PenTest Web – Testes de Intrusão

I. APRESENTAÇÃO:

O treinamento **"PenTest Web – Testes de Intrusão"** tem por objetivo preparar profissionais e organizações para a proteção de suas aplicações web contra as principais ameaças web, a partir dos resultados da aplicação de técnicas de *Pentest web*. As aplicações web desempenham um papel vital em todas as organizações modernas, sendo uma aliada essencial para os negócios. Contudo, se a organização não estiver protegida adequadamente, seus aplicativos web podem se tornar alvos de ataques que podem comprometer as informações e os processos de negócios da empresa. Muitas organizações trabalham com a impressão equivocada de que uma varredura automatizada por vulnerabilidades irá revelar todas falhas de segurança em seus sistemas. Este treinamento irá demonstrar as técnicas mais usadas por especialistas em segurança da informação em testes de intrusão em aplicações web nos cenários mais comuns de vulnerabilidades reportados pela OWASP (*Open Security Application Project*), de forma a permitir uma melhor avaliação e tratativa de proteção. O Estratégia Treinamentos adota metodologia direcionada para a prática, com aplicação de estudos de caso, práticas de laboratório e trabalho em equipe. Ao final do treinamento o aluno estará em condições de compreender as principais técnicas de *pentest web* e aplicá-las em ambiente corporativo, avaliando a resiliência de suas aplicações web, identificando as suas vulnerabilidades e tomando as ações necessárias para a sua adequada proteção.

II. PÚBLICO ALVO:

Analistas de segurança da informação, Administradores de Redes e Sistemas, administradores de aplicações Web, estudantes da área de tecnologia da informação.

III. CARGA HORÁRIA: 40 horas.

IV. BENEFÍCIOS DO TREINAMENTO:

- Permitir ao aluno avaliar a resiliência e eficácia dos mecanismos de segurança propostos pelos administradores de sistemas e desenvolvedores de sistemas web.
- Proporcionar ações além da adoção de scanners de vulnerabilidade web, que automatizam os processos e condicionam analistas de segurança da informação à avaliações limitadas durante os processos de testes de invasão.
- Capacitar analistas a demonstrar e argumentar de maneira convincente os impactos de se trabalhar com mecanismos de segurança inadequados, que se tornaram um grande risco na maioria das organizações.
- Incentivar a prática de uma abordagem com ética sobre processos de testes de invasão como desafio profissional de um White Hat tradicional.
- Proporcionar uma visão completamente prática sobre invasão de computadores e apropriação de informações confidenciais que não poderiam estar expostas em uma organização.
- Conscientizar os alunos sobre os possíveis impactos de se ter aplicações vulneráveis dentro das empresas, bem como as possíveis consequências ligadas diretamente à continuidade dos processos de negócios na organização.

V. CONTEÚDO PROGRAMÁTICO

MÓDULO 1: As Principais Vulnerabilidades em Aplicações Web (OWASP *Top Ten*)

MÓDULO 2: Introdução ao *Hacking*: Primeiros Passos

MÓDULO 3: Instalando e Configurando o Ambiente de Testes

MÓDULO 4: PenTest Web: *Data Injection*

MÓDULO 5: PenTest Web: *Broken Authentication*

MÓDULO 6: PenTest Web: *Sensitive Data Exposure*

MÓDULO 7: PenTest Web: XSS (*Cross Site Scripting*)

VI. CONTEÚDO DETALHADO DO CURSO

MÓDULO 1: AS PRINCIPAIS VULNERABILIDADES EM APLICAÇÕES WEB (OWASP TOP TEN) (6h)

1.1. OBJETIVOS ESPECÍFICOS:

Apresentar uma visão geral sobre as principais vulnerabilidades em aplicações web reportadas pela comunidade OWASP (*Open Security Application Project*).

1.2. TÓPICOS:

- **Introdução**
- **Data Injection (“Injeção de dados”)**
- **Broken Authentication (“Autenticação Quebrada”).**
- **Sensitive Data Exposure (“Exposição de Dados Sensíveis”) .**
- **XML External Entities -XXE (Entidades Externas XML).**
- **Broken Access Control (“Controle de Acesso Quebrado”).**
- **Security Misconfiguration (“Erros de Configuração de Segurança”).**
- **Cross-Site Scripting (XSS).**
- **Insecure Deserialization (“Desserialização Insegura”).**
- **Using Components with Known Vulnerabilities (“Usando Componentes com Vulnerabilidades Conhecidas”).**
- **Insufficient Logging & Monitoring (“Registro e Monitoramento Insuficientes”)**

MÓDULO 2: INTRODUÇÃO AO HACKING: PRIMEIROS PASSOS (4h)

2.1. OBJETIVOS ESPECÍFICOS:

Introduzir ao aluno os primeiros passos sobre categorias existentes de hackers e seus campos de atuação, uma breve introdução à história das distribuições Linux voltadas à atividade hacker, apresentação das estruturas destas distribuições Linux, demonstrar que é possível praticar testes de invasão a partir de sistemas Microsoft apesar de suas limitações e abordagem de conceitos de rede necessários para o processo de pentest.

2.2. TÓPICOS:

- **Introdução.**
- **Introdução as distribuições Linux para *pentesters.***
- **Explicando a infraestrutura das distribuições Linux para *pentesters.***
- **Testes de invasão a partir de sistemas windows.**
- **Conceitos de redes de computadores para *pentest* de aplicações web.**
- **Servidores web.**
- **Entendendo e explorando transferências de servidores de DNS.**
- **Protocolos e métodos HTTP.**
- **Criptografia via SSL.**

MÓDULO 3: INSTALANDO E CONFIGURANDO O AMBIENTE DE TESTES (6h)

3.1 OBJETIVOS ESPECÍFICOS:

Preparar o ambiente de testes para a exploração da estrutura de serviços Web.

