Guia de preparação

Edição 202003

Conteúdo

1. Visão geral 4
2. Requisitos do exame 6
3. Lista de conceitos básicos 9
4. Literatura 11

1. Visão geral

EXIN Ethical Hacking Foundation (EHF.PR)

Escopo

O propósito do Ethical Hacking é o de avaliar, de maneira legal, a segurança de um sistema ou rede de computador por meio da descoberta e exploração das vulnerabilidades.

Resumo

A tecnologia da atualidade está se movendo rapidamente e mudando a forma de fazermos negócios. Por padrão, as empresas digitalizam todas as informações, armazenam seus dados na nuvem e usam software de código aberto. Isso levanta questões de segurança de informações relacionadas com a infraestrutura da rede e do sistema.

O módulo Fundamentos de Ethical Hacking EXIN abrange as etapas básicas do Ethical Hacking: coleta de itens de inteligência, varredura de redes/sistemas de computador e invasão de sistemas. Os candidatos deverão estar muito conscientes da diferença entre o hacking legal e ilegal, bem como das consequências de seu uso indevido.

Mais detalhadamente, o candidato desenvolverá uma compreensão dos seguintes tópicos:
- Detecção de rede (coleta de informações a partir do tráfego de rede)
- Cracking (Quebra de códigos) de uma chave WEP e WPA(2) a partir de uma rede sem fio
- Varredura da vulnerabilidade da rede
- Invasão básica em sistemas de computador
- Cracking de senhas
- Hackeamento baseado na web, contendo Injeções SQL (SQLi), Scripts Cruzados entre Sites (XSS), Inclusões de Arquivos Remotos (RFI)

O exame da Fundação de Ethical Hacking EXIN testa o conhecimento do candidato em:
- fundamentos de Ethical Hacking e
- a prática de Ethical Hacking.

Contexto

O exame EXIN Ethical Hacking Foundation faz parte do programa de qualificação EXIN Ethical Hacking.

Pùblico-alvo

Esta certificação destina-se a agentes de segurança, arquitetos de rede, administradores de rede, auditores de segurança, profissionais de segurança, programadores de computador e especialistas em redes, gerentes que trabalham na área de Ethical Hacking e qualquer pessoa interessada em melhorar e/ou testar a segurança de uma infraestrutura de TI. O módulo destina-se também a hackers éticos (iniciantes), que querem obter certificação e verificar seus conhecimentos.

Requisitos para a certificação

- Conclusão do exame EXIN Ethical Hacking com sucesso.

No entanto, recomenda-se enfaticamente um treinamento em Fundamentos de Ethical Hacking e conhecimento de Linux.

Detalhes do exame

Tipo do exame:	Perguntas de múltipla escolha
Número de questões:	40
Mínimo para aprovação:	65%
Com consulta/observações:	Não
Equipamentos eletrônicos permitidos:	Não
Tempo designado para o exame:	60 minutos

As Regras e Regulamentos dos exames EXIN aplicam-se a este exame.

Taxonomia de Bloom

A certificação EXIN Ethical Hacking Foundation testa os candidatos nos Níveis Bloom 1 e 2 de acordo com a Taxonomia Revisada de Bloom:

- Nível Bloom 1: Lembrança – depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar.
- Nível Bloom 2: Compreensão – um passo além da lembrança. O entendimento mostra que os candidatos compreendem o que é apresentado e podem avaliar como o material de aprendizagem pode ser aplicado em seu próprio ambiente. Este tipo de pergunta pretende demonstrar que o candidato é capaz de organizar, comparar, interpretar e escolher a descrição correta de fatos e ideias.

Treinamento

Horas de contato

A carga horária mínima para este treinamento é de 16 horas. Isto inclui trabalhos em grupo, preparação para o exame e pausas curtas. Esta carga horária não inclui pausas para almoço, trabalhos extra aula e o exame.

Indicação de tempo de estudo

60 horas, dependendo do conhecimento pré-existente.

Provedor de treinamento

Você encontrará uma lista de nossos provedores de treinamento credenciados em www.exin.com.

2. Requisitos do exame

Os requisitos do exame são definidos nas especificações do exame. A tabela a seguir lista os tópicos (requisitos do exame) e subtópicos (especificações do exame) do módulo.

