Objetivos do Exame de Certificação: SY0-401

INTRODUÇÃO

A Certificação CompTIA Security+ é uma credencial que não possui vínculo com nenhum fornecedor ou fabricante. O exame CompTIA Security+ é uma validação reconhecida internacionalmente de habilidades e conhecimento de segurança de nível de fundamentos, e é utilizada por organizações e profissionais de segurança em todo o mundo.

O exame CompTIA Security+ certificará que o candidato aprovado tem o conhecimento e as habilidades necessárias para identificar, participar de atividades de mitigação e oferecer segurança às infraestruturas, aplicações, informações e operações. Além disso, o candidato aprovado estará apto a aplicar controles de segurança para manter a confidencialidade, integridade e disponibilidade, identificar tecnologias e produtos apropriados, solucionar eventos e incidentes de segurança e atuar tendo ciência das políticas, leis e regulamentações aplicáveis.

A Certificação CompTIA Security+ é voltada ao profissional de segurança de TI que tenha:

- No mínimo 2 anos de experiência em administração de TI com foco em segurança
- Experiência técnica em segurança da informação
- Amplo conhecimento de questões e implementações de segurança incluindo os tópicos na lista de domínio abaixo

A certificação CompTIA Security+ está em conformidade com a norma ISO 17024 e como tal, passa por revisões e atualizações regulares dos objetivos do exame. Os seguintes objetivos da certificação CompTIA Security+ refletem as áreas de conhecimento nesta versão do exame, resultado de workshops especializados e focados no assunto e pesquisas abrangentes em toda a indústria quanto as habilidades e conhecimentos exigidos de um profissional de segurança da informação com dois anos de experiência.

Este documento, que descreve a estrutura do exame inclui a ponderação dos domínios, objetivos dos testes e exemplos de conteúdo. Os exemplos de tópicos e conceitos estão incluídos apenas para esclarecer os objetivos do exame portanto não devem ser considerados como uma lista completa de todo o seu conteúdo.

A tabela abaixo lista as áreas dos domínios mensuradas para este exame e o peso aproximado que cada uma representa no exame.

Domínios	% do exame
1.0 Segurança de rede	20%
2.0 Segurança de conformidade e operacional	18%
3.0 Ameaças e vulnerabilidades	20%
4.0 Segurança de aplicativo, dados e host	15%
5.0 Controle de acesso e gerenciamento de identidade	15%
6.0 Criptografia	12%
Total	**100%**

Política de uso autorizado de materiais sobre a CompTIA

A CompTIA Certifications, LLC não está afiliada a, nem autoriza, endossa ou admite o uso de qualquer conteúdo fornecido por sites de treinamento externos não autorizados ou "brain dumps". Os candidatos que usarem esses materiais como preparação para qualquer exame da CompTIA terão suas certificações anuladas e serão suspensos de futuros testes de acordo com o contrato do candidato CompTIA. Com o intuito de comunicar com maior clareza as políticas dos exames CompTIA referentes ao uso de materiais de estudo não autorizados, a CompTIA encaminha todos os candidatos a certificação para a página da Web sobre políticas dos exames de certificação da CompTIA:
http://certification.comptia.org/Training/testingcenters/policies.aspx

Por favor, leia todas as políticas da CompTIA antes de iniciar o processo de estudo para qualquer exame CompTIA. Os candidatos terão de
respeitar o Contrato do Candidato CompTIA
(http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) quando da entrega do exame.

Se um candidato não tiver a certeza se um determinado material de estudo é considerado não autorizado ("brain dump"), deverá efetuar uma pesquisa usando o CertGuard
que se encontra em:
http://www.certguard.com/search.asp

Ou consultar esta lista:
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**Nota: as listas abaixo de cada objetivo não são abrangentes. Outros exemplos de tecnologias, processos ou tarefas pertinentes a cada objetivo podem ser incluídos no exame, embora não estejam listados ou cobertos neste documento de objetivos.

A CompTIA revisa constantemente o conteúdo de seus exames e atualiza as questões para assegurar que os mesmos sejam atuais e a segurança de suas perguntas esteja protegida. Quando necessário, publicaremos exames atualizados baseados nos objetivos existentes. Lembre-se que todos os materiais de preparação de exames ainda serão válidos.

