



Exame A2 – CMCE (Caixa Mágica Certified Engineer)

O Exame A2 é um exame que visa avaliar o utilizador na perspectiva de segurança.

O curso Segurança e Administração de Redes aborda todos os tópicos.

Duração: 2h 00m

Tópico A2.1 – Políticas de Segurança

Políticas de segurança e ataques mais frequentes

Métodos de segurança

Engenharia Social

Descrição: O certificando deve compreender a definição de uma política de segurança fechada com serviços abertos e políticas abertas com serviços fechados. Deve estar a par do conceito: sql injection e buffer overflow. Deve compreender o objectivo das seguintes ferramentas: IDS (Intrusion Detection System), Auditor de Vulnerabilidades, Assinatura digital, Root kit. Deve conhecer o significado de Engenharia Social e alguma das abordagens mais utilizadas.

Ficheiros:

Terminologia / expressões: Hacking, cracking, firewall, DMZ, Sistemas de autenticação (Biométricos, dispositivos smartcard e password), ataque de força bruta, trojan (Cavalo de Tróia), sniffing, spoofing, bombas lógicas, trap doors, buffer overflow, SQL injection, exploits, internet worms, CERT,

Comandos, utilitários e aplicações:

Referências bibliográficas:

Tópico A2.2 – Routing e Firewall

Routing

Firewall (iptables)

Descrição: Deve compreender os conceitos base de routing: como circulam os pacotes numa rede e como são estabelecidas rotas. Deve possuir noções de firewall e a forma de em Linux e através de iptables definir políticas (accept, ou drop), partilha de ligações (SNAT / Masquerading) e Port forwarding (DNAT).

Ficheiros: /proc/sys/net/ipv4/ip_forward,

Terminologia / expressões: router, firewall, port forwarding, masquerading, rota, netfilter, table, chain, rul, policy

Comandos, utilitários e aplicações: ifconfig, route, iptables,

Referências bibliográficas:

Tópico A2.3 – Restrição de recursos

Gestão de utilizadores – restrições de acessos, recursos e serviços

QoS e TrafficShapping

Descrição: O certificando deve saber implementar uma racional gestão de largura de banda através de QoS e TrafficShapping em Linux.

Ficheiros:

Terminologia / expressões: Prioritização, Shapping, fila de espera, largura de banda, latência, qdiscs, Hierarchical Token Bucket (HTB),

Comandos, utilitários e aplicações: tc, iptables,



Referências bibliográficas:

Tópico A2.4 – Ferramentas de Segurança

Assinatura digital - Tripwire

Auditor de vulnerabilidades – Nessus

Scanner de portas – nmap

Actualização de software

Descrição: Saber utilizar as ferramentas de segurança para: assinar digitalmente e verificar a integridade de um ficheiro, auditar as vulnerabilidades de um computador de uma rede e fazer um scanning às portas abertas de um computador na rede. Deve conseguir actualizar o sistema com novas versões de software que corrijam vulnerabilidades existentes.

Ficheiros: /etc/tripwire/site.key, /etc/tripwire/twpol.txt

Terminologia / expressões:

Comandos, utilitários e aplicações: nmap, rpm, twadmin, tripwire, apt-get, cmupdate, nessus-mkcert, nessus-adduser, nessusd, nessus