Universidade do Minho
Mestrado Integrado em Engenharia Informática
Tecnologia de Segurança
TP 2 - Parte B: PenTest - Scanning

Data de submissão: 01/12/2019

Parte 1

Para a parte 1 deste trabalho prático será necessário o uso do ambiente de testes configurado na aula anterior (*i.e.*, VM Kali Linux e VM Metasploitable 2). Certifique-se que há conectividade entre as duas VMs através da sub-rede 172.16.x.0/24. As questões Q1 - Q3 deverão ser respondidas através de *scanning* ativo efetuado a partir da VM Kali Linux, sendo a VM Metasploitable 2 o *target* do *scan*. Para isso, usarão o Nmap[1] e o Wireshark na VM Kali Linux.

Todas as respostas deverão conter imagens que demonstrem os resultados obtidos e sustentem a correspondente discussão.

Q1: Com o Wireshark em modo de captura, execute as opções de *scan* abaixo listadas (usando o Nmap). Apresente e discuta as diferenças entre cada um dos modos de *scan*, os resultados obtidos em cada um deles, as diferenças em termos de volume de dados transmitidos e detectabilidade por parte de *firewalls* e/ou IDSs. Use imagens de amostras de tráfego para demonstrar os resultados obtidos.

Modos de scan:
1) *nmap -sn target*
2) *nmap -sU target*
3) *nmap -sT target*
4) *nmap -sS target*

Q2: Esta questão deverá considerar dois sistemas como target: VM Metasploitable 2 e o servidor com endereço IP 45.33.32.156. Verifique e demonstre que o segundo sistema está ativo. Em seguida, com o Wireshark em modo de captura, execute as opções de *scan* abaixo listadas (usando o Nmap). Apresente e discuta as diferenças entre cada um dos modos de *scan;* os resultados obtidos em cada um deles e para cada sistema target; as diferenças em termos de volume de dados transmitidos; e detectabilidade por parte de *firewalls* e/ou IDSs. Use imagens de amostras de tráfego para demonstrar os resultados obtidos.

Modos de scan:
1) *nmap -sA target*
2) *nmap -sF target*
3) *nmap -sN target*
4) *nmap -sX target*

Q3: Usando os diferentes métodos de *scanning* ativo do Nmap, identifique o Sistema Operativo da VM Metasploitable 2. Use imagens dos resultados que sustentam a sua resposta.

---

[1] É fundamental o uso da documentação oficial do Nmap, que pode ser encontrada em https://nmap.org/

Q4: Usando os diferentes métodos de scanning ativo do Nmap, identifique os serviços ativos na VM Metasploitable 2. Escolha três destes serviços e identifique as três mais recentes vulnerabilidades publicamente conhecidas.

Parte 2

Para a parte 2 do trabalho prático, certifique-se que tem o OpenVAS/*Nessus* e o *Snort* instalados e corretamente configurados na VM Kali Linux. Atualize as assinaturas (*rules*) do *Snort*, para que contenham as últimas assinaturas de vulnerabilidades[2]. Efetue um *scan* ao sistema VM Metasploitabe 2 a partir do OpenVAS/*Nessus*. Durante este processo, garanta que o *Snort* está em modo activo e que a opção *output alert_full: alert.full* foi incluída no ficheiro de configuração[3]. Além disso, capture o tráfego gerado através do Wireshark. Durante o processo de *scanning*, é expectável que o S*nort* identifique parte do tráfego gerado como possível tentativa de intrusão.

Todas as respostas deverão conter imagens que demonstrem os resultados obtidos e sustentem a correspondente discussão.

Q5: Discuta os resultados globais do processo de *scanning* ao sistema VM Metasploitable 2. Para isso, use os resultados apresentados pelo *Nessus*/*OpenVAS*.

Q6: Examine o output do *Snort*[4] e escolha dois eventos identificados como tráfego anómalo. Para cada evento escolhido, identifique o respetivo tráfego capturado via *Wireshark* e o descreva. Se possível, inclua o CVE da vulnerabilidade e o método de exploração usado[5].

Q7: Observe que algumas notificações do IDS não possuem vulnerabilidade correspondente no sistema de Scan (Nessus/OpenVAS). Apresente e discuta as possíveis razões para estas diferenças.

Q8: Nesta atividade você tentará solucionar algumas das vulnerabilidades encontradas na VM Metasploitable 2. Para isso, analise todas as informações disponíveis para cada vulnerabilidade, tendo em conta as bases de dados de vulnerabilidades (*e.g.*, NVD) e as possíveis diferentes maneiras de contornar o respetivo problema (inclua uma descrição genérica sobre a vulnerabilidade). Ao final dos procedimentos escolhidos para cada vulnerabilidade, execute um novo *scan* via OpenVAS/Nessus para garantir que, de facto, esta já não é detetada (não esqueça de incluir os ficheiros no relatório final). Avalie

---

[2] Download disponível em: https://www.snort.org/downloads/#rule-downloads

[3] Ver Secção 3 do documento de instalação e configuração do "ambiente de pentest".

[4] Se necessário, consulte a documentação em https://snort.org/documents#OfficialDocumentation

[5] Como dica, use a descrição fornecida no relatório de scan do Nessus.

também se a solução encontrada resolve outros problemas (*i.e.*, outras vulnerabilidades) e discuta o seu efeito. As vulnerabilidades que deverão ser corrigidas são[6]:

- HTTP TRACK/TRACE Methods Allowed
- rexecd Service Detection
- Bind Shell Backdoor Detection
- VNC Server 'password' Password

[6] Identificadores oriundos do Nessus. A descrição poderá ser diferente no OpenVAS.