1.0 Segurança de rede

1.1 Implementar parâmetros de configuração de segurança em dispositivos de rede e outras tecnologias.

- Firewalls
- Roteadores
- Switches
- Balanceadores de carga
- Proxies
- Gateways de segurança na web
- Concentradores de VPN
- NIDS e NIPS
  - Baseado no comportamento
  - Baseado em assinatura
  - Baseado em anomalia
  - Análise Heurística
- Analisadores de protocolo
- Filtro de spam
- Appliance de segurança UTM
  - Filtro URL
  - Inspeção de conteúdo
  - Inspeção de malware
- WAF vs. firewall de rede
- Dispositivos baseados em aplicações
  - Firewalls
  - IPS
  - IDS
  - Proxies

1.2 Dado um cenário, utilizar os princípios de segurança na administração de redes.

- Gerenciamento baseado em regras
- Regras de firewall
- Gerenciamento de VLAN
- Configuração segura de roteador
- Listas de controle de acesso
- Segurança de porta
- 802.1x
- Proteções contra flooding
- Proteção de loop
- Negação implícita
- Segregação de redes
- Análise de Logs
- Gerenciamento Unificado de ameaças - UTM

1.3 Explicar os elementos e componentes do design de redes.

- DMZ
- Cálculo de Subnetting
- VLAN
- NAT
- Acesso remoto
- Telefonia
- NAC

- Virtualização
- Computação em nuvem
  - Plataforma como Serviço
  - Software como Serviço
  - Infraestrutura como Serviço
  - Privado
  - Público
  - Híbrido
  - Comunitária
- Segurança em camadas/defesa em profundidade

1.4 Dado um cenário, implementar serviços e protocolos comuns.

- Protocolos
  - IPSec
  - SNMP
  - SSH
  - DNS
  - TLS
  - SSL
  - TCP/IP
  - FTPS
  - HTTPS
  - SCP
  - ICMP
  - IPv4
  - IPv6
  - iSCSI
  - Canal de fibra
  - FCoE
  - FTP
  - SFTP
  - TFTP
  - TELNET
  - HTTP
  - NetBIOS
- Portas
  - 21
  - 22
  - 25
  - 53
  - 80
  - 110
  - 139
  - 143
  - 443
  - 3389
- Importância do Modelo OSI

1.5 Dado um cenário, solucionar problemas de segurança relacionados a redes sem fio.

- WPA
- WPA2

- WEP
- EAP
- PEAP
- LEAP
- Filtro de MAC
- Desabilitar o broadcast de SSID
- TKIP
- CCMP
- Posicionamento da antena
- Controles de nível de potência
- Captive Portal
- Tipos de antenas
- Site surveys
- VPN (em redes wireless abertas)

2.0 Segurança operacional de conformidade

2.1 Explicar a importância de conceitos relacionados a riscos.

- Tipos de controle
  - Técnico
  - Gerencial
  - Operacional
- Falsos positivos
- Falsos negativos
- Importância de políticas para reduzir riscos
  - Política de privacidade
  - Uso aceitável
  - Política de segurança
  - Férias obrigatórias
  - Rotatividade do trabalho
  - Segregação de tarefas
  - Privilégio mínimo (least privilege)
- Cálculo de risco
  - Probabilidade
  - ALE
  - Impacto
  - SLE
  - ARO
  - MTTR
  - MTTF
  - MTBF
- Quantitativo vs. Qualitativo
- Vulnerabilidades
- Vetores de ameaça
- Probabilidade/tendência para ameaças
- Estratégias de respostas à riscos:Evitar, transferir, aceptar, mitigar e desencorajar
- Riscos associados à computação em nuvem e virtualização
- RTO e RPO

2.2 Resumir as implicações de segurança da integração de sistemas e dados com terceiros.

- Parceiros comerciais internos/externos
- Redes sociais e/ou aplicativos

- Contratos de interoperabilidade
    - SLA
    - BPA
    - MOU
    - ISA
- Considerações de privacidade
- Consciência dos riscos
- Compartilhamento de dados não autorizado
- Propriedade de dados
- Backups de dados
- Cumprimento das políticas e procedimentos de segurança
- Revisar os requisitos do contrato para garantir os padrões de conformidade e desempenho

