Guia de Preparação

Edição 201807

Conteúdo

1. Visão geral

EXIN Cyber & IT Security Foundation (CISEF.PR)

Escopo

Os assuntos deste módulo são os seguintes:

- Redes TCP/IP
- Sistemas de computador
- Aplicações e bancos de dados
- Criptografia
- Gerenciamento de identidade e acesso
- Computação em nuvem
- Explorando vulnerabilidades

Resumo

A segurança em TI não está se tornando apenas mais importante, mas também mais sofisticada. Face a isso, as organizações estão dedicando cargos à proteção de seus dados e sistemas. O programa EXIN Cyber & IT Security é voltado a fornecer aos candidatos o conhecimento necessário para entender o lado técnico da segurança da informação. Ele abrange o contexto teórico, informações detalhadas sobre infraestrutura de segurança e aborda vulnerabilidades, riscos e medidas necessárias.

Contexto

O Certificado EXIN Cyber & IT Security Foundation é parte do esquema geral de qualificação de Cyber & IT Security.

Público alvo

- Administrador de rede
- Desenvolvedor de aplicativos
- Profissionais de segurança
- Auditor
- Gerente de Qualidade
- Gerente Operacional

Requisitos para a certificação

Conclusão bem-sucedida do exame EXIN Cyber & IT Security Foundation.

Detalhes do exame

Tipo de exame:	Questões de múltipla escolha
Número de questões:	40
Índice mínimo para aprovação:	65%
Permitido consultas de livros/notas:	Não
Permitido utilizar equipamentos eletrônicos:	Não
Tempo permitido para o exame:	60 minutos

As regras e regulamentos do exame do EXIN se aplicam para este exame.

Bloom level

A certificação EXIN Cyber & IT Security Foundation testa candidatos no Bloom Nível 1 e Nível 2 de acordo com a Taxonomia Bloom Revisada:

- Bloom Nível 1: Remembering (Lembrança) - depende da recuperação de informações. Os candidatos precisarão absorver, lembrar, reconhecer e recordar. Este é o elemento fundamental da aprendizagem antes que os candidatos possam avançar para níveis mais elevados.
- Bloom Nível 2: Understanding (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.

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 pequenas pausas. Esta carga horária não inclui trabalhos extra aula, a sessão de exame e pausas para almoço.

Indicação de tempo de estudo

60 horas, dependendo do conhecimento existente.

Provedores de treinamento

Você pode encontrar a lista dos nossos provedores de treinamento: www.exin.com.

2. Requisitos do exame

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

Requisitos do exame	Especificações do exame	Peso %
1. Redes TCP/IP		**10%**
	1.1 Nós, conexão de nós e endereços TCP/IP	5%
	1.2 Modelo OSI, modelo TCP/IP, protocolos	5%
2. Sistemas de computador		**10%**
	2.1 Arquitetura de computadores, sistemas operacionais	5%
	2.2 Vulnerabilidades de sistemas de computador	2.5%
	2.3 Medidas de segurança de sistemas de computador	2.5%
3. Aplicações e bancos de dados		**15%**
	3.1 Desenvolvimento de aplicações	5%
	3.2 Bancos de dados	5%
	3.3 Problemas de segurança e contramedidas	5%
4. Criptografia		**20%**
	4.1 Metodologias e padrões de encriptação	5%
	4.2 Assinaturas digitais, hashing	5%
	4.3 Infraestrutura de chave pública (PKI)	5%
	4.4 SSL/TLS, IPSec	5%
5. Gerenciamento de identidade e acesso		**15%**
	5.1 Identificação, autenticação, biometria, Single sign-on (SSO), gerenciamento de senhas	10%
	5.2 Autorização	5%
6. Computação em nuvem		**15%**
	6.1 Características e modelos de implantação	10%
	6.2 Riscos	5%
7. Explorando vulnerabilidades		**15%**
	7.1 Categorias de ataque & tipos de ameaças	5%
	7.2 Atores a ferramentas	10%
	Total	**100%**

Especificações do exame

1. Redes TCP/IP

1.1 Nós, conexão de nós e endereços TCP/IP

O candidato é capaz de...

1.1.1 descrever o que é um nó.

1.1.2 descrever como os nós são ligados uns aos outros.

1.1.3 explicar os principais conceitos de endereçamento TCP/IP tanto na V4 como na V6.

1.2 Modelo OSI, modelo TCP/IP, protocolos

O candidato é capaz de...

