BLUE TEAM POR ONDE COMEÇAR A ESTUDAR?

COMO HACKEAR?

Você já ouviu falar do Blue Team?

Blue team é um time designado na área de segurança da informação com cujo objetivo é identificar, mitigar e analisar o sistema a procura de qualquer tipo de vulnerabilidade e implementar medidas eficazes de segurança.

Enfim, mas por onde começar a estudar?

Como o blue team se resume a proteger o ambiente e tomar medidas caso algum incidente ocorra, a melhor coisa a se fazer é conhecer os métodos existentes para proteger o seu ambiente.

Veja alguns métodos:

1. Analise de vulnerabilidades, mesmo sendo algo do Red team que foca mais no ofensivo, o blue team também pode identificar as vulnerabilidades por intermédio de softwares de gestão de vulnerabilidades ou até mesmo em conjunto com Red team.
2. Realizar a atualização dos sistemas de segurança da empresa, seja o Firewall, IDS, IPS, HIDS, NIDS e entre outros.
3. Manter os ativos atualizados, implementar patches e procurar por vulnerabilidades novas em sites como Security Focus, 0DAY TODAY, The Hacker News, Mundo Hacker, Experience Security e Cyber Security UP.
4. Montar uma rotina de Backup para evitar qualquer incidente que pode ocorrer.
5. Técnicas de mitigação de risco são essenciais, afinal usar boas regras de firewall, configurar um serviço como SSH/FTP/SMTP com foco em segurança, é essencial para a proteção do seu sistema mesmo eu ter dito isso nos tópicos acima, mas vale a pena focar nisso.

Mas por onde eu começo a estudar o Blue team?

Realmente é fácil você estudar a área de segurança ofensiva, pois além de diversos laboratórios, os sites encontrados na internet se tornam um alvo comum para os estudantes de Red team.

Agora estudar blue team, como faz?

Vamos lá!

1. Necessário ter conhecimentos em Linux, afinal muitas empresas usam servidores linux para gerenciar sua rede e seus arquivos, porém o Windows Server também está nesse impasse, então conhecer os dois é essencial para defender;
2. Conhecer os fundamentos de Firewall é essencial para você poder manusear qualquer outro, seja nativo ou de terceiros;
3. Aprender métodos de criptografia, cifragem ou encoders é um passo a mais para proteger usuários e senhas, seu servidor web e armazenamento de informações;
4. Saber montar uma VPN, um servidor Proxy é ótimo tanto para montar ambientes dentro dessa VPN para efetuar testes como para saber proteger um ambiente descentralizado;
5. Montar servidores DNS, SMTP, FTP, SAMBA, etc, vai ajudar a compreender o funcionamento desses serviços e como proteger tais ambientes;
6. Ter conhecimentos em IDS, IPS, HIDS, NIDS, HONEYPOT, HONEYNET é um dos melhores métodos para implementar a segurança em seu ambiente;
7. Conhecer desenvolvimento seguro, métodos para mitigar alguma vulnerabilidade no seu código vai ajudar a prevenir muitas ameaças;
8. Consulte materiais de mitigação em servidores linux, em serviços ou em redes;
9. Realizar Troubleshooting em pequenos erros já é um bom passo, então sempre que achar um erro anote e anote a solução também;
10. E tenha foco apenas em um tipo de ambiente primeiro, e depois vá se expandindo;
11. Use software de gestão de vulnerabilidades para ver se o seu ambiente tem vulnerabilidades;
12. Monte ambientes desatualizados e vá implementando patches;
13. Procure métodos de backup para você também brincar;
14. Simule um ataque em seu ambiente;
15. Use softwares de monitoramentos, os endpoints free que existem por aí.

Essas são algumas dicas para estudar sobre Blue Team, óbvio que as coisas são mais profundas, mas por enquanto essa é a base que eu posso dar,

porém existe palestras no YouTube que explicam mais profundamente sobre isso.

Caso tenha mais dúvidas, estou convidando vocês a ler aos meus artigos e fique de olho nas páginas: https://www.linkedin.com/in/joas-antonio-dos-santos/

Parceria: Como Hackear, Cyber Security UP, Experience Security e 4Hackers

https://www.facebook.com/cybersecup

https://www.facebook.com/como.hackear.curso/

https://www.facebook.com/Expersec/

https://www.facebook.com/ForHackers/