2.3 Dado um cenário, implementar estratégias de mitigação de riscos apropriadas.

- Gestão de mudança
- Gestão de incidente
- Revisão de permissões e direitos do usuário
- Realizar auditorias de rotina
- Aplicar políticas e procedimentos para prevenir perda ou roubo de dados
- Aplicar controles tecnológicos
    - Prevenção de perda de dados (DLP)

2.4 Dado um cenário, implementar procedimentos forenses básicos.

- Ordem de volatilidade
- Capturar imagem do sistema
- Tráfego de rede e registros
- Capturar vídeo
- Fuso horário de gravação
- Geração hashes
- Capturas de tela
- Testemunhas
- Custos de serviço e despesa
- Cadeia de custódia
- Análise de Big Data

2.5 Resumir procedimentos comuns de resposta de incidente.

- Preparação
- Identificação do incidente
- Escalação e notificação
- Passos de mitigação
- Lições aprendidas
- Documentar
- Procedimentos de recuperação/reconstituição
- First Responder
- Isolamento do incidente
    - Quarentena
    - Remoção de dispositivos
- Violação de dados
- Controle de perdas e danos

2.6 Explicar a importância da conscientização e treinamento relacionados à segurança.

- Treinamento e em política de segurança e procedimentos de segurança
- Treinamento baseado em cenários
- Informações de Identificação Pessoal (PII)
- Classificação de informações
    - Alta
    - Média
    - Baixa
    - Confidencial
    - Privado
    - Público
- Etiquetagem, manuseio e descarte de dados
- Conformidade com leis, melhores práticas e padrões
- Hábitos do usuário
    - Comportamentos de senha
    - Manuseio de dados
    - Políticas de mesa limpa
    - Prevenir utilização não autorizada
    - Dispositivos de propriedade pessoal
- Novas ameaças e novas tendências/alertas de segurança
    - Novos vírus
    - Ataques de phishing
    - Explorações Zero-Day
- Uso de redes sociais e P2P
- Acompanhamento e coleta de métricas de treinamento para validar a conformidade e a postura de segurança

2.7 Determinar as semelhanças e diferenças entre controles físicos de segurança e ambientais.

- Controles ambientais
    - HVAC
    - Supressão de incêndio
    - Blindagem EMI
    - Corredores quente e frio
    - Monitoramento ambiental
    - Controles de temperatura e umidade
- Segurança física
    - Travas de hardware
    - Mantraps
    - Monitoramento em vídeo
    - Cerca
    - Leitores de proximidade
    - Lista de acesso
    - Iluminação adequada
    - Sinalização
    - Guardas
    - Barreiras
    - Biometria
    - Proteção do cabeamento
    - Alarmes
    - Detecção de movimento
- Tipos de controles
    - Desencorajador
    - Preventivo
    - Detectivos
    - Compensatório

    - Técnico
    - Administrativo

2.8 Resumir as boas práticas de gerenciamento de riscos.

- Conceitos de continuidade de negócios
    - Análise do impacto no negócio
    - Identificação de componentes e sistemas importantes
    - Removendo pontos únicos de falha
    - Planejamento e testes de continuidade de negócios
    - Avaliação de riscos
    - Continuidade de operações
    - Recuperação de desastres
    - Planejamento de contingência de TI
    - Planejamento de sucessão
    - Alta disponibilidade
    - Redundância
    - Testes de mesa
- Tolerância da falha
    - Hardware
    - RAID
    - Cluster
    - Balanceamento de carga
    - Servidores
- Conceitos de recuperação de desastre
    - Planos/políticas de backup
    - Execução/frequência de backup
    - Cold site
    - Hot site
    - Warm site

2.9 Dado um cenário, selecionar o controle apropriado para atender as metas de segurança.

- Sigilo
    - Criptografia
    - Controles de acesso
    - Esteganografia
- Integridade
    - Hash
    - Assinaturas digitais
    - Certificados
    - Não-repudio
- Disponibilidade
    - Redundância
    - Tolerância de falha
    - Patching
- Segurança
    - Cerca
    - Iluminação
    - Travas
    - CCTV
    - Planos de evacuação
    - Ensaios
    - Vias de evacuação
    - Controles de teste