1.2.1 descrever as camadas e principais funcionalidades dos modelos OSI e TCP/IP.

1.2.2 explicar os principais protocolos de rede, suas funcionalidades e como eles se encaixam nos modelos de referência OSI e TCP/IP.

2. Sistemas de computador

2.1 Arquitetura de computadores, sistemas operacionais

O candidato é capaz de...

2.1.1 explicar os componentes de um sistema de computação.

2.1.2 descrever como funciona um sistema operacional.

2.1.3 listar os principais sistemas operacionais.

2.2 Vulnerabilidades de sistemas de computador

O candidato é capaz de...

2.2.1 identificar os tipos mais comuns de vulnerabilidades do sistema de computador.

2.3 Medidas de segurança de sistemas de computador

O candidato é capaz de...

2.3.1 identificar as principais medidas de segurança relacionadas aos sistemas de computador.

3. Aplicações e bancos de dados

3.1 Desenvolvimento de aplicações

O candidato é capaz de...

3.1.1 explicar os diferentes métodos e fases do ciclo de vida de desenvolvimento de sistemas.

3.1.2 descrever as vantagens e desvantagens de cada um dos diferentes métodos do ciclo de vida de desenvolvimento de sistemas.

3.1.3 explicar como abordar a segurança durante o ciclo de vida de desenvolvimento de sistemas.

3.2 Bancos de dados

O candidato é capaz de...

3.2.1 descrever diferentes modelos de bancos de dados.

3.2.2 explicar a funcionalidade do banco de dados e os sistemas de gerenciamento de banco de dados.

3.3 Problemas de segurança e contramedidas

O candidato é capaz de...

3.3.1 descrever os problemas de segurança predominantes relacionados ao desenvolvimento de aplicativos e bancos de dados.

3.3.2 explicar as contramedidas contra questões de segurança relacionadas a aplicativos e bancos de dados.

4. Criptografia

4.1 Metodologias e padrões de encriptação

O candidato é capaz de....

4.1.1 diferenciar encriptação simétrica e assimétrica.

4.1.2 identificar padrões e algoritmos de encriptação.

4.2 Assinaturas digitais, hashing

O candidato é capaz de....

4.2.1 explicar como as assinaturas digitais fornecem autenticidade e não repúdio.

4.2.2 explicar como o hashing fornece a integridade da informação digital.

4.2.3 descrever os principais padrões de hashing.

4.3 Infraestrutura de chave pública (PKI)

O candidato é capaz de....

4.3.1 descrever os componentes, partes e processos de uma infraestrutura de chave pública.

4.3.2 explicar o que são certificados digitais e seus casos de uso.

4.4 SSL/TLS, IPSec

O candidato é capaz de....

4.4.1 explicar a tecnologia e casos de uso de SSL/TLS.

4.4.2 explicar a tecnologia e os casos de uso do IPSec.

5. Gerenciamento de identidade e acesso

5.1 Identificação, autenticação, biometria, Single sign-on (SSO), gerenciamento de senhas

O candidato é capaz de....

5.1.1 diferenciar entre identificação e autenticação.

5.1.2 descrever as principais tecnologias de autenticação e autenticação de dois fatores.

5.1.3 explicar a biometria e seus casos de uso.

5.1.4 explicar os conceitos e os diferentes tipos de Single sign-on (SSO).

5.1.5 explicar o gerenciamento de senhas e seus casos de uso.

5.2 Autorização

O candidato é capaz de...

5.2.1 descrever como os princípios de Necessidade de Saber, Menor Privilégio e Separação de Deveres (SoD) se relacionam com a autorização.

5.2.2 descrever modelos de autorização, como controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributo (ABAC).

5.2.3 descrever as especificações e funcionalidade do OpenID Connect e do OAuth.

6. Computação em nuvem

6.1 Características e modelos de implantação

O candidato é capaz de...

6.1.1 diferenciar entre os modelos de implantação, nuvem pública, nuvem privada e nuvem híbrida.

6.1.2 explicar os modelos de serviço SaaS, PaaS, IaaS, SECaaS e IDaaS.

6.2 Riscos

O candidato é capaz de...

6.2.1 identificar os riscos da computação em nuvem.

7. Explorando vulnerabilidades

7.1 Categorias de ataque & tipos de ameaças

O candidato é capaz de...

7.1.1 identificar as principais categorias de ataque de cibercrime.

7.2 Atores e ferramentas

O candidato é capaz de...