3.2. TÓPICOS:

- **Preparando o ambiente de testes.**
- **Configurações e ajustes.**
- **Selecionando ferramentas de pentest.**

MÓDULO 4: PENTEST WEB: DATA INJECTION *(6h)*

4.1 OBJETIVOS ESPECÍFICOS:

Apresentar as técnicas empregadas em ataques de *Data Injection* e contramedidas de proteção a partir de um cenário preparado para testes de intrusão.

4.2. TÓPICOS:

- **Introdução ao Data Injection.**
- **Coletando e aproveitando-se das informações:** vetores, parâmetros, serviços Web, etc.
- **Falhas de injeção:** consultas SQL, LDAP, XPath ou NoSQL, comandos SO, analisadores XML, cabeçalhos SMTP, etc.)
- **Escalando privilégios.**
- **Exemplos de ataques de Data Injection.**
- **Contramedidas.**
- **Prática de Laboratório:** pentest web com Data Injection.

MÓDULO 5: PENTEST WEB: BROKEN AUTHENTICATION *(6h)*

5.1 OBJETIVOS ESPECÍFICOS:

Apresentar as técnicas empregadas em ataques de "Autenticação Quebrada" para obtenção de informações e exploração de gerenciamento de sessões a partir de um cenário preparado para testes de intrusão.

5.2. TÓPICOS:

- **Introdução ao *Broken Authentication.***
- **Coletando e aproveitando-se das informações:** nome de usuário válido, combinações de senha para credencial, contas padrão, tokens de sessão, etc.
- **Controle de identidade e acesso.**
- **Exploração de Autenticação interrompida.**
- **Ataques de dicionário.**
- **Exemplos de ataques de *Bronken Authentication*.**
- **Contramedidas.**
- **Prática de Laboratório:** pentest web com exploração de *Bronken Authentication*.

MÓDULO 6: PENTEST WEB: SENSITIVE DATA EXPOSURE *(6h)*

6.1 OBJETIVOS ESPECÍFICOS:

Apresentar as técnicas empregadas em ataques de obtenção e exploração de dados sensíveis ou críticos a partir de um cenário preparado para testes de intrusão.

6.2. TÓPICOS:

- **Introdução a Sensitive Data Exposure.**
- **Coletando e aproveitando-se das informações:** registros de saúde, credenciais, dados pessoais e de cartões de crédito.
- **Algoritmos, cifras e protocolos comuns.**
- **Páginas sem implementação de TLS.**
- **Downgrade de conexões de HTTPS para HTTP e sequestro de sessão.**
- **Dados não criptografados.**
- **Gerenciamento de chaves fracas.**
- **Hashing de senhas em banco de dados.**
- **Exemplos de ataques a dados sensíveis ou críticos.**
- **Contramedidas.**
- **Prática de Laboratório:** pentest web com obtenção e exploração de dados sensíveis ou críticos.

MÓDULO 7: PENTEST WEB: XSS (CROSS SITE SCRIPTING) *(6h)*

7.1 OBJETIVOS ESPECÍFICOS:

Apresentar as técnicas empregadas em ataques de XSS para obtenção de informações e exploração de gerenciamento de sessões.

7.2. TÓPICOS:

- **Introdução ao XSS (Cross Site Scripting).**
- **Reflected XSS, Stored XSS, DOM XSS.**
- **Conceitos sobre Arquitetura Web:** HTML, CSS, Scripts, DOM (*Document Object Model*).
- **Scripts maliciosos:** principais vetores.
- **Dados não confiáveis:** Bypass da Lógica de Validação (Ofuscação).
- **Sanitização e Validação de dados de entrada.**
- **Sessões mal gerenciadas:** Roubo/Vazamento de *Cookie.*
- **Exemplos de ataques XSS.**
- **Contramedidas.**
- **Prática de Laboratório:** pentest web com ataques XSS.

VII. RECURSOS DIDÁTICOS:

Instalação e configuração de ambiente laboratório, apresentação de *slides*, vídeos e material de apoio.

VIII. Metodologia:

- Treinamento completamente *hands-on.*
- Esclarerimento de dúvidas frequentes.
- Aulas completamente interativas com os alunos.

IX. INSTRUTOR

RODRIGO ALMEIDA, Grad

Graduado em Redes de computadores pelo Centro Universitário do Norte - *Laureate International Universities*.

Diretor fundador da Bash IT Services & Security Audit.

FORMAÇÃO ACADÊMICA: Graduado em Redes de Computadores pelo Centro Universitário do Norte - *Laureate International Universities*. **2. ATIVIDADES DOCENTES/INSTITUIÇÕES DE ENSINO/EXPERIENCIAS PROFISSIONAIS:** Possui mais de 17 anos no mercado de sistemas Unix/Linux, infraestrutura e segurança da informação em empresas como Global Crossing, Salcomp, Samsung, Força Aérea Brasileira, Nokia e Microsoft. Possui experiência internacional na área de segurança da informação, tendo atuado em tratativas de segurança em ambientes tecnológicos da China, Twain, Índia e Finlândia. Fundador e Diretor da empresa de Segurança da Informação Bash IT Services & Security Audit (2015).

X. TREINAMENTOS *IN COMPANY*

Solicite a sua proposta em nosso website.