3.0 Ameaças e vulnerabilidades

3.1 Explicar os tipos de malware.

- Adware
- Vírus
- Spyware
- Trojan
- Rootkits
- Backdoors
- Bomba lógica
- Botnets
- Ransomware
- Malware polimórfico
- Armored vírus

3.2 Resumiros diversos tipos de ataques.

- Man-in-the-middle
- DDoS
- DoS
- Replay
- Ataque Smurf
- Spoofing
- Spam
- Phishing
- Spim
- Vishing
- Spear phishing
- Xmas
- Pharming
- Escalação de privilégio
- Ameaça interna
- Envenenamento de DNS e envenenamento de ARP
- Acesso transitivo
- Ataques client-side
- Ataques a senhas
    - Força bruta
    - Ataques de dicionário
    - Híbrido
    - Ataques de aniversário
    - Rainbow tables
- Erros de digitação propositais/sequestro de URL
- Ataque watering hole

3.3 Resumir os ataques de engenharia social e a eficácia associada a cada ataque.

- Olhar sobre os ombros Shoulder surfing
- Dumpster diving
- Utilização não autorizada
- Personificação
- Hoaxes
- Whaling
- Vishing
- Princípios (motivos para eficácia)

- Autoridade
- Intimidação
- Consenso/prova social
- Escassez
- Urgência
- Familiaridade/preferência
- Confiança

3.4 Explicar os tipos de ataques a rede sem fio.

- Pontos de acesso maliciosos
- Jamming/interferência
- Evil twin
- War driving
- Bluejacking
- Bluesnarfing
- War chalking
- Ataque por vetor de inicialização
- Packet sniffing
- Comunicação a curta distância
- Ataques por repetição
- Ataques WEP/WPA
- Ataques WPS

3.5 Explicar os tipos de ataques a aplicativos.

- Cross-site scripting
- ISQL injection
- LDAP injection
- XML injection
- Command Injection/Directory path traversal
- Buffer overflow
- Integer overflow
- Zero-Day
- Cookies e anexos
- LSO (objetos localmente compartilhados)
- Flash Cookies
- Add-ons maliciosos
- Sequestro de sessão
- Manipulação de cabeçalho
- Execução de código arbitrário/execução de código remoto

3.6 Analisar um cenário e selecionar o tipo apropriado de técnicas de mitigação e desencorajamento.

- Monitorar logs de sistema
  - Logs de evento
  - Logs de auditoria
  - Logs de segurança
  - Logs de acesso
- Hardening
  - Desabilitar serviços desnecessários
  - Proteger interfaces e aplicativos de gerenciamento
  - Proteger por senha
  - Desabilitar contas desnecessárias
- Segurança de rede
  - Restrição e filtro de MAC

    - 802.1x
    - Desabilitar interfaces e portas de serviço não usadas
    - Detectar máquinas não autorizadas
- Postura de segurança
    - Configurar baseline inicial
    - Monitoramento contínuo de segurança
    - Remediação
- Relatórios
    - Alarmes
    - Alertas
    - Tendências
- Controles de detecção vs. controles de prevenção
    - IDS vs. IPS
    - CFTV vs. vigia

3.7 Dado um cenário, usar ferramentas de avaliação e técnicas apropriadas para descobrir ameaças de segurança e vulnerabilidades.

- Interpretar resultados de ferramentas de avaliação de segurança
- Ferramentas
    - Analisador de protocolo
    - Scanner de vulnerabilidade
    - Honeypots
    - Honeynets
    - Scanner de porta
    - Ferramentas passivas vs. ativas
    - Captura de banner
- Cálculos de risco
    - Ameaça vs. probabilidade
- Tipos de avaliação
    - Risco
    - Ameaça
    - Vulnerabilidade
- Técnica de avaliação
    - Relatório de baseline
    - Análise de código
    - Determinar superfície de ataque
    - Revisão de arquitetura
    - Revisão de designs

3.8 Explicar o uso adequado de testes de invasão em comparação com escaneamento de vulnerabilidades.

- Teste de invasão
    - Verificar se existe uma ameaça
    - Contornar controles de segurança
    - Testar ativamente controles de segurança
    - Explorar vulnerabilidades
- Escanear vulnerabilidade
    - Testar passivamente controles de segurança
    - Identificar vulnerabilidade
    - Identificar falta de controles de segurança
    - Identificar configurações incorretas comuns
    - Intrusivo vs. não intrusivo
    - Com credencial vs. sem credencial
    - Falso positivo
- Black box
- White box

