Website: WWW.AVTECHUSA.COM

CBROPS 200-201 + Security Ethical Hacking + 22 Hands-on Lab

Target Candidates:
Preferred candidates with minimum 2 years working experience in computer networking or degree in Computer Science, Information System, and Computer Engineering.

Course Description:
This course will provide students the complete understanding of cyber security and network forensics elements. The student will have understanding of Advance Persistent Threat (APT) and Tactics, Techniques, Procedures (TTP) and will be using tools, techniques and industry accepted methodologies. Student will get familiar with concepts of network security and forensics tools and how those concepts can be applied in securing organizational infrastructure.

CBROPS (200-201)

20% 1.0 Security Concepts			
	1.1 Describe the CIA triad		Mapped From SECOPS
	1.2 Compare security deployments		Mapped From SECFND
		1.2.a Network, endpoint, and application security systems	Mapped From SECFND
		1.2.b Agentless and agent-based protections	Mapped From SECFND
		1.2.c Legacy antivirus and antimalware	Mapped From SECFND
		1.2.d SIEM, SOAR, and log management	Mapped From SECFND (SOAR is New)
	1.3 Describe security terms		
		1.3.a Threat intelligence (TI)	New Item
		1.3.b Threat hunting	New Item
		1.3.c Malware analysis	Mapped From SECOPS
		1.3.d Threat actor	Mapped From SECFND
		1.3.e Run book automation (RBA)	Mapped From SECFND

		1.3.f Reverse engineering	Mapped From SECFND
		1.3.g Sliding window anomaly detection	Mapped From SECFND
		1.3.h Principle of least privilege	Mapped From SECFND
		1.3.i Zero trust	New Item
		1.3.j Threat intelligence platform (TIP)	New Item
	1.4 Compare security concepts		
		1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment)	Mapped From SECFND
		1.4.b Threat	Mapped From SECFND
		1.4.c Vulnerability	Mapped From SECFND
		1.4.d Exploit	Mapped From SECFND
	1.5 Describe the principles of the defense-in-depth strategy		Mapped From SECFND
	1.6 Compare access control models		
		1.6.a Discretionary access control	Mapped From SECFND
		1.6.b Mandatory access control	Mapped From SECFND
		1.6.c Nondiscretionary access control	Mapped From SECFND
		1.6.d Authentication, authorization, accounting	New Item
		1.6.e Rule-based access control	New Item
		1.6.f Time-based access control	New Item
		1.6.g Role-based access control	New Item
	1.7 Describe terms as defined in CVSS		
		1.7.a Attack vector	Mapped From SECOPS
		1.7.b Attack complexity	Mapped From SECOPS
		1.7.c Privileges required	Mapped From SECOPS
		1.7.d User interaction	Mapped From SECOPS
		1.7.e Scope	Mapped From SECOPS
	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection		New Item

	1.9 Identify potential data loss from provided traffic profiles		Mapped From SECFND
	1.10 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs		Mapped From SECOPS
	1.11 Compare rule-based detection vs. behavioral and statistical detection		New Item
25% 2.0 Security Monitoring			
	2.1 Compare attack surface and vulnerability		Mapped From SECFND
	2.2 Identify the types of data provided by these technologies		
		2.2.a TCP dump	Mapped From SECFND
		2.2.b NetFlow	Mapped From SECFND
		2.2.c Next-gen firewall	Mapped From SECFND
		2.2.d Traditional stateful firewall	Mapped From SECFND
		2.2.e Application visibility and control	Mapped From SECFND
		2.2.f Web content filtering	Mapped From SECFND
		2.2.g Email content filtering	Mapped From SECFND
	2.3 Describe the impact of these technologies on data visibility		
		2.3.a Access control list	Mapped From SECFND
		2.3.b NAT/PAT	Mapped From SECFND
		2.3.c Tunneling	Mapped From SECFND
		2.3.d TOR	Mapped From SECFND
		2.3.e Encryption	Mapped From SECFND
		2.3.f P2P	Mapped From SECFND
		2.3.g Encapsulation	Mapped From SECFND
		2.3.h Load balancing	Mapped From SECFND
	2.4 Describe the uses of these data types in security monitoring		

