CCNA CYBEROPS

IT EDUCATION
CENTRE

1.0 Network Concepts

1.1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models
1.2 Describe the operation of the following
- 1.2.a IP
- 1.2.b TCP
- 1.2.c UDP
- 1.2.d ICMP

1.3 Describe the operation of these network services
- 1.3.a ARP
- 1.3.b DNS
- 1.3.c DHCP

1.4 Describe the basic operation of these network device types
- 1.4.a Router
- 1.4.b Switch
- 1.4.c Hub
- 1.4.d Bridge
- 1.4.e Wireless access point (WAP)
- 1.4.f Wireless LAN controller (WLC)

1.5 Describe the functions of these network security systems as deployed on the host, network, or the cloud:
- 1.5.a Firewall
- 1.5.b Cisco Intrusion Prevention System (IPS)
- 1.5.c Cisco Advanced Malware Protection (AMP)
- 1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security
- 1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security

1.6 Describe IP subnets and communication within an IP subnet and between IP subnets
1.7 Describe the relationship between VLANs and data visibility
1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices
1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation
1.10 Compare and contrast inline traffic interrogation and taps or traffic mirroring
1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring & NetFlow in the analysis of network traffic
1.12 Identify potential data loss from provided traffic profiles

2.0 Security Concepts

2.1 Describe the principles of the defense in depth strategy

2.2 Compare and contrast these concepts
- 2.2.a Risk
- 2.2.b Threat
- 2.2.c Vulnerability
- 2.2.d Exploit

2.3 Describe these terms
- 2.3.a Threat actor
- 2.3.b Run book automation (RBA)
- 2.3.c Chain of custody (evidentiary)
- 2.3.d Reverse engineering
- 2.3.e Sliding window anomaly detection
- 2.3.f PII
- 2.3.g PHI

2.4 Describe these security terms
- 2.4.a Principle of least privilege
- 2.4.b Risk scoring/risk weighting
- 2.4.c Risk reduction
- 2.4.d Risk assessment

- 2.5.b Mandatory access control
- 2.5.c Nondiscretionary access control

2.6 Compare and contrast these terms
- 2.6.a Network and host antivirus
- 2.6.b Agentless and agent-based protections
- 2.6.c SIEM and log collection

2.7 Describe these concepts
- 2.7.a Asset management
- 2.7.b Configuration management
- 2.7.c Mobile device management
- 2.7.d Patch management
- 2.7.e Vulnerability management

IT EDUCATION
CENTRE

3.0 Cryptography

3.1 Describe the uses of a hash algorithm\

3.2 Describe the uses of encryption algorithms

3.3 Compare and contrast symmetric and asymmetric encryption algorithms

3.4 Describe the processes of digital signature creation and verification

3.5 Describe the operation of a PKI

3.6 Describe the security impact of these commonly used hash algorithms
- 3.6.a MD5
- 3.6.b SHA-1
- 3.6.c SHA-256
- 3.6.d SHA-512

3.7 Describe the security impact of these commonly used encryption algorithms and secure communications protocols
- 3.7.a DES
- 3.7.b 3DES
- 3.7.c AES
- 3.7.d AES256-CTR
- 3.7.e RSA
- 3.7.f DSA
- 3.7.g SSH
- 3.7.h SSL/TLS

3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation

3.9 Describe these items in regards to SSL/TLS
- 3.9.a Cipher-suite
- 3.9.b X.509 certificates
- 3.9.c Key exchange
- 3.9.d Protocol version
- 3.9.e PKCS

IT EDUCATION CENTRE

4.0 Host-Based Analysis

4.1 Define these terms as they pertain to Microsoft Windows
- 4.1.a Processes
- 4.1.b Threads
- 4.1.c Memory allocation
- 4.1.d Windows Registry
- 4.1.e WMI
- 4.1.f Handles
- 4.1.g Services

4.2 Define these terms as they pertain to Linux
- 4.2.a Processes
- 4.2.b Forks
- 4.2.c Permissions
- 4.2.d Symlinks

4.2.e Daemon

4.3 Describe the functionality of these endpoint technologies in regards to security monitoring
- 4.3.a Host-based intrusion detection
- 4.3.b Antimalware and antivirus
- 4.3.c Host-based firewall
- 4.3.d Application-level whitelisting/blacklisting
- 4.3.e Systems-based sandboxing (such as Chrome, Java, Adobe reader)

4.4 Interpret these operating system log data to identify an event
- 4.4.a Windows security event logs
- 4.4.b Unix-based syslog
- 4.4.c Apache access logs
- 4.4.d IIS access logs

IT EDUCATION
CENTRE

5.0 Security Monitoring

5.1 Identify the types of data provided by these technologies
- 5.1.a TCP Dump
- 5.1.b NetFlow
- 5.1.c Next-Gen firewall
- 5.1.d Traditional stateful firewall
- 5.1.e Application visibility and control
- 5.1.f Web content filtering
- 5.1.g Email content filtering

5.2 Describe these types of data used in security monitoring
- 5.2.a Full packet capture
- 5.2.b Session data
- 5.2.c Transaction data
- 5.2.d Statistical data
- 5.2.f Extracted content
- 5.2.g Alert data

5.3 Describe these concepts as they relate to security monitoring
- 5.3.a Access control list
- 5.3.b NAT/PAT
- 5.3.c Tunneling
- 5.3.d TOR
- 5.3.e Encryption
- 5.3.f P2P
- 5.3.g Encapsulation
- 5.3.h Load balancing

5.4 Describe these NextGen IPS event types
- 5.4.a Connection event
- 5.4.b Intrusion event
- 5.4.c Host or endpoint event
- 5.4.d Network discovery event
- 5.4.e NetFlow event

5.5 Describe the function of these protocols in the context of security monitoring
- 5.5.a DNS
- 5.5.b NTP
- 5.5.c SMTP/POP/IMAP
- 5.5.d HTTP/HTTPS

6.0 Attack Methods

6.1 Compare and contrast an attack surface and vulnerability

6.2 Describe these network attacks
- 6.2.a Denial of service
- 6.2.b Distributed denial of service
- 6.2.c Man-in-the-middle

6.3 Describe these web application attacks
- 6.3.a SQL injection
- 6.3.b Command injections
- 6.3.c Cross-site scripting

6.5 Describe these endpoint-based attacks
- 6.5.a Buffer overflows
- 6.5.b Command and control (C2)
- 6.5.c Malware
- 6.5.d Rootkit
- 6.5.e Port scanning
- 6.5.f Host profiling

6.6 Describe these evasion methods
- 6.6.a Encryption and tunneling
- 6.6.b Resource exhaustion
- 6.6.c Traffic fragmentation
- 6.6.d Protocol-level misinterpretation
- 6.6.e Traffic substitution and insertion
- 6.6.f Pivot

6.7 Define privilege escalation

6.8 Compare and contrast remote exploit and a local exploit

IT EDUCATION
CENTRE