- Gray box

4.0 Segurança de aplicativo, dados e host

4.1 Explicar a importância das técnicas e controles de segurança dos aplicativos.

- Fuzzing
- Conceitos de codificação segura
  - Tratamento de erro e exceção
  - Validação de entrada
- Prevenção de cross-site scripting
- Prevenção de Cross-site Request Forgery (XSRF)
- Baseline de configuração de aplicativo (ajustes adequados)
- Hardening de aplicativo
- Gerenciamento de patch de aplicativo
- Bancos de dados não SQL vs. SQL
- Validação server-side vs. client-side

4.2 Resumir as tecnologias e os conceitos de segurança móvel.

- Segurança do dispositivo
  - Criptografia total do dispositivo integral
  - Limpeza de dados remoto
  - Bloqueio de dispositivo
  - Bloqueio de tela
  - GPS
  - Controle de aplicativos
  - Segmentação de armazenamento
  - Rastreamento de ativos
  - Controle de inventário
  - Gerenciamento de dispositivos móveis
  - Controle de acesso a dispositivos
  - Armazenamento removível
  - Desabilitar recursos não usados
- Segurança dos aplicativos
  - Gerenciamento de chaves
  - Gerenciamento de credenciais
  - Autenticação
  - Geo-taggingGeo-tagging
  - Criptografia
  - White list de aplicativos
  - Confiança/autenticação transitiva
- Preocupações BYOD
  - Proprietário dos dados
  - Responsável pelo suporte
  - Gerenciamento de patch
  - Gerenciamento de anti-vírus
  - Procedimentos forenses
  - Privacidade
  - Procedimentos de Integração e desligamento
  - Adesão às políticas corporativas
  - Concordância do usuário
  - Considerações sobre arquitetura/infraestruturas
  - Aspectos jurídicos
  - Política de uso aceitável
  - Câmera/vídeo interno

4.3 Dado um cenário, selecionar a solução apropriada para estabelecer a segurança do host.

- Segurança do sistema operacional e configurações
- Hardening do SO
- Anti-malware
  - Antivírus
  - Anti-spam
  - Anti-spyware
  - Bloqueadores de pop-up
- Gerenciamento de patch
- White listing vs. Black listing de aplicativos
- SO confiável
- Firewalls baseados em host
- Detecção de intrusão baseada em host
- Segurança de hardware
  - Travas de cabo
  - Cofre
  - Armários com chave
- Baseline de software no host
- Virtualização
  - Snapshots
  - Compatibilidade de patch
  - Disponibilidade/elasticidade de host
  - Testes de controle da segurança
  - Isolamento de processos

4.4 Implementar os controles apropriados para garantir a segurança dos dados.

- Cloud storage
- SAN
- Gerenciamento de Big Data
- Encriptação de dados
  - Todo o disco
  - Banco de dados
  - Arquivos individuais
  - Mídia removível
  - Dispositivos móveis
- Dispositivos de criptografia baseada em hardware
  - TPM
  - HSM
  - Criptografia USB
  - Disco rígido
- Dados em trânsito, dados em repouso, dados em uso
- Permissões/ACL
- Políticas de dados
  - Eliminação
  - Descarte
  - Retenção
  - Armazenamento

4.5 Estabelecer as semelhanças e diferenças entre métodos para mitigar riscos de segurança em ambientes estáticos.

- Ambientes
  - SCADA
  - Embarcado (impressora, Smart TV, controle HVAC)

    - Android
    - iOS
    - Mainframe
    - Consoles de jogos
    - Sistemas de computação em veículos
- Métodos
    - Segmentação de redes
    - Camadas de segurança
    - Firewalls de aplicativos
    - Atualizações manuais
    - Controle da versão do firmware
    - Wrappers
    - Diversidade e redundância de controles

