Transcrição de simulação
Execute o reconhecimento de rede com ferramentas de varredura de rede

Tarefa 1: Explore o prompt de comando

1. Nesta simulação, você verá como realizar reconhecimento de rede com ferramentas de varredura de rede para reunir informações sobre uma rede de computador. Selecione a **seta Avançar** para continuar.

2. Primeiro você usará ferramentas de linha de comando. Uma interface de linha de comando (CLI) é uma interface de usuário na qual os usuários digitam comandos para navegar e gerenciar o sistema. Com ele você conclui algumas tarefas mais rápido e até as automatiza. Selecione a seta **Avançar** para continuar (observe que a versão para Windows do CLI chama-se prompt de comando. Selecione **X** para fechar esta janela e continuar.)

3. Você pode acessar o prompt de comando de maneiras diferentes. Nessa simulação, você o abrirá no **menu Iniciar**. Primeiro, selecione o ícone **Iniciar**, que é o ícone do Windows na barra de tarefas.

4. O menu **Iniciar** será aberto. Role até o fim da lista de aplicativos e selecione **Windows System (Sistema Windows)**.

5. Selecione **Command Prompt (Prompt de comando)** na lista.

6. A janela Command Prompt (Prompt de comando) será exibida. O prompt contém o diretório ou a pasta atual em que você está trabalhando. No momento você está trabalhando em `C:\Users\cyber`. Selecione a **seta Avançar** para continuar.

7. Agora vamos explorar alguns comandos úteis para reconhecimento de rede. Você vai executar esses comandos em scanme.nmap.org. O criador do Nmap's, Gordon Lyon, configurou este host para você digitalizá-lo para testar o Nmap. Mas, por enquanto, você vai digitalizá-lo com ferramentas de linha de comando. Selecione a **seta Avançar** para continuar.

8. Nslookup é uma ferramenta de linha de comando muito utilizada para solucionar problemas de rede, verificar configurações de DNS e reunir informações sobre nomes de domínio específicos. Digite `nslookup scanme.nmap.org` no prompt de comando e pressione **Enter**.

9. A saída contém o endereço IP 45.33.032.156 associado ao nome de domínio informado. Selecione a **seta Avançar** para continuar.

10. Agora, você executará um teste de Ping para descobrir até que ponto o host está localizado em sua rede. Digite `ping 45.33.32.156` no prompt de comando e pressione **Enter**.

11. Analise a saída. O tempo de resposta, medido em milissegundos, indica quanto tempo levou para cada pacote chegar ao seu destino, e o tempo de cada pacote ativo (TTL) é 53. A seção Estatísticas do ping lista o número total de pacotes enviados e recebidos. Selecione a **seta Avançar** para continuar.

12. Agora você executará um traceroute para mapear a conexão entre seu dispositivo e o host de destino. Digite `tracert 45.33.32.156` no prompt de comando e pressione **Enter**.

13. A saída indica que há 14 switches ou roteadores entre o seu dispositivo e o host. Ela também revela informações sobre todos os dispositivos do caminho, incluindo seu endereço IP e o período de tempo para cada salto na jornada do pacote. Selecione a **seta Avançar** para continuar.

14. Agora você fechará a janela do prompt de comando e retornará à área de trabalho. Selecione o botão **Fechar**.

Tarefa 2: Varrer uma rede com o Zenmap

15. Outra ferramenta de varredura de rede é o Nmap, um programa de linha de comando. Nesta simulação, você usará o Zenmap, a GUI oficial do Nmap. Selecione **Nmap – Zenmap GUI (Nmap – GUI do Zenmap)**.

16. Será exibida a janela do Zenmap. Para realizar uma verificação, primeiro, você deve informar o endereço da web do host de destino. Digite `scanme.nmap.org` no campo **Target (Alvo)** e pressione **Enter**.

17. Ao longo desta simulação, observe como o texto no campo **Command (Comando)** é atualizado à medida que você altera os campos **Target (Alvo)** e **Profile (Perfil)**. O texto do campo **Command (Comando)** é o comando que você executaria se executasse a varredura na ferramenta de linha de comando do Nmap. Selecione a **seta Avançar** para continuar.

18. O mapa de dados pode realizar varreduras que variam de acordo com o número de portas verificadas e outras informações coletadas. Quanto mais profunda a varredura, mais tempo a varredura demora. No primeiro teste, você escolherá uma varredura rápida. Selecione a seta para a lista **Profile (Perfil)**. Em seguida, selecione **Quick Scan (Varredura rápida)**.

19. Selecione **Scan (Verificar)** para começar a verificação.

20. Veja a saída da verificação no painel Nmap Output (Saída do Nmap) no painel do Zenmap. Quando terminar de visualizar a saída, selecione a **seta Avançar** para continuar.

21. Observe que a saída lista as portas *interessantes* do host de destino. As portas interessantes são portas abertas, as mais suscetíveis a ataques e portas em um estado incomum para esse sistema. Selecione a **seta Avançar** para continuar.

22. Agora vamos fazer uma varredura mais lenta, mas abrangente. Selecione a seta para a lista **Profile (Perfil)**. Em seguida, selecione **Intense Scan (Varredura intensa)**.

23. Selecione **Scan (Verificar)**.

24. Visualize a saída no painel Nmap Output (Saída do Nmap). Observe que contém detalhes como o sistema operacional do host e a versão do kernel, bem como os resultados do traceroute. Role até o fim para ver toda a saída. Quando terminar de visualizar a saída, selecione a **seta Avançar** para continuar.

25. Os outros blocos do painel destacam partes dessa saída. Selecione a guia **Ports/Hosts (Portas/Hosts)** para ver todas as portas interessantes do sistema de destino.

26. No painel Ports/Hosts (Portas/Hosts), um círculo verde indica uma porta aberta. Um círculo vermelho indica que a porta está fechada ou que o Zenmap não pode determinar o estado da porta. Observe que esse painel também lista o número da versão de qualquer aplicativo correspondente à porta. Selecione a **seta Avançar** para continuar.
27. Selecione a guia **Topology (Topologia)** para visualizar um mapa interativo de hosts em uma rede.
28. O painel Topology (Topologia) mostra o caminho de rede do seu computador para o host de destino e inclui cada host encontrado ao longo do caminho. Selecione a **seta Avançar** para continuar.
29. A cor de um host indica o número de portas abertas: verde significa menos de 3, amarelo significa de 3 a 6 e vermelho significa mais de 6. Branco significa que o Zenmap não digitalizou o host, portanto o número de portas abertas do host é desconhecido. Selecione a **seta Avançar** para continuar.
30. Selecione a guia **Host Details (Detalhes do host)** para visualizar um detalhamento organizado de detalhes sobre o host de destino.
31. O painel Host Details (Detalhes do host) contém detalhes como o status do host de destino, endereços, nomes de host e sistema operacional. Role até o fim para visualizar toda a saída. Ao terminar de visualizar a saída, selecione a **seta Avançar** para continuar.
32. Observe que o ícone na linha “Last boot” (Última inicialização) indica a vulnerabilidade estimada com base no número de portas abertas. O baú do tesouro mostrado aqui significa 3 a 4 portas abertas. Selecione a **seta Avançar** para continuar.

Conclusão

Você executou com êxito o reconhecimento de rede para coletar informações sobre uma rede de computadores. Você fez isso com várias ferramentas de linha de comando e o Zenmap.