7.2.1 reconhecer Black hat hackers, White hat hackers, Grey hat hackers, script kiddies e hacktivists.

7.2.2 identificar quais ferramentas os cibercriminosos usam.

7.2.3 identificar as etapas que os cibercriminosos tomam para explorar vulnerabilidades.

3. Lista de conceitos básicos

Este capítulo contém os termos com que os candidatos devem se familiarizar. Os termos estão listados por assunto, em ordem alfabética. Alguns termos podem se aplicar a assuntos diferentes. Eles são mencionados somente uma vez nesta lista.

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.

TCP/IP networking	**Redes TCP/IP**
Address Resolution Protocol (ARP)	Address Resolution Protocol (ARP)
Alternative routing	Roteamento alternativo
American National Standards Institute (ANSI)	American National Standards Institute (ANSI)
Anomaly based	Baseado em anomalias
Application level	Nível de aplicação
Architecture	Arquitetura
Bastion host	Bastion host
Blocking	Bloqueio
Boundary router	Roteador de borda
Broadcast domain	Domínio de broadcast
BSID	BSID
Cabling	Cabeamento
Challenge-Response	Desafio e resposta
Compartmentalization	Compartimentalização
Connection	Conexão
Data link	Enlace – Link de Dados
Deep packet inspection	Inspeção profunda de pacotes
Defense Advanced Research Projects Agency (DARPA)	Agência de Projetos de Pesquisa Avançada de Defesa (DARPA)
Defense in Depth	Defesa em Profundidade
Demilitarized Zone (DMZ)	Zona desmilitarizada (DMZ)
Destination node	Nó de destino
Direct link	Link direto
(Distributed) Denial of Sevice ((D)DoS) attack	Ataque (Distribuído) de negação de domínio ((D)DoS)
Diverse routing	Roteamento diverso
Domain Name System (DNS)	Sistema de nomes de domínio (DNS)
EIA/TIA	EIA/TIA
Ethernet	Ethernet
External footprint	Pegada externa
False negative / False positive	Falso negativo / falso positivo
File Transfer Protocol (FTP)	Protocolo de transferência de arquivos (FTP)
Filter	Filtro
Firewall (rules)	Firewall (regras)

Frame	Quadro
Gateway	Gateway
Hardware address	Endereço de hardware
Honeypot	Honeypot
Host-based intrusion detection system (HIDS)	Sistema de detecção de intrusão baseado em host (HIDS)
HTTP	HTTP
Hub	Hub
Institute of Electrical and Electronics Engineers (IEEE)	Instituto de Engenheiros Elétricos e Eletrônicos (IEEE)
Interface	Interface
Internet Engineering Task Force (IETF)	Força-Tarefa de Engenharia da Internet (IETF)
Internet of things (IoT)	Internet das coisas (IoT)
Internet protocol (IP) – IPv4 – IPv6	Protocolo de Internet (IP) - IPv4 - IPv6
Intrusion detection	Detecção de intrusão
Intrusion prevention	Prevenção de intrusões
Intrusion Prevention System (IPS)	Sistema de Prevenção de Intrusões (IPS)
IP spoofing	Falsificação de IP
IPSec	IPSec
Last mile	Última milha
Layered defense	Defesa em camadas
Link	Link
Load balancing	Balanceamento de carga
Local Area Network (LAN)	Rede local (LAN)
Logical address	Endereço lógico
Long-haul	Longa distância
MAC address	Endereço MAC
Mail relay	Retransmissão de email
Man-in-the-Middle	Man-in-the-Middle
Network access	Acesso à rede
Network address translation	Tradução do Endereço da Rede (NAT)
Network model	Modelo de rede
Network segmentation	Segmentação de rede
Next-generation firewall	Firewall de próxima geração
NIC	NIC
NIDS	NIDS
NOC	NOC
Node	Nó
Open ports	Portas abertas
OSI	OSI
Outbound traffic	Tráfego de saída
Packet	Pacote
Penetration test	Teste de invasão
Perimeter	Perímetro