		2.4.a Full packet capture	Mapped From SECFND
		2.4.b Session data	Mapped From SECFND
		2.4.c Transaction data	Mapped From SECFND
		2.4.d Statistical data	Mapped From SECFND
		2.4.e Metadata	Mapped From SECFND
		2.4.f Alert data	Mapped From SECFND
	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle		Mapped From SECFND
	2.6 Describe web application attacks, such as SQL injection, command injections, and cross- site scripting		Mapped From SECFND
	2.7 Describe social engineering attacks		Mapped From SECFND
	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware		Mapped From SECFND
	2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies		Mapped From SECFND
	2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)		New Item
	2.11 Identify the certificate components in a given scenario		
		2.11.a Cipher-suite	Mapped From SECFND
		2.11.b X.509 certificates	Mapped From SECFND
		2.11.c Key exchange	Mapped From SECFND
		2.11.d Protocol version	Mapped From SECFND
		2.11.e PKCS	Mapped From SECFND
20% 3.0 Host-Based Analysis			
	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring		
		3.1.a Host-based intrusion detection	Mapped From SECFND
		3.1.b Antimalware and antivirus	Mapped From SECFND
		3.1.c Host-based firewall	Mapped From SECFND
		3.1.d Application-level whitelisting/blacklisting	Mapped From SECFND

		3.1.e Systems-based sandboxing (such as Chrome, Java, Adobe Reader)	Mapped From SECFND
	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario		Mapped From SECFND
	3.3 Describe the role of attribution in an investigation		
		3.3.a Assets	Mapped From SECOPS
		3.3.b Threat actor	Mapped From SECOPS
		3.3.c Indicators of compromise	New Item
		3.3.d Indicators of attack	New Item
		3.3.e Chain of custody	New Item
	3.4 Identify type of evidence used based on provided logs		
		3.4.a Best evidence	Mapped From SECOPS
		3.4.b Corroborative evidence	Mapped From SECOPS
		3.4.c Indirect evidence	Mapped From SECOPS
	3.5 Compare tampered and untampered disk image		New Item
	3.6 Interpret operating system, application, or command line logs to identify an event		Mapped From SECFND
	3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)		
		3.7.a Hashes	Mapped From SECOPS
		3.7.b URLs	Mapped From SECOPS
		3.7.c Systems, events, and networking	Mapped From SECOPS
20% 4.0 Network Intrusion Analysis			
	4.1 Map the provided events to source technologies		
		4.1.a IDS/IPS	Mapped From SECOPS
		4.1.b Firewall	Mapped From SECOPS
		4.1.c Network application control	Mapped From SECOPS
		4.1.d Proxy logs	Mapped From SECOPS
		4.1.e Antivirus	Mapped From SECOPS

		4.1.f Transaction data (NetFlow)	Mapped From SECOPS
	4.2 Compare impact and no impact for these items		
		4.2.a False positive	Mapped From SECOPS
		4.2.b False negative	Mapped From SECOPS
		4.2.c True positive	Mapped From SECOPS
		4.2.d True negative	Mapped From SECOPS
		4.2.e Benign	New Item
	4.3 Compare deep packet inspection with packet filtering and stateful firewall operation		Mapped From SECFND
	4.4 Compare inline traffic interrogation and taps or traffic monitoring		Mapped From SECFND
	4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic		Mapped From SECFND
	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark		Mapped From SECOPS
	4.7 Identify key elements in an intrusion from a given PCAP file		
		4.7.a Source address	Mapped From SECOPS
		4.7.b Destination address	Mapped From SECOPS
		4.7.c Source port	Mapped From SECOPS
		4.7.d Destination port	Mapped From SECOPS
		4.7.e Protocols	Mapped From SECOPS
		4.7.f Payloads	Mapped From SECOPS
	4.8 Interpret the fields in protocol headers as related to intrusion analysis		
		4.8.a Ethernet frame	Mapped From SECOPS
		4.8.b IPv4	Mapped From SECOPS
		4.8.c IPv6	Mapped From SECOPS
		4.8.d TCP	Mapped From SECOPS

