Nozioni fondamentali sulla sicurezza (98-367)

Le competenze che vengono misurate. Questo esame misura le capacità di svolgere i compiti tecnici elencati in basso. Le percentuali indicano l'importanza di ciascun argomento principale sull'esame.

Comprendere gli Strati di Sicurezza

Comprendere i principi fondamentali di sicurezza.
Questo obiettivo può includere tra i vari argomenti: riservatezza, integrità, disponibilità; come minacce e e rischi influenzano i principi; principio del minimo privilegio; ingegneria sociale; superficie di attacco
• Comprendere la sicurezza fisica.
o Questo obiettivo può includere tra i vari argomenti: sicurezza del sito, sicurezza del computer, dispositivi rimovibili e unità, controllo di accesso, sicurezza dei dispositivi mobili; Accesso disabilitato localmente; keylogger
• Comprendere la sicurezza Internet
o Questo obiettivo può includere tra i vari argomenti: impostazioni del browser, zone; siti Web sicuri
• Comprendere la sicurezza wireless.
o Questo obiettivo può includere tra i vari argomenti: vantaggi e svantaggi dei tipi di sicurezza specifici; chiavi, SSID, filtri MAC

Comprendere la Sicurezza del Sistema Operativo

• Comprendere l'autenticazione degli utenti.
o Questo obiettivo può includere tra i vari argomenti: multifattoriale; smart card, RADIUS; Infrastrutture a chiave pubblica (PKI); capire la catena di certificati, dati biometrici; Kerberos e inclinazione del tempo; utilizzo di Esegui come per eseguire le funzioni amministrative, le procedure di reimpostazione della password
• Comprendere le autorizzazioni.
o Questo obiettivo può includere tra i vari argomenti: file; condivisione; registry; Active Directory; NTFS anziché FAT, attivare o disattivare l'ereditarietà, i comportamenti spostando o copiando file all'interno dello stesso disco o su un altro disco; più gruppi con autorizzazioni diverse ; permessi di base e autorizzazioni avanzate; assumere la proprietà; delega;
• Comprendere le politiche di password.
o Questo obiettivo può includere tra i vari argomenti: complessità delle password, blocco degli account, lunghezza della password; cronologia delle password; tempo tra le modifiche delle password; imporre l'utilizzo di politiche di gruppo; comuni metodi di attacco
• Comprendere le politiche di audit.
o Questo obiettivo può includere tra i vari argomenti: tipi di audit; ciò che può essere sottoposto a audit; abilitare l'audit; dove salvare i dati di audit; come proteggere le informazioni di audit
• Comprendere la crittografia.
o Questo obiettivo può includere tra i vari argomenti: EFS; in che modo le cartelle crittografate con EFS incidono su spostare / copiare i file, BitLocker (To Go), TPM, la crittografia basata su software; crittografia di MAIL , la firma e altri usi; VPN; chiave pubblica / chiave privata; algoritmi di cifratura; proprietà del certificato; servizi di certificazione; PKI / infrastruttura dei servizi di certificazione; dispositivi token
• Comprendere il malware.
o Questo obiettivo può includere tra i vari argomenti: overflow del buffer, worm, trojan, spyware;

Comprendere la Sicurezza della Rete

• Comprendere i firewall dedicati.
o Questo obiettivo può includere tra i vari argomenti: tipi di firewall hardware e loro caratteristiche; perché utilizzare un firewall hardware invece di un firewall software; MSC e UMT; ispezione stateful vs stateless
• Comprendere la Protezione di Accesso di Rete (NAP).
o Questo obiettivo può includere tra i vari argomenti: scopo del NAP, requisiti per NAP
• Comprendere l'isolamento della rete.
o Questo obiettivo può includere tra i vari argomenti: VLAN, routing, honeypot, DMZ, NAT, VPN, Ipsec, Isolamento del

Dominio e del Server.
• Comprendere il protocollo di protezione.
o Questo obiettivo può includere tra i vari argomenti: spoofing del protocollo; IPSec, tunneling; DNSsec; sniffing di rete; comuni metodi di attacco

Comprendere la sicurezza del Software

- • Comprendere la protezione del client.
  o Questo obiettivo può includere tra i vari argomenti: antivirus, User Account Control (UAC); sistema client mantenendo operativo e il software aggiornato; cifrare cartelle non in linea; Criteri di restrizione del software
  • Comprendere la protezione delle e-mail.
  o Questo obiettivo può includere tra i vari argomenti: antispam, antivirus, spoofing, phishing e pharming; protezione client vs protezione server; record SPF; record PTR
  • Comprendere la protezione del server.
  Questo obiettivo può includere tra i vari argomenti: la separazione dei servizi; hardening; mantenere aggiornato il server; aggiornamenti sicuri dinamici del DNS; disabilitare i protocolli di autenticazione non sicuri; Read-Only Domain Controllers, gestione separata di VLAN; Microsoft Baseline Security Analyzer (MBSA)