Physical address	Endereço físico
POP3	POP3
Port numbers	Números de porta
Port scanning	Varredura de portas
Private address	Endereço privado
Protocol	Protocolo
Protocol flaws	Falhas de protocolo
Proxy (firewall / server)	Proxy (firewall / servidor)
Public address	Endereço público
Redundancy	Redundância
Regional Internet Registry (RIR)	Registro Regional da Internet (RIR)
Remote access	Acesso remoto
Request for Change (RfC)	Requisição de Mudança (RfC)
Request for Comment	Pedido de comentário
Request for Proposal (RfP)	Requisição de Proposta (RfP)
Rogue device	Dispositivo malicioso
Screened subnet	Sub-rede filtrada
Secure Shell	Shell seguro
Secure Socket Layer (SSL)	Secure Socket Layer (SSL)
Secure/Multipurpose Internet Mail Extensions (S/MIME)	Secure/Multipurpose Internet Mail Extensions (S/MIME)
Security protocols	Protocolos de segurança
Session hijacking	Sequestro de sessão
Signature based	Baseado em assinatura
Simple Network Management Protocol (SNMP)	Simple Network Management Protocol (SNMP)
SMTP	SMTP
Sniffing	Varredura
Source node	Nó de origem
Source routing	Roteamento de origem
Spoofing	Spoofing
SSH	SSH
SSID	SSID
Star topology	Topologia em estrela
Stateful / Stateless firewall	Firewall com estado / sem estado
Storage Area Network (SAN)	Storage Area Network (SAN)
Subnet	Sub-rede
Switch	Switch
System on Chip (SOC)	Sistema em Chip (SOC)
TCP/IP	TCP / IP
Transport Layer Security (TLS)	Transport Layer Security (TLS)
True negative / True positive	Verdadeiro negativo / Verdadeiro positivo
User Datagram Protocol (UDP)	User Datagram Protocol (UDP)
Virtual Circuit	circuito virtual

Virtual Network Connection (VNC)	Virtual Network Connection (VNC)
Virtual Private Network (VPN)	Rede Privada Virtual (VPN)
Voice over IP (VOIP)	Voz sobre IP (VOIP)
Wide Area Network (WAN)	Rede de longa distância (WAN)
Wire tapping	escuta / grampo
Computer systems	**Sistema de computador**
.Net	.Net
2-tier	2 camadas (2 tier)
3-tier	3 camadas (3 tier)
Android	Android
Apache	Apache
Appaserver	Appaserver
Application server	Servidor de aplicação
Backdoor	Porta dos fundos
Backup	Cópia de segurança
Backup schedule	Agendamento de backup
Buffer overflow	Estouro de buffer
Client/Server (C/S)	Cliente/Servidor (C/S)
Core	Núcleo
Covert channel	Canal secreto
Data leakage	Vazamento de informações
Data retention	Retenção de dados
Database server	Servidor de banco de dados
Desktop Virtualization	Virtualização de Desktop
Emanation	Emanação
Exchange	Exchange
Exploit	Exploit
External hot site	Hotsite externo
Fat server	Fat server
File server	Servidor de arquivos
File system	Sistema de arquivo
Firmware	Firmware
Grid	Grid
Hardening	Hardening
Hardware	Hardware
High-availability systems	Sistemas de alta disponibilidade
Hypertext Preprocessor (PHP)	Hypertext Preprocessor (PHP)
I/O	E/S
Internet Information Services (IIS)	Serviços de Informações da Internet (IIS)
Kolab	Kolab
Layered OS	SO (sistema operacional) em camadas
Log entries	Entradas de Log

Log reports	Relatórios de log
Longevity	Longevidade
Mail server	Servidor de e-mail
Mainframe	Mainframe
Media sanitization	Sanitização de mídia
Memory card	Cartão de memória
Mobile devices	Dispositivos móveis
Monolithic	Monolítico
Multiprocessing	Multiprocessamento
Multithreading	Multithreading
MySQL	MySQL
Non-volatile random-access memory (NVRAM)	Memória de acesso aleatório não volátil (NVRAM)
N-tier	N-camada (N-tier)
Oracle	Oracle
OS hardening	Endurecimento do SO (sistema operacional)
OS standardization	Padronização de SO (sistema operacional)
Out of band channels	Canais fora da banda
Parity	Paridade
Patch logs	Logs de Patch
Patch management	Gerenciamento de patches
Peer to Peer	Ponto a Ponto (Peer to Peer)
Peripheral	Periférico
Primary storage	Armazenamento primario
Print server	Servidor de impressão
Process	Processo
Radio-frequency identification (RFID)	Identificação por radiofrequência (RFID)
RAID	RAID
Recovery	Recuperação
Redundant power supply	Fonte de energia redundante
Remote buffer overflow	Estouro de buffer remoto
Remote lock	Bloqueio remoto
Remote support	Suporte remoto
Remote wipe	Limpeza remota
Restore	Restaurar
Root kit	Rootkit
Secondary storage	Armazenamento secundário
Security domains	Domínios de segurança
Security information and event management (SIEM)	Security information and event management (SIEM)
Security tokens	Tokens de segurança
Single Point of Failure (SPOF)	Ponto único de falha (SPOF)
SQL server	Servidor SQL
SSD	SSD

