APOSTILA: DICAS BÁSICAS PARA PENTESTERS

PROF. JOAS ANTONIO

DICA #1

- Para ser um bom PenTester não adianta decorar todos os comandos do NMAP, METASPLOIT, SQLMAP, SETOOLKIT e etc...
- Para ser um bom PenTester você precisa adquirir conhecimentos fundamentais em redes de computadores, arquitetura de sistemas, noções de sistemas operacionais, base computacional, arquitetura de redes, desenvolvimento web, programação de alto e baixo nível e principalmente de novas tecnologias que vem surgindo a cada dia.
- Adquirir fundamentos é essencial para você compreender a funcionalidade do Nmap e como você pode trabalhar em diferentes tipos de ambientes.

DICA #2

- Estude Metodologias de PenTest, lembre-se que pentest não só se resume em ligar seu notebook, ter acesso a rede e ir ganhando shell em cada máquina existente no ambiente.
- Fazer PenTest é ter planejamento e organização, para isso você precisa utilizar metodologias para distribuir as tarefas e fazer um pentest mais preciso.
- Conheça as metodologias:

1. Open-Source Security Testing Metodology Manual (OSSTM)
2. Penetration Testing Execution Standard (PTES)
3. Open Web Application Security Project (OWASP)
4. National Institute of Standards and Technology – 800-15 (NIST)

DICA #3

- Aprenda diferente tipos de métodos de ataque, evitando a famosa receita de bolo
- Eu recomendo acessar sites de noticias relacionado a segurança da informação para aprender novos métodos de ataques
- Além disso é bom sempre estar praticando toda vez que encontrar um novo método de ataque

DICA #4

- Não se baseie em outras pessoas, estude pelo que você necessita e não por moda, evite estudar algo porque está na moda hoje em dia
- Estude novas tecnologias, até mesmo tecnologias que ninguém tira tempo para aprender

DICA #5

- Saiba trabalhar em diferentes tipos de ambientes de risco, seja em sistemas mais básicos até sistemas críticos
- É elevando seus níveis sendo, Windows a Scada (Sistemas operacionais)
- Usando essa analogia do Windows como (Usuário)
- E o sistema Scada como (Usinas)
- Ou seja, foco em ambientes de grande risco

DICA #6

- Jogue CTFs de vez em quando para fortalecer seu conhecimento
- Monte laboratórios ou baixe máquinas virtuais do site “vulnhub.com” e tente comprometer pelo menos 1 por dia
- Além disso, aprenda novas tecnologias para exploração, seja uma nova falha, um novo método para escalar privilégios e etc...

DICA #7

- Crie um cronograma de estudos mesmo que seja complicado hoje em dia, mas essa área requer dedicação diária, afinal a cada dia surge um novo conceito que pode revolucionar até mesmo a forma de exploração de uma falha, seja com um exploit 0-day ou uma ferramenta mais avançada ou um método melhor.
- Entrou na área de segurança não adianta, você precisa estudar pelo menos 2 horinhas por dia.

DICA #8

- Para se tornar um jedi em segurança da informação é necessário conhecimento não só em PenTest como em outras áreas
- A famosa frase: “Se sabe atacar, saberá defender”
- Então estude outros segmentos que a área de segurança tem proporcionado, pois isso ajuda demais a trabalhar melhor na realização de um PenTest, quando se deparar com alguma politica de segurança, dispositivos de segurança ou endpoints de segurança e afins

DICA #9

- Evite os famosos cursos de Hackers, que promete tornar você um PenTester em 3 dias ou que promete colocar você no mercado
- Pois imagine a lógica, você não tem conhecimentos de segurança da informação, não tem fundamentos de tecnologia e já sair auditando ambientes corporativos sem ao menos saber como funciona um sistema Linux ou como trabalha determinado serviço

DICA #10

- Aprenda a explorar falhas manualmente, como SQL Injection, RCE, XSS e até falhas em redes e sistemas por desenvolver exploits e scripts que difere da exploração convencional

DICA #11

- Acompanhe palestras e canais de pessoas que trabalham na área de segurança
- É essencial para o seu desenvolvimento profissional ir adquirindo novos conhecimentos conforme o tempo passa

DICA #12

- Não desista!
- Foque em se tornar alguém que atraia o mercado de trabalho com suas habilidades
- Se for tirar certificações como CEH, OSCP, OSCE, GPEN, ECSA e etc...
- Lembre-se! Certificação não diz que você sabe, mas que você conhece, então foque em saber PenTest e não somente conhecer.

INDICAÇÕES

- https://esecurity.com.br
- https://desecsecurity.com
- https://comohackear.com.br/
- http://expersec.com/
- https://www.facebook.com/cybersecup
- https://hackaflag.com/
- https://www.youtube.com/user/ricardolongatto
- https://www.youtube.com/user/daybsonbruno
- https://www.youtube.com/channel/UCuQ8zW9VmVyml7KytSqJDzg
- https://www.youtube.com/channel/UCxHzA-Z97sjfK3OISjkbMCQ
- https://www.youtube.com/channel/UC7oYG2WHVxlOJRng4v-CIFQ
- https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w

INDICAÇÕES

- https://www.vulnhub.com/
- https://shellterlabs.com/pt/account/login/
- https://www.hackthebox.eu/
- https://hackersec.com/
- https://ctftime.org/
- https://acaditi.com.br
- https://udemy.com