5.0 Controle de acesso e gerenciamento de identidade

5.1 Estabelecer semelhanças e diferenças entre a função e finalidade dos serviços de autenticação.

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- LDAP seguro

5.2 Dado um cenário, selecionar a autenticação, autorização ou controle do acesso apropriados.

- Identificação vs. autenticação vs. autorização
- Autorização
    - Least privilege
    - Segregação de tarefas
    - ACLs
    - Mandatory access
    - Discretionary access
    - Controle de acesso com base em regras
    - Controle de acesso com base em funções
    - Restrições de horas do dia
- Autenticação
    - Tokens
    - Cartão de acesso comum
    - Smart card
    - Autenticação multifator
    - TOTP
    - HOTP
    - CHAP
    - PAP
    - Single sign-on
    - Controle de acesso
    - Negação implícita
    - SO confiável
- Fatores de autenticação
    - Algo que você é
    - Algo que você tem
    - Algo que você sabe

    - Algum local em que você está
    - Algo que você faz
- Identificação
    - Biometria
    - Cartão de verificação de identificação pessoal
    - Nome de usuário
- Federação
- Confiança/autenticação transitiva

5.3 Instalar e configurar controles de segurança ao gerenciar contas, com base nas boas práticas.

- Mitigar problemas associados a usuários com múltiplas contas/funções e/ou contas compartilhadas
- Aplicação da política de conta
    - Gerenciamento de credenciais
    - Política de grupo
    - Complexidade da senha
    - Expiração
    - Recuperação
    - Desabilitar
    - Bloqueio
    - Histórico de senhas
    - Reutilização de senha
    - Comprimento da senha
    - Proibição de conta genérica
- Privilégios baseados em grupo
- Privilégios atribuídos ao usuário
- Revisão de acesso de usuário
- Monitoramento contínuo

6.0 Criptografia

6.1 Dado um cenário, aplicar conceitos gerais de criptografia.

- Simétrico vs. assimétrico
- Chaves de sessão
- Troca de chaves in-band vs.out of band
- Diferenças fundamentais e métodos de criptografia
    - Block vs. stream
- Criptografia de transporte
- Não-repudio
- Hash
- Troca de chave
- Esteganografia
- Assinaturas digitais
- Uso de tecnologias comprovadas
- Curva elíptica e criptografia quântica
- Chave temporária
- Perfect forward secrecy

6.2 Dado um cenário, usar métodos de processamento apropriados.

- WEP vs. WPA/WPA2 e chave pré-compartilhada
- MD5
- SHA

- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparativo de forças e desempenho de algoritmos
- Uso de algoritmos/protocolos com criptografia de transporte
    - SSL
    - TLS
    - IPSec
    - SSH
    - HTTPS
- Família de Cifras
    - Codificação forte vs. fraca
- Key stretching
    - PBKDF2
    - Bcrypt

6.3 Dado um cenário, usar uma PKI apropriada, gerenciamento de certificados e componentes associados.

- Autoridades certificadoras e certificados digitais
    - CA
    - CRLs
    - OCSP
    - CSR
- PKI
- Agente de recuperação
- Chave pública
- Chave privada
- Registro
- Key Scrow
- Modelos de confiança

ACRÔNIMOS CompTIA Security+

3DES – Triple Digital Encryption Standard

AAA – Authentication, Authorization, and Accounting

ACL – Access Control List

AES - Advanced Encryption Standard
AES256 – Advanced Encryption Standards 256bit
AH - Authentication Header
ALE - Annualized Loss Expectancy
AP - Access Point
API - Application Programming Interface
ASP - Application Service Provider
ARO - Annualized Rate of Occurrence
ARP - Address Resolution Protocol
AUP - Acceptable Use Policy
BAC – Business Availability Center
BCP – Business Continuity Planning
BIA- Business Impact Analysis
BIOS – Basic Input / Output System
BPA – Business Partners Agreement
BYOD – Bring Your Own Device
CA – Certificate Authority
CAC - Common Access Card
CAN - Controller Area Network
CAPTCHA- Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR- Corrective Action Report
CCMP – Counter-Mode/CBC-Mac Protocol
CCTV - Closed-circuit television
CERT – Computer Emergency Response Team
CHAP – Challenge Handshake Authentication Protocol
CIO-- Chief Information Officer
CIRT – Computer Incident Response Team
COOP – Continuity of Operation Planning
CP – Contingency Planning
CRC – Cyclical Redundancy Check
CRL – Certification Revocation List
CSR – Control Status Register
CSU – Channel Service Unit
CTO- Chief Technology Officer
DAC – Discretionary Access Control
DBA– Database Administrator
DDOS – Distributed Denial of Service
DEP – Data Execution Prevention
DES – Digital Encryption Standard
DHCP – Dynamic Host Configuration Protocol
DHE – Data-Handling Electronics
DHE - Diffie-Hellman Ephemeral