Storage capacity	Capacidade de armazenamento
Storage device	Dispositivo de armazenamento
Striping	Striping
Sun	Sun
Supercomputer	Supercomputador
Tablet	Tablet
TEMPEST	TEMPEST
Thin client	Thin client
Trojan	Trojan
Unattended screens	Telas não supervisionadas
Unix	Unix
Unpatched	Sem correção
Virtual memory	Memória virtual
Virtualization	Virtualização
Web security	Segurança da Web
Worm	Worm
z/OS	z/OS
z/VM	z/VM
Zimbra	Zimbra
Applications	**Aplicações**
Active X	Active X
Application development	Desenvolvimento de aplicações
Application Programming Interface (API)	Interface de programação de aplicativos (API)
Application security	Segurança de aplicativos
Application virtualization	Virtualização de aplicativos
Automatic Teller Machine (ATM)	Caixa eletrônico (ATM)
Code review	Revisão de código
Cross-site scripting (XSS)	Cross-site scripting (XSS)
Debugging	Depuração
Dialog box	Caixa de diálogo
E-banking	E-banking
Electronic Data Interchange (EDI)	Intercâmbio Eletrônico de Dados (EDI)
Electronic Fund Transfer (EFT)	Transferência Eletrônica de Fundos (TEF)
Electronic payment	Pagamento eletrônico
Flash	Flash
Geographic software	Software geográfico
HyperText Markup Language (HTML)	HyperText Markup Language (HTML)
Implementation flaws	Falhas de implementação
Input attacks	Ataques de entrada
Input sanitization	Sanitização de entrada
Java	Java
Java script	Javascript

Java security manager	Gerenciador de segurança Java
Malicious code	Código malicioso
Mobile code	Código móvel
Office suits	Suíte Office
Privileged access	Acesso Privilegiado
Sandbox	Sandbox
Silverlight	Silverlight
Software development	Desenvolvimento de software
SQL injection	SQL injection
Testing	Testando
Ubiquitous	Onipresente
Unicode attack	Ataque Unicode
User acceptance testing	Testes de aceitação do usuário
User interface	Interface de usuário
VBscript	VBscript
Web applications	Aplicações web
Databases	**Banco de dados**
Aggregation	Agregação
Big data	Big Data
Bypass attack	Ataque de bypass
Concurrency	Concorrência
Data Base Management System (DBMS)	Sistema de gerenciamento de banco de dados (DBMS)
Data contamination	Contaminação de dados
Data Control Language (DCL)	Data Control Language (DCL)
Data custodian	Guardião de dados
Data Definition Language (DDL)	Data Definition Language (DDL)
Data dictionary	Dicionário de dados
Data integrity	Integridade de dados
Data Manipulation Language (DML)	Data Manipulation Language (DML)
Data mining	Mineração de dados
Data owner	Proprietário dos dados
Data warehouse	Armazém de dados
Database hardening	Fortalecimento de banco de dados
Deadlock	Deadlock
Directory services	Serviços de diretório
Foreign key	Chave estrangeira
Inference	Inferência
Injection attack	Ataque de injeção
Integrity	Integridade
Lightweight Directory Access Protocol (LDAP) - OpenLDAP	LDAP (Lightweight Directory Access Protocol) - OpenLDAP
Maintainability	Manutenção