Requisito do exame	Especificaçao do exame	Peso
1. Introdução ao Ethical Hacking		**15%**
	1.1 A Ética hacker	
	1.2 Princípios básicos	
2. Detecção de rede		**10%**
	2.1 Ferramentas	
	2.2 Extração de informações	
3. Hackeamento de redes sem fio		**10%**
	3.1 Preparação	
	3.2 Aircrack-NG	
4. Invasão no sistema		**35%**
	4.1 Coleta de Informações	
	4.2 Ferramentas de software (Nmap, Metasploit)	
	4.3 Impressões digitais e vulnerabilidades	
	4.4 Exploração e pós-exploração	
5. Hackeamento baseado na web		**30%**
	5.1 Ataques a bancos de dados	
	5.2 Ataques ao cliente	
	5.3 Ataques ao servidor	
	Total	**100%**

Especificações do exame

1 Introdução ao Ethical Hacking

1.1 Ética hacker

O candidato …

1.1.1 compreende as implicações jurídicas do hacking.

1.1.2 pode descrever diferentes tipos de hackers.

1.2 Princípios básicos

O candidato …

1.2.1 sabe a diferença entre o teste white box (caixa branca) e o black box (caixa preta).

1.2.2 pode descrever as diferentes fases no processo de hacking.

2 Detecção de rede

2.1 Ferramentas

O candidato …

2.1.1 conhece os diferentes tipos de ferramentas de Detecção de Rede.

2.1.2 sabe usar as ferramentas mais comuns de Detecção de Rede.

2.2 Extração de informações

O candidato …

2.2.1 sabe a função dos cabeçalhos HTTP.

2.2.2 pode extrair informações dos cabeçalhos HTTP.

3 Hacking de redes sem fio

3.1 Preparação

O candidato …

3.1.1 pode encontrar informações sobre seu próprio adaptador de rede.

3.2 Aircrack-NG

O candidato …

3.2.1 sabe explicar o Airodump-NG.

3.2.2 conhece os diferentes tipos de funções de ferramentas no Aircrack.

3.2.3 sabe o que ESSID&BSSID significa.

4 Invasão no sistema

4.1 Coleta de Informações

O candidato …

4.1.1 sabe encontrar informações sobre um alvo on-line.

4.1.2 sabe encontrar informações sobre um alvo dentro de uma rede.

4.2 Ferramentas de software (Nmap, Metasploit)

O candidato …

4.2.1 é capaz de analisar um alvo.

4.2.2 sabe como combinar as ferramentas.

4.3 Impressões digitais e vulnerabilidades

O candidato …

4.3.1 sabe encontrar vulnerabilidades com base nos resultados de uma varredura.

4.3.2 sabe realizar a coleta manual de impressões digitais.

4.4 Exploração e pós-exploração

O candidato …

4.4.1 sabe explorar uma vulnerabilidade com o Metasploit.

4.4.2 sabe extrair informações do sistema após a exploração.

5 Hacking baseado na web

5.1 Ataques a bancos de dados

O candidato …

5.1.1 conhece os passos para testar as vulnerabilidades de SQLi.

5.1.2 sabe explicar como extrair dados com a SQLi.

5.1.3 conhece as seguintes funções: CONCAT, LOAD_FILE, UNION, SELECT, @@version, ORDER BY, LIMIT

5.2 Ataques ao cliente

O candidato …

5.2.1 sabe criar uma PoC (Prova de Conceito) de XSS.

5.2.2 conhece os conceitos básicos de sequestro de sessão i/c/w XSS.

5.2.3 sabe evitar os filtros básicos de XSS.

5.3 Ataques ao servidor

O candidato …

5.3.1 sabe como um RFI é executado.

5.3.2 conhece as funcionalidades básicas dos shells php, como r57 e c99.

5.3.3 sabe a diferença entre os shells connect Bind & Back e o que eles fazem.

3. Lista de conceitos básicos

Este capítulo contém os termos e abreviaturas com que os candidatos devem se familiarizar.

Por favor, note que o conhecimento destes termos de maneira independente não é suficiente para o exame; O candidato deve compreender os conceitos e estar apto a fornecer exemplos.