DLL - Dynamic Link Library
DLP - Data Loss Prevention
DMZ – Demilitarized Zone
DNAT – Destination Network Address Transaction
DNS – Domain Name Service (Server)
DOS – Denial of Service
DRP – Disaster Recovery Plan
DSA – Digital Signature Algorithm
DSL - Digital Subscriber line
DSU – Data Service Unit
EAP - Extensible Authentication Protocol
ECC - Elliptic Curve Cryptography
ECDHE – Elliptic Curve Diffie-Hellman Ephemeral
EFS – Encrypted File System
EMI – Electromagnetic Interference
ESN- Electronic Serial Number
ESP – Encapsulated Security Payload
FACL- File System Access Control List
FDE– Full Disk Encryption
FTP – File Transfer Protocol
FTPS – Secured File Transfer Protocol
GPG – Gnu Privacy Guard
GPO – Group Policy Object
GPS – Global Positioning System
GPU - Graphic Processing Unit
GRE - Generic Routing Encapsulation
HDD – Hard Disk Drive
HIDS – Host Based Intrusion Detection System
HIPS – Host Based Intrusion Prevention System
HMAC – Hashed Message Authentication Code
HOTP – HMAC based One Time Password
HSM – Hardware Security Module
HTML – HyperText Markup Language
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol over SSL
HVAC – Heating, Ventilation Air Conditioning
IaaS - Infrastructure as a Service
ICMP - Internet Control Message Protocol
ID – Identification
IDS – Intrusion Detection System
IKE – Internet Key Exchange
IM - Instant messaging
IMAP4 - Internet Message Access Protocol v4

IP - Internet Protocol
IPSEC – Internet Protocol Security
IR– Incident Response
IRC - Internet Relay Chat
IRP – Incident Response Procedure
ISA – Interconnection Security Agreement
ISP – Internet Service Provider
ISSO- Information Systems Security Officer
ITCP – IT Contingency Plan
IV - Initialization Vector
JBOD– Just a Bunch of Disks
KDC - Key Distribution Center
L2TP – Layer 2 Tunneling Protocol
LAN – Local Area Network
LDAP – Lightweight Directory Access Protocol
LEAP – Lightweight Extensible Authentication Protocol
MaaS- Monitoring as a Service
MAC – Mandatory Access Control / Media Access Control
MAC - Message Authentication Code
MAN - Metropolitan Area Network
MBR – Master Boot Record
MD5 – Message Digest 5
MOU – Memorandum of Understanding
MPLS – Multi-Protocol Layer Switch
MSCHAP – Microsoft Challenge Handshake Authentication Protocol
MTBF – Mean Time Between Failures
MTTR – Mean Time to Recover
MTTF – Mean Time to Failure
MTU - Maximum Transmission Unit
NAC – Network Access Control
NAT – Network Address Translation
NDA – Non-Disclosure Agreement
NFC– Near Field Communication
NIDS – Network Based Intrusion Detection System
NIPS – Network Based Intrusion Prevention System
NIST – National Institute of Standards & Technology
NOS – Network Operating System
NTFS - New Technology File System
NTLM – New Technology LANMAN
NTP - Network Time Protocol
OCSP – Online Certificate Status Protocol
OLA – Open License Agreement