Metadata	Metadados
Misdirection	Misdirection
NoSQL	NoSQL
Online Transaction Processing (OLTP)	Processamento de Transações Online (OLTP)
Primary key	Chave primária
Query attack	Ataque de consulta
Relational model	Modelo relacional
Reusability	Reutilização
Sensitive data	Dados sensíveis
Structured Query Language (SQL)	Structured Query Language (SQL)
Transaction persistence	Persistência de transação
Unattended disks	Discos não supervisionados
View	View
X.500	X.500
Cryptography	**Criptografia**
3DES (Triple DES) - Data Encryption Standard	3DES (Triple DES) - Padrão de Encriptação de Dados
Advanced Encryption Standard (AES)	Padrão de Encriptação Avançada (AES)
Algorithm	Algoritmo
Asymmetric encryption	Encriptação assimétrica
Authenticity	Autenticidade
Brute force	Força bruta
Caesar	César
Certificate Authority (CA)	Autoridade de Certificação (CA)
Certificate Revocation List (CRL)	Lista de Revogação de Certificados (CRL)
Ciphertext	Texto cifrado
Cleartext	Texto claro
Closed message format	Formato de mensagem fechado
Confidentiality	Confidencialidade
Cracking	Craqueamento
Cryptanalysis	Criptoanálise
Crypto system	Sistema de criptografia
Cryptogram	Criptograma
Data at rest	Dados em repouso
Data in situ	Dados no local
Decryption	Descriptografia
Dictionary attack	Ataque de dicionário
Diffie-Hellman	Diffie-Hellman
Digital certificate	Certificado digital
Digital signature	Assinatura digital
Elliptic curve cryptography (ECC)	Criptografia de curva elíptica (ECC)
Encrypted passwords	Senhas criptografadas
Encryption	Encriptação

Encryption strength	Força da encriptação
Hash value	Valor de hash
Hashing	Hashing
Hybrid encryption	Encriptação híbrida
International Data Encryption Algorithm (IDEA)	Algoritmo Internacional de Encriptação de Dados (IDEA)
Kerckhoffs' principle	Princípio de Kerckhoff
Key	Chave
Key length	Comprimento da chave
Key management	Gerenciamento de chaves
Key rings	Chaveiro
Keyspace	Espaço de chaves
Mathematical function	Função matemática
MD4 , MD5	MD4, MD5
Message Authentication Code (MAC)	Código de Autenticação de Mensagem (MAC)
Message integrity	Integridade da mensagem
No security by obscurity	Nenhuma segurança pela obscuridade
Non-repudiation	Não repúdio
Online Certificate Status Protocol (OCSP)	Protocolo de status de certificado on-line (OCSP)
Open message format	Formato aberto de mensagem
OpenPGP	OpenPGP
Plaintext	Texto simples
Pretty Good Privacy (PGP)	Pretty Good Privacy (PGP)
Private key	Chave privada
Proof of origin	Prova de origem
Public key	Chave pública
Public Key Infrastructure (PKI)	Infraestrutura de chave pública (PKI)
Quantum encryption	Encriptação quântica
RC4, RC5, RC6	RC4, RC5, RC6
Registration Authority (RA)	Autoridade de Registro (RA)
Rijndael	Rijndael
ROT13	ROT13
RSA	RSA
SAFER (Secure And Fast Encryption Routine)	SAFER (Rotina de Criptografia Segura e Rápida)
Secrecy	Segredo
Secret key	Chave secreta
Secure Hash Algorithm (SHA)	Algoritmo de hash seguro (SHA)
Session key	Chave de sessão
Side channel attack	Ataque do canal lateral
Substitution cipher	Cifra de substituição
Symmetric encryption	Encriptação simétrica
Symmetric key	Chave simétrica

Temporal Key Integrity Protocol (TKIP)	Protocolo de integridade de chave temporal (TKIP)
Transposition cipher	Cifra de transposição
Trusted Third Party	Terceiro Confiável
Validation Authority (VA)	Autoridade de validação (VA)
Weak encryption	Encriptação fraca
WiFi Protected Access (WPA)	WiFi Protected Access (WPA)
Wired Equivalent Privacy (WEP)	Wired Equivalent Privacy (WEP)
Work factor	Fator de trabalho
X.509	X.509
Identity & Access Management	**Gerenciamento de Identidade e Acesso**
Access control	Controle de acesso
Access control matrix	Matriz de controle de acesso
Access privileges	Privilégios de acesso
Access rule violations	Violações de regra de acesso
Accessibility	Acessibilidade
Account lockout	Bloqueio de conta
Account ownership	Propriedade da conta
Accountability	Prestação de contas
Attribute-Based Access Control (ABAC)	Controle de Acesso Baseado em Atributos (ABAC)
Audit logs	Logs de auditoria
Authentication	Autenticação
Authentication hijacking	Sequestro de Autenticação
Authentication server	Servidor de autenticação
Authorization	Autorização
Biometric authentication	Autenticação biométrica
Biometrics	Biometria
Cookies	Cookies
Credentials	Credenciais
Cross-over error rate	Taxa de erro cruzada
Discretionary	Discricionário
eXtensible Access Control Markup Language (XACML)	eXtensible Access Control Markup Language (XACML)
Facial scanning	Digitalização facial
False match	Falso verdadeiro
Fingerprint scanning	Digitalização de impressões digitais
Handpalm scanning	Digitalização da palma da mão
HTTP-based authentication	Autenticação Baseada em HTTP
Identification	Identificação
Identity & Access	Identidade e Acesso
Iris scanning	Varredura da íris
Kerberos	Kerberos
Keystroke dynamics	Dinâmica de digitação

