilizado e assumir o controle do subdomínio. Isso permite ações como hospedagem de conteúdo malicioso, phishing ou injeção de scripts, sem alertar os mecanismos de segurança baseados apenas no domínio raiz. Empresas de grande porte já foram vítimas dessa falha, que é muitas vezes ignorada em processos tradicionais de segurança.

O desafio é que muitos testes de segurança não validam todos os subdomínios ou não verificam a presença de registros órfãos. Portanto, é fundamental entender a topologia do DNS e revisar frequentemente os registros DNS ativos, em especial CNAMEs para serviços de terceiros, de

modo a evitar que configurações inativas se tornem pontos vulneráveis exploráveis por adversários.

Enunciado:

Com base no texto e em seus conhecimentos sobre o funcionamento do DNS e as vulnerabilidades exploráveis por Subdomain Takeover, **qual das alternativas representa a prática mais eficaz para mitigar esse tipo de ataque em ambientes corporativos?**

E) Realizar varreduras periódicas e automatizadas nos registros DNS da organização, validando a existência dos recursos apontados por CNAMEs e removendo entradas órfãs.

QUESTÃO 10

Contexto:

Durante uma simulação de ataque direcionado em um laboratório de Red Team, uma equipe de analistas recebeu a missão de identificar potenciais vulnerabilidades de exposição pública de uma empresa fictícia chamada **SkyCom Technologies**.

A análise deveria partir exclusivamente de fontes abertas (OSINT), sem contato direto com os sistemas internos da organização. Um dos membros da equipe sugeriu o uso da ferramenta **Maltego**, que permite a visualização e correlação de dados de maneira gráfica e automatizada.

Ao longo do exercício, os analistas conseguiram mapear relacionamentos entre subdomínios, descobrir e-mails de funcionários expostos em vazamentos passados, além de identificar conexões entre IPs públicos e

servidores hospedados em provedores distintos. Tudo isso com poucos cliques e uso estratégico de *transforms* nativas da ferramenta.

A partir da análise do cenário descrito e de seus conhecimentos sobre ferramentas de coleta e análise de informações, avalie as afirmativas abaixo:

I – O Maltego é uma ferramenta de OSINT que permite a **automatização de transformações sobre entidades**, facilitando a descoberta de relacionamentos entre alvos.

II – A ferramenta possui módulos capazes de realizar ataques ativos e invasivos, sendo utilizada como parte da fase de exploração técnica.

III – O uso do Maltego está fortemente associado à **visualização gráfica de relacionamentos**, o que o torna útil tanto para fins ofensivos quanto para investigações forenses e análise de risco.

IV – Embora poderosa, a ferramenta é de uso restrito a ambientes corporativos que possuam infraestrutura cloud, sendo incompatível com redes locais ou pequenas investigações individuais.

Assinale a alternativa correta:

B) Apenas as afirmativas I e III estão corretas.