OS – Operating System
OVAL – Open Vulnerability Assessment Language
P2P – Peer to Peer
PAC– Proxy Auto Configuration
PAM – Pluggable Authentication Modules
PAP – Password Authentication Protocol
PAT - Port Address Translation
PBKDF2 – Password Based Key Derivation Function 2
PBX – Private Branch Exchange
PCAP – Packet Capture
PEAP – Protected Extensible Authentication Protocol
PED - Personal Electronic Device
PGP – Pretty Good Privacy
PII – Personally Identifiable Information
PIV – Personal Identity Verification
PKI – Public Key Infrastructure
POTS – Plain Old Telephone Service
PPP - Point-to-point Protocol
PPTP – Point to Point Tunneling Protocol
PSK – Pre-Shared Key
PTZ – Pan-Tilt-Zoom
RA – Recovery Agent
RAD - Rapid application development
RADIUS – Remote Authentication Dial-in User Server
RAID – Redundant Array of Inexpensive Disks
RAS – Remote Access Server
RBAC – Role Based Access Control
RBAC – Rule Based Access Control
RC4 – RSA Variable Key Size Encryption Algorithm
RIPEMD – RACE Integrity Primitives Evaluation Message Digest
ROI – Return of Investment
RPO – Recovery Point Objective
RSA – Rivest, Shamir, & Adleman
RTO – Recovery Time Objective
RTP – Real-Time Transport Protocol
S/MIME – Secure / Multipurpose Internet Mail Extensions
SAML – Security Assertions Markup Language
SaaS - Software as a Service
SAN – Storage Area Network
SCADA – System Control and Data Acquisition
SCAP - Security Content Automation Protocol
SCEP- Simple Certificate Enrollment Protocol
SCSI - Small Computer System Interface

SDLC - Software Development Life Cycle
SDLM - Software Development Life Cycle Methodology
SEH – Structured Exception Handler
SHA – Secure Hashing Algorithm
SFTP – Secured File Transfer Protocol
SHTTP – Secure Hypertext Transfer Protocol
SIEM – Security Information and Event Management
SIM – Subscriber Identity Module
SLA – Service Level Agreement
SLE - Single Loss Expectancy
SMS - Short Message Service
SMTP – Simple Mail Transfer Protocol
SNMP - Simple Network Management Protocol
SOAP – Simple Object Access Protocol
SONET – Synchronous Optical Network Technologies
SPIM - Spam over Internet Messaging
SQL – Structured Query Language
SSD – Solid State Drive
SSH – Secure Shell
SSL – Secure Sockets Layer
SSO – Single Sign On
STP – Shielded Twisted Pair
TACACS+ – Terminal Access Controller Access Control System
TCP/IP – Transmission Control Protocol / Internet Protocol
TGT– Ticket Granting Ticket
TKIP - Temporal Key Integrity Protocol
TLS – Transport Layer Security
TOTP – Time-Based One-Time Password
TPM – Trusted Platform Module
TSIG – Transaction Signature
UAT - User Acceptance Testing
UEFI – Unified Extensible Firmware Interface
UDP- User Datagram Protocol
UPS - Uninterruptable Power Supply
URI- Uniform Resource Identifier
URL - Universal Resource Locator
USB – Universal Serial Bus
UTM- Unified Threat Management
UTP – Unshielded Twisted Pair
VDI – Virtualization Desktop Infrastructure
VLAN – Virtual Local Area Network
VoIP - Voice over IP
VPN – Virtual Private Network

VTC – Video Teleconferencing
WAF- Web-Application Firewall
WAP – Wireless Access Point
WEP – Wired Equivalent Privacy
WIDS – Wireless Intrusion Detection System
WIPS – Wireless Intrusion Prevention System
WPA – Wireless Protected Access
WPA2 – WiFi Protected Access 2
WPS – WiFi Protected Setup
WTLS – Wireless TLS
XML – Extensible Markup Language
XSRF- Cross-Site Request Forgery
XSS - Cross-Site Scripting

Sugerir equipamento de sala de aula para o equipamento da certificação Security+

- Roteador
- Firewall
- Access point
- Switch
- IDS/IPS
- Servidor
- Filtro de conteúdo
- Cliente
- Dispositivo móvel
- Concentrador de VPN
- Aparelho tudo-em-um
- Gerentes de segurança de empresas/conjunto SIEM
- Balanceador de carga

Peças sobressalentes/hardware
- Teclados, mouses
- Cabos de rede
- Monitores

Ferramentas
- Analisadores de WiFi

Software
- Backtrack
- Servidor proxy
- Kali/BackTrack
- Software de virtualização
- Aparelhos de virtualização
- Wireshark
- TCPdump
- NMAP

- OpenVAS
- Metasploit
- Backorifice
- Cain & Abel
- John the Ripper
- PF Sense
- Security Onion
- Roo
- Qualquer UTM

Outro

- Source Forge