**26/03/2024 - VULNVERSITY**

<https://tryhackme.com/r/room/vulnversity>

1. Varredura com Nmap
   1. sV – determinar a versão dos serviços que estão rodando
   2. -p- – todas as portas
   3. -p-X – portas até X valor
   4. -A – descobrir versão do sistema operacional
   5. -v – habilita modo verboso do nmap

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Escaneamento com Gobuster
   1. -u – url do alvo
   2. -w – path da wordlist
   3. -U e -P – usuário e senha para auth
   4. -e – url completa

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Visualização no navegador
   1. acesso ao ip + path

Interface gráfica do usuário, Site

Descrição gerada automaticamente

1. Ataque sniper utilizando Intrudter do Burp Suite
   1. configuração do file name $.php$ para apresentar variações do php
   2. payloads com wordlist de php
   3. teste de qual extensão poderia fazer upload

Tabela

Descrição gerada automaticamente com confiança média

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Upload de um PHP reverse shell
   1. reverse shell obriga fazer conexão com quem enviou
   2. adicionar ip próprio
   3. <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>
   4. executar via url
   5. flag do usuário bill

Texto

Descrição gerada automaticamente

1. Escalar privilégios
   1. SUID – arquivos com permissões dependendo do privilégio
   2. find / -perm -4000 2>/dev/null – acha APENAS arquivos com SUID
   3. documentação de arquivos SUID GTFOBins para privilege escalation
   4. /bin/systemtcl – exploit para escalar privilégio
   5. transformação em root com reverse shell também é possível

Texto

Descrição gerada automaticamente