CCNA SECURITY

Okruhy na skúšku

Pozn. Číslo modulu v zátvorkách vychádza z obsahu v NetAcad kurze Network Security a z prednášok. Poradie okruhov je zhruba rovnaké ako poradie prednášok.

Okruh č. 1 (NetAcad Modul 2-4):

1) Popíšte typy útočníkov (*threat actors*).
2) Definujte rozdiely medzi *white, gray* a *black hat hacker*.
3) Uveďte a v krátkosti popíšte nástroje, ktoré využívajú zraniteľnosti siete.
4) Definujte pojem *malware*.
5) Uveďte a popíšte typy *malware*.
6) Popíšte tri hlavné kategórie sieťových útokov: prieskumnícke (*reconnaissance*) útoky, prístupové (*access*) útoky a DoS útoky.
7) Vysvetlite pojem triáda CIA v súvislosti s bezpečnosťou.
8) Ako je možné zmierniť prieskumnícke útoky (*reconnaissance attacks*)?
9) Ako je možné zmierniť útoky zamerané na prístup (*access attack*)?
10) Popíšte tri prístupy k implementácii smerovača na okraji siete (*edge router*): jeden smerovač (*single router*), *defense-in-depth*, DMZ.
11) Popíšte dodatočné prístupy k zabezpečeniu hesla na smerovači (napr. min. dĺžka hesla atď.).
12) Je MD5 naďalej bezpečné? Ak nie, aký iný algoritmus pre hashovanie hesiel by ste na smerovači použili (ak by bol dostupný)? Vysvetlite prečo.
13) Popíšte spôsoby ako je možné z bezpečnostného hľadiska zlepšiť proces prihlásenia sa na smerovač.

Okruh č. 2 (NetAcad Modul 5-7):

1) Aký je význam privilege úrovní (*priviledge levels*)?
2) Popíšte protokoly CDP a LLDP.
3) Aký je rozdiel medzi *in-band* a *out-of-band* manažmentom?
4) Popíšte Syslog a jeho funkcionalitu.
5) Popíšte NTP protokol a vysvetlite jeho význam.
6) Popíšte SNMP protokol.
7) Charakterizujte AAA koncept.
8) Kde a na čo sa používajú protokoly TACASC+ a RADIUS?
9) Popíšte serverovú AAA autorizáciu a účtovanie.

Okruh č. 3 (NetAcad Modul 8-10):

1) Aký je význam prístupových zoznamov? Popíšte rozdiel medzi štandardným a rozšíreným ACL.
2) Na čo slúži *wildcard* maska?
3) Popíšte IPv6 ACL.
4) Charakterizujte firewall.
5) Popíšte základné typy firewall: bezstavový (*packet filtering*) firewall, stavový firewall, *application gateway* firewall a NG firewall.
6) Definujte pojem DMZ.
7) Na čo slúži ZPF (*Zone-based Policy Firewall*)?
8) Aký je postup pri návrhu ZPF?

Okruh č. 4 (NetAcad Modul 11-12):

1) Charakterizujte útok typu *zero-day*.
2) Charakterizujte IPS a IDS systémy.
3) Popíšte dva typy IPS: hostový (*host-based*) IPS a sieťový (*network-based*).
4) Popíšte dva módy, v ktorých môže ISP/IDS fungovať: *promiscuous* mód a *inline* mód.
5) Popíšte SPAN.
6) Popíšte ISP signatúry.
7) Čo je Snort IPS?

Okruh č. 5 (NetAcad Modul 13-14):

1) Definujte pojem *netwrok access control*.
2) Charakterizujte 802.1X autentifikáciu.
3) Uveďte a popíšte niektoré typy útokov na prepínač.
4) Ako sa realizuje útok typu *MAC address table flooding*?
5) Čím je možné zmierniť útoky na MAC tabuľku?
6) Popíšte útok typu *VLAN hopping*.
7) Popíšte útok typu *VLAN double-tagging*.
8) Ako je možné zmierniť útoky typu *VLAN hopping*?
9) Charakterizujte privátne VLAN. Popíšte tri typy PVLAN rozhraní: *promiscuous*, *isolated* a *community*.
10) Popíšte dva typy DHCP útokov: *DHCP starvation* útok a *DHCP spoofing* útok.
11) Ako je možné zmierniť útok typu *DHCP spoofing*?
12) Popíšte *ARP spoofing*.
13) Ako je možné zmierniť *ARP spoofing* útok?
14) Popíšte útok na STP a spôsoby jeho zmiernenia.

Okruh č. 6 (NetAcad Modul 15-17):

1) Charakterizujte transpozičné a substitučné šifry.
2) Aké sú metódy rozlúštenia (*cracking*) hesiel?
3) Aký je rozdiel medzi kryptografiou a kryptoanalýzou?
4) Popíšte štyri prvky zabezpečenej komunikácie: integrita dát, autentifikácia zdroja, dôvernosť dát a nepopierateľnosť dát (*non-repudiation*).
5) Popíšte fungovanie hashovacej funkcie.
6) Charakterizujte HMAC.
7) Definujte pojmy dĺžka kľúča (*key length*) a *keyspace*.
8) Charakterizujte symetrické šifrovanie.
9) Charakterizujte asymetrické šifrovanie.
10) Popíšte fungovanie Diffie-Hellman algoritmu.
11) Čo je to a na čo sa používa digitálny podpis (*digital signature*)?
12) Charakterizujte PKI (*Public Key Infrastructure*) a uveďte jej použitie.

Okruh č. 7 (NetAcad Modul 18-19):

1) Aký je význam VPN?
2) Popíšte základné rozdiely medzi *site-to-site* a *remote-access* VPN.
3) Charakterizujte IPsec štandard.
4) Popíšte dva IPsec protokoly: AH (*Authentication Header*) a ESP (*Encapsulated Security Payload*)
5) Charakterizujte IKE protokol.