		4.8.e UDP	Mapped From SECOPS
		4.8.f ICMP	Mapped From SECOPS
		4.8.g DNS	New Item
		4.8.h SMTP/POP3/IMAP	New Item
		4.8.i HTTP/HTTPS/HTTP2	Mapped From SECOPS
		4.8.j ARP	New Item
	4.9 Interpret common artifact elements from an event to identify an alert		
		4.9.a IP address (source / destination)	Mapped From SECOPS
		4.9.b Client and server port identity	Mapped From SECOPS
		4.9.c Process (file or registry)	Mapped From SECOPS
		4.9.d System (API calls)	Mapped From SECOPS
		4.9.e Hashes	Mapped From SECOPS
		4.9.f URI / URL	Mapped From SECOPS
	4.10 Interpret basic regular expressions		Mapped From SECOPS
15% 5.0 Security Policies and Procedures			
	5.1 Describe management concepts		
		5.1.a Asset management	Mapped From SECFND
		5.1.b Configuration management	Mapped From SECFND
		5.1.c Mobile device management	Mapped From SECFND
		5.1.d Patch management	Mapped From SECFND
		5.1.e Vulnerability management	Mapped From SECFND
	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61		Mapped From SECOPS
	5.3 Apply the incident handling process (such as NIST.SP800-61) to an event		Mapped From SECOPS
	5.4 Map elements to these steps of analysis based on the NIST.SP800-61		

		5.4.a Preparation	Mapped From SECOPS
		5.4.b Detection and analysis	Mapped From SECOPS
		5.4.c Containment, eradication, and recovery	Mapped From SECOPS
		5.4.d Post-incident analysis (lessons learned)	Mapped From SECOPS
	5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)		
		5.5.a Preparation	Mapped From SECOPS
		5.5.b Detection and analysis	Mapped From SECOPS
		5.5.c Containment, eradication, and recovery	Mapped From SECOPS
		5.5.d Post-incident analysis (lessons learned)	Mapped From SECOPS
	5.6 Describe concepts as documented in NIST.SP800-86		
		5.6.a Evidence collection order	Mapped From SECOPS
		5.6.b Data integrity	Mapped From SECOPS
		5.6.c Data preservation	Mapped From SECOPS
		5.6.d Volatile data collection	Mapped From SECOPS
	5.7 Identify these elements used for network profiling		
		5.7.a Total throughput	Mapped From SECOPS
		5.7.b Session duration	Mapped From SECOPS
		5.7.c Ports used	Mapped From SECOPS
		5.7.d Critical asset address space	Mapped From SECOPS
	5.8 Identify these elements used for server profiling		
		5.8.a Listening ports	Mapped From SECOPS
		5.8.b Logged in users/service accounts	Mapped From SECOPS
		5.8.c Running processes	Mapped From SECOPS
		5.8.d Running tasks	Mapped From SECOPS

		5.8.e Applications	Mapped From SECOPS
	5.9 Identify protected data in a network		
		5.9.a PII	Mapped From SECOPS
		5.9.b PSI	Mapped From SECOPS
		5.9.c PHI	Mapped From SECOPS
		5.9.d Intellectual property	Mapped From SECOPS
	5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion		Mapped From SECOPS
	5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)		New Item

Hands On Lab

1.0 Installing CyberOps Workstation Virtual Machine

2.0 Identify Running Process

3.0 Exploring Processes, Threads, Handles and Windows Registry

4.0 Getting Familiar with Linux Shell

5.0 Passive and Active Information Gathering

6.0 Port Scanning

7.0 Using Wireshark to Observe TCP 3-Way Handshake

8.0 Examine TCP, UDP, DNS, HTTP, HTTPS traffic

9.0 Encrypting and Decrypting Data Using OpenSSL

10.0 Hashing Thing out

11.0 CA Stores

12.0 Anatomy of Malware

13.0 Social Engineering

14.0 Password Attack

15.0 Metasploit Payload

16.0 Bypassing anti-virus

17.0 Attacking MySQL Database

18.0 Snort and Firewall Rules

19.0 Convert Data into a Universal Format

20.0 Interpret HTTP and DNS Data to Isolate Threat Actor

21.0 Isolate Compromised Host using 5-Tuple

22.0 Incident Handling