Checklist: Do Diploma ao Primeiro Job como Pentester Subtítulo: Guia Prático de Estudos e Carreira

Introdução

Parabéns pela sua graduação! Agora, o próximo passo é conquistar seu primeiro emprego como *Pentester*. Este guia prático oferece um checklist detalhado e um roteiro para te ajudar a trilhar esse caminho com sucesso.

Este ebook cobre os principais pilares para você estar preparado para o mercado de trabalho, desde a base técnica até as habilidades comportamentais e éticas.

1. Sólida Base Técnica

Para se destacar como Pentester, é fundamental construir uma base técnica sólida. Os pilares principais incluem:

- **Redes de Computadores:** Compreenda os protocolos TCP/IP, modelo OSI, sub-redes, roteamento e firewalls.
- **Linux:** Domine a linha de comando, administração de sistemas, scripting (Bash) e segurança.

- **Segurança Web:** Entenda as vulnerabilidades OWASP Top 10, como injeção SQL, XSS e CSRF. Conheça a fundo o funcionamento das aplicações web, desde o front-end até o back-end.

2. Onde Praticar

A teoria é importante, mas a prática é essencial. Explore as seguintes plataformas para aprimorar suas habilidades:

- **TryHackMe:** Plataforma com diversos caminhos de aprendizado e máquinas virtuais com vulnerabilidades para explorar.
- **Hack The Box:** Similar ao TryHackMe, com foco em desafios mais avançados e CTFs.
- **PortSwigger Academy:** Focado em segurança web, com laboratórios práticos para explorar as vulnerabilidades OWASP Top 10.

3. Ferramentas Indispensáveis

Familiarize-se com as seguintes ferramentas:

- **Nmap:** Scanner de portas e descoberta de serviços.
- **Subfinder/Amass:** Ferramentas para enumeração de subdomínios.
- **Burp Suite:** Proxy para interceptar e manipular o tráfego web. Essencial para testar aplicações web.
- **Metasploit:** Framework para exploração de vulnerabilidades.
- **SQLmap:** Ferramenta para automatizar a exploração de vulnerabilidades de injeção SQL.
- **Netcat (nc):** Canivete suíço para conexões TCP/UDP. Útil para transferir arquivos, criar shells reversos, etc.

4. Certificações de Entrada

Certificações podem te ajudar a se destacar no mercado de trabalho. Considere as seguintes:

- **eJPT (eLearnSecurity Junior Penetration Tester):** Certificação introdutória de penetration testing.
- **CompTIA Security+:** Certificação que cobre os fundamentos de segurança da informação.
- **BTL1 (Blue Team Level 1):** Certificação que foca na defesa cibernética e análise de logs.

5. Soft Skills e Ética

Além das habilidades técnicas, as soft skills são cruciais:

- **Escrita de Relatórios:** Seja claro, conciso e objetivo ao comunicar suas descobertas. Um bom relatório é essencial para o sucesso de um Pentest.
- **Mindset Ético:** Entenda e siga os princípios éticos do penetration testing. Obtenha permissão antes de testar qualquer sistema. Atue sempre de forma responsável e legal.

Checklist Detalhado

Este checklist consolida os pontos-chave abordados neste guia. Use-o como um guia para acompanhar seu progresso e garantir que você está no caminho certo para conquistar seu primeiro emprego como Pentester.

[ ] Dominar os fundamentos de redes (TCP/IP, OSI, Sub-redes, Roteamento, Firewalls)

[ ] Familiarizar-se com a linha de comando do Linux e administração de sistemas

[ ] Entender a fundo a segurança web e as vulnerabilidades OWASP Top 10

[ ] Praticar em plataformas como TryHackMe, Hack The Box e PortSwigger Academy

[ ] Dominar ferramentas como Nmap, Subfinder/Amass, Burp Suite, Metasploit, SQLmap e Netcat

[ ] Obter uma certificação de entrada (eJPT, CompTIA Security+, BTL1)

[ ] Aprimorar suas habilidades de escrita de relatórios

[ ] Desenvolver um mindset ético e responsável

Próximos Passos

Agora que você possui este guia, o próximo passo é colocar em prática o que aprendeu. Comece explorando as plataformas de prática, aprofunde seus conhecimentos nas ferramentas e considere obter uma certificação. Com dedicação e persistência, você estará pronto para conquistar seu primeiro emprego como Pentester!