English	Brazilian Portuguese
@@ version	@@ version
+x eXecute	+x eXecute
Aircrack-ng	Aircrack-ng
Aireplay-ng	Aireplay-ng
Airodump-ng	Airodump-ng
arpspoof	arpspoof
BackTrack	BackTrack
Bind & Back (Reverse) connect shells	Shells connect Bind & Back (Reverse)
Black box testing	Testes black box
BSSID & ESSID	BSSID & ESSID
Command line Interface (CLI)	Interface de linha de comandos (CLI)
CONCAT	CONCAT
Cross-Site Scripting (XSS)	Scripts Cruzados entre Sites (XSS)
Default Gateway	Gateway Padrão
Dynamic Host Configuration Protocol (DHCP)	Protocolo de Configuração de Host Dinâmico (DHCP)
Domain Name System (DNS)	Sistema de Nomes de Domínios (DNS)
Fingerprinting	Impressões digitais
FTP server	Servidor FTP
Graphical User Interface (GUI)	Interface Gráfica do Usuário (GUI)
Hackers	Hackers
o Black hat hackers	o Hackers black hat (chapéu preto)
o Grey hat hackers	o Hackers grey hat (chapéu cinza)
o Hacktivists	o Hacktivistas
o White hat hackers	o Hackers white hat (chapéu branco)
Hashdump	Hashdump
HTTP	HTTP
ipconfig /all	ipconfig /all
iwconfig	Iwconfig
John The Ripper (JTR)	John The Ripper (JTR)
Kali Linux	Kali Linux
Keyloggers	Keyloggers
Kismet	Kismet
LIMIT	LIMIT
LOAD_FILE	LOAD_FILE
Local File Inclusion (LFI)	Inclusão de Arquivos Locais (LFI)
MAC address	Endereço MAC

Metasploit	Metasploit
Meterpreter payload	Carga do meterpreter
Nessus	Nessus
Netcat	Netcat
Network File System (NFS)	Network File System (NFS)
Nikto	Nikto
Nmap	Nmap
Nonce	Nonce
ORDER BY	ORDER BY
Packet sniffers	Detectores de pacotes
Penetration test	Teste de Invasão
php-shell o c99shell o r57shell	php-shell o c99shell o r57shell
Ping	Ping
Privilege Escalation Exploit / Kernel exploit	Exploração de escalonamento de privilégios / exploração de kernel
Proof of Concept (PoC)	Prova de Conceito (PoC)
Reconnaissance	Reconhecimento
Remote File Inclusion (RFI)	Inclusão de Arquivos Remotos (RFI)
Scanning	Varredura
SELECT	SELECT
Session Hijacking	Sequestro de sessão
Shell	Shell
Spoofing	Forjamento
SQL- MySQL	SQL- MySQL
SQL injection (SQLi)	Injeção SQL (SQLi)
sqlmap	Sqlmap
SSH server	Servidor SSH
SYN scan	Varredura SYN
TCPdump	TCPdump
TCP three-way handshake	Handshake de três vias TCP
Tshark	Tshark
UNION	UNION
VNC Injection payload	Carga de Injeção VNC
WEP key	Chave WEP
White box testing	Testes white box
WPA2	WPA2

4. Literatura

Literatura do exame

O conhecimento necessário para o exame é coberto na seguinte literatura:

A. Georgia Weidman
Testes de Invasão: Uma introdução prática ao hacking
ISBN-10: 8575224077
ISBN-13: 978-8575224076

B. **Article EXIN Ethical Hacking Foundation**
Free download on www.exin.com.

Literatura adicional

C. Stuart McClure, Joel Scambray, George Kurtz
Hacking Exposed 7: Network Security Secrets & Solutions (Hacking Exposed: Network Security Secrets & Solutions)
ISBN-13: 978-0071780285

D. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

E. **Prosecuting Computer Crimes Manual**
http://www.justice.gov/criminal/cybercrime
Documents and reports - Manuals
Chapter 1

Justificativa de escolhas

A literatura adicional destina-se exclusivamente a referência e aprofundamento do conhecimento. A literatura adicional (**C**) pode ser lida pelo candidato para que ela obtenha um conhecimento mais profundo do assunto. **D** (Legislação da UE) e **E** (Legislação dos EUA) abrangem as consequências legais de uso indevido de sistemas de computador e dados de computador.

Matriz da literatura

Requisito do exame	Especificação do exame	Literatura
1. Introdução ao Ethical Hacking		
	1.1 A Ética hacker	B: Cap. 1, 2
	1.2 Princípios básicos	B: Cap. 3
2. Detecção de rede		
	2.1 Ferramentas	A: Cap. 7
	2.2 Extração de informações	A: Cap. 7
3. Hackeamento de redes sem fio		
	3.1 Preparação	A: Cap. 15
	3.2 Aircrack-NG	A: Cap. 15
4. Invasão no sistema		
	4.1 Coleta de Informações	A: Cap. 5, 7
	4.2 Ferramentas de software (Nmap, Metasploit)	A: Cap. 5
	4.3 Impressões digitais e vulnerabilidades	A: Cap. 6, 10
	4.4 Exploração e pós-exploração	A: Cap. 4
5. Hackeamento baseado na web		
	5.1 Ataques a bancos de dados	A: Cap. 14
	5.2 Ataques ao cliente	A: Cap. 14
	5.3 Ataques ao servidor	A: Cap. 14

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER