Segurança no Desenvolvimento de Aplicações
Fatec Araras
Prof. Jonas Bodê

1. O que é Ethical Hacking e qual a sua importância no mercado de segurança? Justifique a sua resposta.

   Ethical Hacking é um processo pelo qual um hacker ético trabalha para encontrar vulnerabilidades em um sistema ou ambiente, realizando diversos testes que vão desde a identificação de falhas já conhecidas até a testes de penetração, onde o hacker ético atua de forma similar a um hacker malicioso, na intenção de descobrir novas vulnerabilidades não conhecidas, com essas praticas do Ethical Hacking sendo cruciais para o mercado de segurança pois garantem que as empresas que as implementem tenham uma maior segurança digital e conheçam melhor seus pontos e fracos.

2. Qual a diferença entre Red Team, Blue Team e Purple Team? Qual dessas funções estão mais exigidas? Justifique a sua resposta.

   Esses times diferenciam-se pelas suas especialidades no campo do Etjhical Hacking, com o Red Team atuando como os atacantes em testes de penetração e de vulnerabilidade, já o Blue Team atua como os defensores da aplicação, defendendo-a de ataques reais e de ataques “simulados” de membros do Red Team, em meio a ambos os times temos o Purple Team, que atua como um “fullstack” da segurança, abrangendo tanto os testes de ataque quanto os de defesa, sendo por isso os mais procurados do mercado.

3. Qual a importância de um Pentest no desenvolvimento e empresas no mercado atual? Justifique a sua reposta.

   O pentest é de grande importância por permitir que a empresa contratante identifique vulnerabilidades de sua própria infraestrutura, o que permite que a mesma possa direcionar recursos para a correção dessas brechas e falhas de segurança, com grandes empresas de

tecnologia e de segurança ofertando o pentest em seu catálogo, entre elas: Palo Alto Networks, Oi Soluções e Kaspersky.

4. A coleta de informações é uma etapa importante na área de segurança? Justifique a sua resposta.
   Sim, a coleta de informações é uma etapa crucial dos processos da área de segurança digital, pois é nessa fase dos testes de vulnerabilidade em que podemos identificar detalhes expostos publicamente que possam ser utilizados como brechas, como por exemplo os dados pessoais dos clientes ou funcionários de uma organização e os possíveis pontos fracos de sua infraestrutura.

5. Atualmente, como podemos classificar o Bug Bounty no Brasil? Justifique a sua resposta.
   Atualmente o Bug Bounty se encontra em fase de adoção no Brasil, com muitas empresas ainda desconfiando da prática não a incentivando e não oferecendo grandes “recompensas” pelos BUGs encontrados, o que se diferencia do cenário internacional em que grandes empresas como Google, Facebook e Amazon incentivam e fazem um grande uso a prática, porém mesmo em fase de adoção e com o pouco incentivo dos grandes players nacionais a prática já tem o envolvimento de mais de 1500 testers, que juntos já encontraram mais de 250 vulnerabilidades.

6. O que são ataques DDoS? Justifique a sua resposta.
   Os ataques DdoS atuam de forma semelhante aos ataques DoS, ou seja, eles fazem com que os sistemas e plataformas alvos se tornem incapazes de responder a novas requisições e executar suas tarefas, fazendo isso a partir do envio massivo de requisições e dados que sobrecarregam o servidor ou ambiente alvo, com essas requisições vindo de dezenas ou mesmo milhares de computadores, dos quais muitos desses são “zumbis”.

7. No desenvolvimento, qual a importância da segurança? Justifique a sua resposta.

A segurança é muito importante para o desenvolvimento de software pois é durante esse processo que muitas brechas de segurança conhecidas podem ser evitadas e em que muitos mecanismos de defesa são implementados.