Hackthebox and Vulnhub – Dicas e Truques

Joas Antonio

Detalhes

- Fiz esse PDF para passar algumas dicas e truques e auxiliar aqueles que estão iniciando suas jornadas no mundo de CTF e esta por dentro das plataformas Vulnhub e Hackthebox;
- Não é um guia que vai te tornar um Pro Player, mas pode te ajudar a iniciar e avançar dentro dessas plataformas;

Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

Conhecimentos fundamentais

- Antes de iniciar sua jornada nessas plataformas, eu recomendo que você tenha conhecimentos fundamentais em:
- Noções de Redes de Computadores (Protocolos e Serviços, Modelo TCP/IP, Modelo OSI, Utilitários básicos de rede como por exemplo o netcat, conhecimentos de requisições web);
- Conhecimentos em sistemas operacionais Linux e Windows (Powershell, Shell Script, linhas de comandos);
- Conhecimentos em Lógica de programação e Linguagem de Programação (Python é uma das linguagens bastante usadas dentro dos CTFs, além da linguagem C);
- Conhecimentos em testes de invasão, vulnerabilidades e vetores de ataques (Essencial conhecer dos vetores de ataque em cada tipo de plataforma, seja uma infraestrutura de redes ou uma aplicação web e entender as vulnerabilidades para aprimorar cada vez mais suas habilidades e aumentar o impacto de um vetor);

Dicas e Truques: Organização e Metodologia

- Primeiramente a organização é fundamental, eu recomendo criar pastas, documentos e links de pesquisas para cada máquina que está tentando comprometer, além dos passo a passo que você utilizou para compromete-la;
- Tenha uma metodologia de PenTest bem estruturada, desde a coleta de informação até a pós exploração e apagar os seus rastros;
- Complementando a dica de cima, eu recomendo que você monte um arsenal de ferramentas que você utiliza frequentemente e estruture conforme o processo de PenTest que você vai realizando;
- Sempre certifique-se de levantar informações suficientes do seu alvo, mesmo que uma informação possa parecer irrelevante, muita das vezes em um processo futuro, ela acaba se tornando útil, como já presenciei. Lembre-se que nada é irrelevante, conforme você vai atingindo um nível de habilidade, Hackear se torna algo mágico;

Dicas e Truques: Desafios

- Qual área você tem mais habilidade? Ataques Web, Infraestrutura, Desenvolvimento de Exploits? É uma pergunta besta, mas com certeza tem pessoas que curtem desafios que envolvem desenvolver seu próprio vetor de ataque, comprometer uma aplicação web ou atacar uma infraestrutura;
- Eu recomendo que ao escolher uma máquina, veja se ela é desafiadora, pois a graça é quebrar os seus limites e fazer você pensar fora da caixa, por isso, escolha máquinas que mesclem diversos vetores de ataques, seja seu foco aplicação web, uma infraestrutura, desenvolver um exploit, sistemas industriais e por ai vai;

Dicas e Truques: Em busca da Flag #WEB

Agora vem a parte que todo mundo gosta!

- Quando falamos de aplicações web, obviamente que uma das etapas a ser feita é analisar o servidor de aplicação, rodando um portscanner e fazendo um banner grapping para entender qual versão esta sendo rodando no servidor web, qual sistema operacional e outros detalhes, versão de PHP, Plugins e Frameworks;
- Enumerar diretórios do website, procurar principalmente diretórios ocultos e filtrar sua busca para encontrar páginas HTML, PHP, XML e etc, que estejam escondidas;
- Além disso, procurar páginas de Administração, verificar se a aplicação é um CMS (Wordpress, Joomla, Drupal e etc);
- Testar campos de entradas de dados, páginas de login e outros locais que podem ser utilizados como vetor de ataque, como arquivos de configuração;

Lembre-se: Enumerar é essencial!

Dicas e Truques: Em busca da Flag #Infra ou System Hacking

- Em infraestrutura, vou incluir as box de System Hacking, pois o conceito é o mesmo;
- Portscanner e Enumeração de serviço é fundamental, assim você verifica se tem uma versão vulnerável ou até mesmo um serviço mal configurado;
- Procurar vulnerabilidades que afetam um determinado serviço ou recurso do sistema, tentar técnicas de brute force para quebrar um SSH ou até mesmo conseguir transferir arquivos para o alvo;
- As caixas do HTB já possuem uma vulnerabilidade, se for necessário desenvolver um exploit, não tenha medo de pesquisar e perguntar, além disso é essencial que você enumere bastante e seja uma pessoa analítica;
- Metasploit ele é seu canivete suíço, mas entenda como a exploração funciona e quem sabe você não encontre alternativas criativas ou até mesmo desenvolve seu próprio exploit;

Lembre-se: Enumerar é essencial!