Least privilege	Privilégio mínimo
Logical access	Acesso lógico
Mandatory	Obrigatório
Multi-factor	Multi-fator
Need-to-know	Necessidade de saber (need-to-know)
OASIS	OÁSIS
OAuth 2.0	OAuth 2.0
OpenID Connect	OpenID Connect
Passphrase	Passphrase
Physical access control	Controle de acesso físico
PIN code	Código PIN
Retina scanning	Varredura de retina
Role mining	Mineração de papel
Role-Based Access Control (RBAC)	Controle de acesso baseado em função (RBAC)
Salting	Salting
Security Assertion Markup Language (SAML)	Security Assertion Markup Language (SAML)
Separation of duties (SoD)	Separação de funções (SoD)
Single sign-on (SSO)	Single sign-on (SSO)
Single-factor	Único fator
Smartcard	Smartcard
Strong authentication	Autenticação forte
Strong password	Senha forte
System for Cross-domain Identity Management (SCIM)	Sistema para Gerenciamento de Identidade entre Domínios (SCIM)
Token devices	Dispositivos de token
Two-factor	Dois fatores
User ID	ID do usuário
Vascular pattern	Padrão vascular
Voice recognition	Reconhecimento de voz
Cloud computing	**Computação em nuvem**
Cloud	Nuvem
Cloud checklist	Lista de verificação da nuvem
Community cloud	Nuvem comunitária
Customer lock-in	Bloqueio do cliente
Data retrieval	Recuperação de dados
Data storage	Armazenamento de dados
Deployments	Implantações
Dropbox	Dropbox
EU-US Privacy Shield	Escudo de privacidade UE-EUA
Exit strategy	estratégia de saída
Google docs	Documentos Google
Hardware platform	Plataforma de hardware

Hybrid cloud	Nuvem híbrida
iCloud	iCloud
Identity as a Service (IDaaS)	Identidade como um Serviço (IDaaS)
Infrastructure as a Service (IaaS)	Infraestrutura como Serviço (IaaS)
Jurisdiction	Jurisdição
Multi-tenant	Multi-inquilino
OneDrive	OneDrive
OpenStack	OpenStack
Platform as a Service (PaaS)	Plataforma como serviço (PaaS)
Private cloud	Nuvem privada
Public cloud	Nuvem pública
Safe Harbor	Porto Seguro
Security as a Service (SECaaS)	Segurança como serviço (SECaaS)
Service Level Agreement (SLA)	Acordo de Nível de Serviço (SLA)
Software as a Service (SaaS)	Software como serviço (SaaS)
Software platform	Plataforma de software
Vendor default	Padrão do fornecedor
Vendor lock-in	Bloqueio de fornecedor
Web services	serviços web
Exploiting Vulnerabilities	**Explorando Vulnerabilidades**
Active probing	Sondagem ativa
Actor	Ator
Advanced Persistent Threat (APT)	Ameaça persistente avançada (APT)
Anonymous	Anônimo
Antivirus software	Software antivírus
Attacks	Ataques
Auditing	Auditoria
Black hat hacker	Black hat hacker
Blackbox pentest	Blackbox pentest
Confidentiality, Integrity, Availability (CIA)	Confidencialidade, Integridade, Disponibilidade (CID)
Configuration weakness	Fragilidade de configuração
Containment	Contenção
Countermeasures	Contramedidas
Cracker	Cracker
Data breach	Violação de dados
Decoy files	Arquivos de chamariz
Defacing	Desfiguração
Detection	Detecção
Email attachments	Anexos de e-mail
Environmental security	Segurança ambiental
Ethical hacker	Hacker ético
Event	Evento

