Universidade Comunitária da Região de Chapecó

Curso: Ciência da Computação

Disciplina: Tópicos em Redes de Computadores

Professor: Lucas Antunes da Rocha Volfe

TRABALHO FINAL - EXPLORAÇÃO DE MÁQUINA NO TRYHACKME

Acadêmicos: Gustavo Bones, Mariana Wagner, Naieli Loeblein e Pedro Knebel

Chapecó, 14 de dezembro de 2025

PASSOS PARA RESOLUÇÃO DA BOX:

1º - Configuração do ambiente:

Para a configuração do ambiente do TryHackMe, é necessário iniciar a VPN com o arquivo de configuração adquirido diretamente na plataforma. Utilizando o comando *sudo openvpn <caminho para o arquivo .ovpn>*, iniciamos a VPN e, posteriormente, a máquina do desafio.

2º - Exploração e reconhecimento do ambiente:

Primeiramente, para encontrarmos a primeira resposta, utilizamos o comando *nmap* para mapear todas as portas abertas no IP da máquina, por meio do comando *nmap -sV <ip da máquina>*. A flag *-sV* foi utilizada para descobrir o serviço em execução em cada porta e sua respectiva versão, respondendo assim às três primeiras perguntas.

Após isso, para encontrarmos os diretórios ocultos no IP da máquina, utilizamos o Gobuster, que realiza um de força bruta para descobrir diretórios com base em uma lista de palavras contida em um arquivo .txt. Foi utilizado o comando *gobuster dir -u http://<ip da máquina>/ -w <caminho para a lista de palavras>*. A lista de palavras foi obtida no repositório https://github.com/danielmiessler/SecLists.git. Após a execução do Gobuster, alguns diretórios foram descobertos.

3º - Aplicando o Reverse Shell:

Para aplicar o shell reverso, encontramos um repositório no GitHub que possui um exemplo de arquivo para shell reverso em .php. O PHP foi escolhido pois é compatível com servidores Apache. O repositório utilizado foi: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php.

Após isso, alteramos o IP presente no script para o IP da máquina do TryHackMe e tentamos realizar o upload do arquivo. No entanto, o diretório */panel* bloqueava a importação de arquivos .php. Para contornar esse problema, alteramos a extensão do arquivo para .php5, o que possibilitou o upload. Para confirmar que a importação ocorreu com sucesso, retornamos ao diretório */upload,* onde foi possível verificar que o script havia sido executado.

Para obter acesso ao shell, utilizamos o Netcat, que é um listener de rede usado para ler e escrever dados por meio de conexões TCP e UDP, executando o comando *nc -lvpn 1234*. Em seguida, executamos o arquivo .php5 que foi importado na máquina virtual. Após isso, já estávamos dentro da máquina, o que pôde ser confirmado com o comando *whoami*. Para

encontrar a resposta desta etapa, executamos o comando find para localizar o arquivo user.txt e obter a chave correta. O comando completo utilizado foi *find / -name user.txt.*

4º - Escalando privilégio:

Para realizar o escalonamento de privilégios, utilizamos novamente o comando find, porém desta vez com as flags *-user root*, para localizar arquivos pertencentes ao usuário root, *-perm /4000*, para identificar arquivos que possuem o bit SUID ativado (ou seja, são executados com privilégios de root), e *2>/dev/null*, que evita a exibição de mensagens de erro relacionadas à falta de permissão de acesso. O comando completo utilizado foi find / -user root -perm /4000 2>/dev/null.

Após analisar o retorno do comando, identificamos a existência de um arquivo Python, que respondeu à primeira pergunta dessa etapa, pois poderia ser utilizado para o escalonamento de privilégios.

Em seguida, acessamos o site https://gtfobins.github.io/gtfobins/python/#suid, onde encontramos um comando que permite a execução de um shell com privilégios de root. O comando utilizado foi *usr/bin/./python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'*. Dessa forma, seguindo as orientações do site, foi possível abrir um shell com privilégios de administrador.

Confirmamos o acesso com o comando whoami, que retornou root, e ao executar o comando ls, localizamos o arquivo root.txt, que continha a última chave necessária para concluir a sala.