Dicas e Truques: Escalação de privilégios

- Após obter a sua shell, obviamente a escalação de privilégios é necessária para obter controle total do alvo, para isso algumas informações são cruciais;
- Informações do usuário e seus grupos, quais os usuários se encontram na maquina, quais pertencem ao grupo administrativo, qual é a versão do kernel do sistema operacional e o sistema do alvo, além disso, os processos que estão executando no servidor;
- Se o seu alvo for um Linux, com certeza procurar executáveis SUID é uma das formas para escalar privilégios;
- Abusar de elevação de privilégios como o SUDO ou o UAC do Windows, pode ser uma alternativa, além de verificar quais aplicações executam como Admin e procurar exploits locais para o mesmo;
- Utilizar scripts de enumeração local tanto para Linux como para Windows é fundamental;
- Testar as credenciais que você descobriu em mais de um usuário na máquina;
- Quais arquivos você pode ler, escrever ou até mesmo modificar;
- E procurar por exploits que exploram a nível Kernel para conseguir elevar seus privilégios;
- Procurar técnicas para escalar privilégios por meio de uma aplicação, como exemplo temos o tradicional LXC que nos possibilita escalar privilégios, assim é possível também com Docker e até mesmo outros binários;

Dicas e Truques: Escalação de privilégios

- Procurar processos executando em background ou que estão configurados para executar certo horário;
- Verificar se existem mais de uma interface de rede e outras placas de redes conectadas em uma outra rede;
- Analisar as configurações de Rede e serviços de redes;
- Tentar redirecionar o trafego de uma porta ou até mesmo interagir;
- Tentar enumerar arquivos confidenciais ou de configurações e tentar abri-los;
- Puxar o histórico de comandos que o usuário rodou e outros eventos que ele fez;
- Existem outras partições dentro da máquina, algum sistema de arquivo montado e etc;
- Utilizar os binários que você consegue executar para te auxiliar na escalação de privilégios, por exemplo, se você consegue executar o GCC, faça o upload do exploit local feito em C e execute o GCC para compilar e executa-lo depois;

Essas são algumas dicas, mas como sempre, enumerar e vasculhar cada ponto do sistema operacional é crucial, eu recomendo que você aprenda Shell Script, PowerShell, Linha de comando para deixar sua exploração mais performática.

Dicas e Truques: Helps #PrivEsc

- https://github.com/frizb/Linux-Privilege-Escalation
- https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
- https://gtfobins.github.io/
- https://lolbas-project.github.io/
- https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite
- My ebooks: https://bit.ly/3rQNjKa (Aqui conta com mais referencias e guias de pesquisas)
- https://payatu.com/guide-linux-privilege-escalation
- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://github.com/rebootuser/LinEnum
- https://www.secjuice.com/tryhackme-common-linux-privilege-escalation/

Fontes de Pesquisas

- https://ippsec.rocks/?#
- https://www.youtube.com/channel/UCNSdU_1ehXtGclimTVckHmQ
- https://www.youtube.com/c/JohnHammond010
- https://www.youtube.com/user/GynvaelEN
- https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA
- https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w
- https://www.youtube.com/channel/UCCZDt7MuC3Hzs6IH4xODLBw
- https://www.youtube.com/channel/UCQN2DsjnYH60SFBIA6IkNwg
- https://www.youtube.com/channel/UChjC1q6Ami7W0E71TzPZELA
- https://medium.com/ctf-writeups
- https://github.com/enaqx/awesome-pentest
- https://github.com/apsdehal/awesome-ctf

Fontes de Pesquisas

- https://github.com/paralax/Awesome-Pentest-1
- https://github.com/x0x8x/awesome-pentester
- https://github.com/CyberSecurityUP/Awesome-PenTest-Practice
- https://github.com/0x4D31/awesome-oscp
- https://github.com.cnpmjs.org/topics/oscp-prep
- https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/
- https://github.com/burntmybagel/OSCP-Prep
- https://cybersecurity.att.com/blogs/security-essentials/how-to-prepare-to-take-the-oscp
- https://medium.com/@galolbardes/passing-the-oscp-while-working-full-time-29cb22d622e0
- https://medium.com/@gavinloughridge/a-beginners-guide-to-vulnhub-part-1-52b06466635d
- https://www.youtube.com/channel/UCXPdZsu8g1nKerd-o5A75vA

Dicas da comunidade

- https://medium.com/bug-bounty-hunting/beginner-tips-to-own-boxes-at-hackthebox-9ae3fec92a96
- https://forum.hackthebox.eu/discussion/1649/one-month-of-htb-impressions-and-tips-from-a-noob
- https://forum.hackthebox.eu/discussion/155/guide-for-noobs
- https://www.reddit.com/r/hackthebox/comments/fyco8v/hack_the_box_guide/
- https://0x00sec.org/t/my-hackthebox-ctf-methodology-from-fresh-box-to-root/13980
- https://blog.nviso.eu/2020/02/13/my-journey-reaching-1-spot-on-hack-the-box-belgium-10-tips-tricks-and-lessons-learned/
- https://forum.hackthebox.eu/discussions/tagged/tips/p1

Dicas da comunidade

- https://technicalnavigator.in/tips-tricks-for-htbhack-the-box/
- https://www.reddit.com/r/oscp/comments/g47xso/windows_privilege_escalation_guide/
- https://www.youtube.com/results?search_query=privilege+escalation

CONCLUSÃO

- Esse foi um guia básico para quem está começando no hackthebox, Vulnhub ou qualquer outro CTF, espero que seja útil e te ajude de alguma forma;
- Caso queira mais conteúdos e artigos referente a Red Team e um pouco de Blue Team, acesse meu LinkedIn que lá conto com quase 200 artigos;
- Meu LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/
- Além disso, eu possuo diversos ebooks e documentos como esse, principalmente sobre pentest, caso queira dar uma olhada, segue o link: https://bit.ly/3rQNjKa
- Agradeço imensamente você que leu até aqui e curte meu trabalho, fique a vontade em me contatar ;)