Evidence	Evidência
Exposures	Exposições
External threat	Ameaça externa
Forensics	Forense
Freenet	Freenet
Gray hat hacker	Gray hat hacker
Hacker	Hacker
Hacktivist	Hacktivista
Identity theft	Roubo de identidade
Incident	Incidente
Incident management	Gerenciamento de incidentes
Incident response	Resposta ao incidente
Information theft	Roubo de informações
Internal threat	Ameaça interna
Logging	Logging
Macros	Macros
Malware	Malware
Mantrap	Armadilha
Metasploit	Metasploit
MIME content	Conteúdo MIME
Monitoring	Monitoramento
Nessus	Nessus
Nmap	Nmap
Novice	Novato
Penetration	Invasão
Pentest	Pentest
Phishing	Phishing
Physical security	Segurança física
Pivot	Pivô
Prevention	Prevenção
Reaction	Reação
Reconnaissance	Reconhecimento
Remote Administration Tool (RAT)	Ferramenta de Administração Remota (RAT)
Scanning	Varredura
Script kiddie	Script kiddie
Scripting	Scripting
Security baseline	Linha de base de segurança
Security monitoring	Monitoramento de segurança
Sensitivity	Sensibilidade
Social engineering	Engenharia social

STRIDE • Spoofing identity • Tampering with data • Repudiation • Information disclosure • Denial of Service • Elevation of privilege	STRIDE • falsificação de identidade • adulteração de dados • repúdio • divulgação de informações • negação de serviço • elevação de privilégio
Threat assessment	Avaliação de ameaça
Tools	Ferramentas
Tor	Tor
Vandalism	Vandalismo
Virus detection	Detecção de vírus
Vulnerability	Vulnerabilidade
Vulnerability assessment	Avaliação de vulnerabilidade
Vulnerability exploitation	Exploração de vulnerabilidade
Vulnerability scan	Verificação de vulnerabilidade
Warez	Warez
White hat hacker	White hat hacker
Worms	Worms
Zero-day exploit	Zero-day exploit

4. Literatura

Literatura do exame

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

A. David Kim, Michael; G. Solomon
Fundamentals of Information Systems Security
Jones & Bartlett Learning, LLC (2018, 3rd edition)
ISBN: 978-1-284-11645-8

Literatura adicional

B. Hans van den Bent, Eline Kleijer
EXIN Ethical Hacking Foundation – Exam Literature
EXIN (versão mais recente)
Download gratuito em http://bit.ly/EHF-literature

Justificativa de escolhas

A literatura adicional destina-se exclusivamente a referência e aprofundamento do conhecimento. Este artigo B foi escrito como literatura complementar de exame para a EXIN Ethical Hacking Foundation, e também cobre a especificação 7.2 deste módulo EXIN Cyber & IT Security Foundation.

Matriz da literatura

Requisito do exame	Especificação do exame	Referência da literatura
1. Redes TCP/IP		
	1.1 Nós, conexão de nós e endereços TCP/IP	A: Capítulo 2, 10
	1.2 Modelo OSI, modelo TCP/IP, protocolos	A: Capítulo 10
2. Sistemas de computador		
	2.1 Arquitetura de computadores, sistemas operacionais	A: Capítulo 1, 6, 11
	2.2 Vulnerabilidades de sistemas de computador	A: Capítulo 1, 6
	2.3 Medidas de segurança de sistemas de computador	A: Capítulo 5, 6, 7, 8
3. Aplicações e bancos de dados		
	3.1 Desenvolvimento de aplicações	A: Capítulo 6
	3.2 Bancos de dados	A: Capítulo 5, 6
	3.3 Problemas de segurança e contramedidas	A: Capítulo 5, 6
4. Criptografia		
	4.1 Metodologias e padrões de encriptação	A: Capítulo 9
	4.2 Assinaturas digitais, hashing	A: Capítulo 9
	4.3 Infraestrutura de chave pública (PKI)	A: Capítulo 9
	4.4 SSL/TLS, IPSec	A: Capítulo 9
5. Gerenciamento de identidade e acesso		
	5.1 Identificação, autenticação, biometria, Single sign-on (SSO), gerenciamento de senhas	A: Capítulo 5, 9
	5.2 Autorização	A: Capítulo 5
6. Computação em nuvem		
	6.1 Características e modelos de implantação	A: Capítulo 5
	6.2 Riscos	A: Capítulo 4
7. Explorando vulnerabilidades		
	7.1 Categorias de ataque & tipos de ameaças	A: Capítulo 3, 11
	7.2 Atores a ferramentas	A: Capítulo 1, 11 B: Capítulo 1, 2, 3

Contato EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER