Administração e Segurança de Redes de Computadores

C.T. Informática para Internet

Prof. Vinícius Alves Hax

Antes

- Conceito de auditoria
- Reconhecimento passivo

Hoje

- Descobrindo mais informações a partir da rede
- Explorando vulnerabilidades

Revisando as etapas do pentest

- Reconhecimento
  - Passivo: sem entrar em contato → ex: descobrir informações na Internet
  - Ativo: entrando em contato. Ex: usar ping para descobrir hosts ativos
- Sondagem da rede
- Sondagem dos hosts
- Exploração de vulnerabilidade
- Escalada de privilégios

Entrando na rede

- Para entrar na rede, as tentativas mais comuns são:
  - Pode-se tentar acesso físico a um conector RJ45
  - Tentar o primeiro acesso através da rede WiFi do estabelecimento
  - Se a invasão começar a partir da Internet pode-se começar a testar primeiro os servidores DNS e Web

Sondagem

- Rede primeiro x Host primeiro
  - Dependendo do contexto a ordem dessas etapas pode ser invertida
  - Quando já se está dentro da rede, geralmente o próximo passo é descobrir os hosts da rede
  - Quando já existe um alvo definido (ex: servidor específico), geralmente a próxima etapa é sondar esse host

Passo: Descoberta de hosts

- Após descobrir informações sobre o alvo com o reconhecimento passivo (sem entrar em contato com o alvo) e o reconhecimento ativo (entrando em contato) o próximo passo muitas vezes é descobrir quais hosts da rede
- Pode-se até usar com hosts da Internet mas esse passo é mais interessante quando já se está dentro da rede

Ferramenta nmap

- O nmap é uma das ferramentas mais utilizas tanto para sondar (usa-se bastante o termo “varrer” e/ou “scanning”) a rede e também algum host específico
- O nmap tem muitas opções e seu uso aprofundado não é o tópico desse curso
- Ele também é bastante usado em diagnóstico de problemas
- Seu uso pode ser detectado pelo administrador de redes

Nmap para varrer a rede

- Exemplo de uso:

  $ nmap -sP 172.19.20.*

  - Vai procurar todos os hosts dentro da rede atual cujo IP começam com 172.19.20

Host scanning com nmap

- Uma vez descoberto os IPs pode-se usar novamente o nmap para descobrir mais informações (qual sistema operacional e versão do mesmo, quais portas estão abertas, etc)

  $ nmap IP

- Exemplo

  $ nmap 127.0.0.1

Explorando vulnerabilidades

- Uma vez obtidas informações sobre a rede e principalmente sobre o host (sistema operacional, portas abertas, etc) a próxima etapa é explorar possíveis vulnerabilidades.
  - Um caminho nesse momento é procurar vulnerabilidades. Essa procura pode ser:
    - Manual através de procura em sites como https://www.exploit-db.com/
    - Semi-automatizada através de softwares como metasploit ou burp suite

Auditoria externa

- Contratada:
  - Para reduzir custos
  - Por não ter o “*know how*”
  - Para dar mais confiabilidade: muito comum em auditoria fiscal. Ex: Padrões ISO
- Órgãos de controle
  - Entre órgãos públicos. Ex: Controladoria Geral da União (CGU)
  - Para agentes privados. Ex: fiscalização sanitária

Tipos de auditoria

- Financeira
- Ambiental
- De qualidade
- De segurança do trabalho
- De segurança da informação
- ???
- ???
- Etc

Em TI, auditoria está muito ligada à segurança da informação.

- Por que isso acontece?

Auditoria

- Padrões:
  - Internos (desenvolvidos pela própria organização)
  - Normas e leis: NBR 27001/27002; Lei Geral de Proteção de Dados (LGPD); etc.

Auditoria de Segurança da Informação

- “Podemos definir auditoria como a medição de algo contra um padrão. Apesar de estarmos tratando de Segurança da Informação, o conceito de auditoria pode ser aplicado em qualquer área, como qualidade, ambiental, financeira, de conformidade etc.”

PEIXINHO, Ivo de Carvalho; FONSECA, Francisco M.; LIMA, Franscisco M. Segurança de Redes e Sistemas. Escola Superior de Redes RNP", Rio de Janeiro/RJ, 2013.

Auditoria de Segurança da Informação (2)

“Quando tratamos especificamente de auditoria de SI, podemos estar auditando o cumprimento de uma política de segurança, a eficácia de um novo sistema de segurança (como um firewall), se um sistema está com todas as correções conhecidas aplicadas, entre outros. [...] Entre as técnicas utilizadas em auditorias, as mais comuns são a análise de vulnerabilidades e os testes de penetração (penetration testing ou pentest).”

Peixinho et al

Técnicas comuns

- Análise de vulnerabilidade: mais específica; geralmente contra um “alvo” único: hardware ou software; informações internas;
- Pentest: mais abrangente, geralmente contra uma rede ou um sistema; teste “black box”;
  - Teste black box: o testador não sabe nada sobre o funcionamento interno do sistema
    - É o contrário do teste “white box” no qual o testador usa o conhecimento do sistema para elaborar os testes

Análise de vulnerabilidade

- Podemos averiguar:
  - Senhas e configurações padrão
    - Exemplo: cofre
  - Ataques de negação de serviço
  - Controle de acesso
  - Falhas comuns (especialmente recentes)
    - Geralmente com uso de ferramentas automatizadas
  - Código-fonte (backdoors e/ou erros de programação)

Etapas de um Pentest

- 1. Descoberta de informações públicas: Envolve obter informações públicas sobre o alvo
- 2. Mapeamento de hosts da rede/portas abertas
- 3. Exploração de vulnerabilidades contra host/sistema
- 4. Escalada de privilégios
- 5. Pós-exploração

Pós-exploração

- 1. Decidir quais próximos alvos na rede
- 2. Procurar alguma informação específica no host comprometido
- 3. Cobrir os rastros
- 4. Elaborar relatório contendo sugestões de melhoria

Descoberta de informações

- A descoberta de informações geralmente se dá a partir de fora da rede.
- Pode ser classificada em ativa ou passiva:
  - Passiva: Usa-se somente informações públicas. O host pode nem saber que está sendo atacado.

Referências

- Pentest fundamentals
  https://tryhackme.com/r/room/pentestingfundamentals
- Passive Reconnaissance
  https://tryhackme.com/r/room/passiverecon
- PEIXINHO, Ivo de Carvalho; FONSECA, Francisco M.; LIMA, Franscisco M. Segurança de Redes e Sistemas. Escola Superior de Redes RNP", Rio de Janeiro/RJ, 2013.