TAWG 1, Domains Risk Assessment and Risk Management Strategies

SIG 1 (LO 1748) Learning Objective **Understand the fundamentals of network and application vulnerability scanners, common commercial and open source tools, and how to defend against them.**

Certification Domain **Scanning: Network and Application Vulnerability scanning and tools**

Security+ - CompTIA Security+ (CompTIA)

Responsibility Area **Identify and mitigate vulnerabilities**

CONCEPTS

Access control
Access control threats
Advanced Persistent Threat
ARP poisoning
Attack prevention tools and techniques
Attacks against private-key ciphers
Backdoors
Bluejacking
Bluesnarfing
Buffer overflow
Certificate forgery
Compare and contrast alternative methods to mitigate security risks in in-vehicle computing systems
Compare and contrast alternative methods to mitigate security risks in iOS
Control system security testing (active and passive techniques)
Cookie and attachment attacks
Countermeasures
Credentialed vs. non-credentialed vulnerability scanning
Cross-site Request Forgery (XSRF) prevention
Cross-site scripting
Cross-site scripting prevention
Cyber asset vulnerabilities, access, and attack vector identification
Cyber threats, attacks, and mitigations to control systems
DDoS
Defensive techniques and measures
Dictionary attack
Differential attack
Directory traversal/command injection
Disable SSID broadcast
Disabling unused application service ports
Disabling unused interfaces
DoS
Flash cookies
Frequency-based attacks
HTTP
Hybrid attack
Identify common misconfigurations
Identify vulnerability
Identifying assets, threats, vulnerabilities, and consequences
Intrusive vs. non-intrusive vulnerability scanning
IV attack
LDAP injection
Linear attack

Location tracking

Malicious add-ons

Malware

Malware-based attack

Man-in-the-middle

Masquerading

Meet-in-the-middle attack

Mitigate issues associated with users with multiple account/roles and/or shared accounts

Network security

OS hardening

Passive vs. active threat/vulnerability discovery tools

Password cracking

Polymorphic malware

Port 22

Port 25

Port 443

Port 53

Port scanner

Power-consumption attacks

Privilege escalation

Protocol analyzer

Replay attack

Replay attacks

Review architecture to discover security threats and vulnerabilities

Review designs to discover security threats and vulnerabilities

Rogue access points

Rogue machine detection

Rootkits

Safe website identifers

Sandboxing

Session hijacking

Smurf attack

Spoofing

Tailgating

Vulnerabilities

Vulnerability scanner

WEP/WPA attacks

Wireless technology

Wiretapping

XML injection

TAWG 1, Domains Risk Assessment and Risk Management Strategies

SIG 2 (LO 1351) Learning Objective **Understand Penetration Testing *(PT)***

CEH - Certified Ethical Hacker (EC-Council)

Responsibility Area **Analyze security incidents**

CONCEPTS

Affidavits related to digital forensics
Attack classification
BYOD forensics
Cyber asset vulnerabilities, access, and attack vector identification
Effects of breaches in access control
Incident detection tools and techniques
Incident response
Log analysis
Malware inspection
Mobile forensics
Network log analysis
Off-line analysis
Pull-the-plug vs. triage
Reported alarms
Security auditing and analysis
Sources of digital evidence
Verify a threat exists
Virus

Responsibility Area **Exploit penetration targets**

CONCEPTS

Ethical hacking
Exploiting vulnerabilities
Timing attacks

Responsibility Area **Identify penetration targets and map attack vectors**

CONCEPTS

Brute force attack
Client-side attacks
Determine attack surface
DNS poisoning
Rainbow table attack
Threat vectors
WPS attacks
Xmas attack

TAWG 2, Domains: Awareness and Training and Business Environment

SIG 3 (LO 7682) Learning Objective **Explain the importance of security related awareness and training**

Certification Domain **Compliance and Operational Security**

Security+ - CompTIA Security+ (CompTIA)

Responsibility Area **Develop and manage personnel**

CONCEPTS

Acceptable use
Anticipatory ethics
BYOD user acceptance
Code of ethics
Cyber-hygiene
Ethics and Equity/Diversity
Human security factors
Introduction to control systems
Job rotation
Mandatory vacation
Professional ethics and codes of conduct
Reasons for social engineering attack effectiveness
Role-based training
Security policy training
Shoulder surfing
Social media networks and/or applications
Succession planning
Unauthorized data sharing
User behavior metrics

Responsibility Area **Manage process and procedures**

CONCEPTS

Acceptable use
Access control
Account credential management policy enforcement
Account expiration policy enforcement
Account lockout policy enforcement
Account password length policy enforcement
Administrative controls
Application patch management
Asset tracking
Audit benchmarks
Audit data collection methods
Audit plan
Business continuity planning and testing
BYOD acceptable use policy
BYOD adherence to corporate policies
BYOD legal concerns
Chain of custody
Change management
Cloud administration
Code review
Control system security policy
Control system security standards and compliance
Data backup methods

Data classification standards
Data disposing policy
Data erasure methods
Data in transit, data at rest, data in use
Data labeling, handling and disposal
Data loss/theft prevention policies and procedures
Data ownership
Data retention policy
Data storage policy
Data wiping policy
Database administration
Disaster Recovery Plan
Discretionary access
FERPA
Firmware version control
GDPR
Generic account prohibition policy enforcement
GLB compliance
GLBA Privacy Rule
HIPPA
Inventory control
ISO/IEC 27002
IT contingency planning
MOU
MTTR
National Institute of Standards and Technology (NIST)
On-boarding/off-boarding business partners
Operating System administration
OS system task automation
Preventive controls
Private data security litigation
Protecting management interfaces and applications
Recovery time objective
SOX compliance
Stored Communications Act
System process administration
US Cybersecurity Act of 2015
User access review

TAWG 2, Domains: Awareness and Training and Business Environment

SIG 4 (LO 1468) Learning Objective **Understand processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices**

Certification Domain **Information Systems Operations, Maintenance and Support**

CISA - Certified information Security Auditor (ISACA)

SSCP - Systems Security Certified Practitioner (ISC)2

Responsibility Area **Communicate results**

CONCEPTS

Post-audit activities

Reported trends

Responsibility Area **Manage security operations**

CONCEPTS

Access control

Access control lists

Access control, monitoring, and authentication

Account disablement policy enforcement

Account password history policy enforcement

Account password reuse policy enforcement

Account recovery policy enforcement

ACLs

Actively test security controls

AES

Anti-spam

Anti-spyware

Anti-virus software

Antivirus management

Application control

Architectural security and strategies

Attribute-based Access Control (ABAC)

Authenticated encryption

Authentication

Behavior-based NIDS/NIPS

Biometric authentication

Biometric identification

BYOD architecture/infrastructure considerations

BYOD on-board camera/video

BYOD on-boarding/off-boarding

BYOD Patch management

Certificate authority

Certificate transparency

Cold site

Common access card

Confidentiality

Configuration management

Content-Dependent Access Control

Continuity of operations

Continuous monitoring

Control system network security

Control system security for field devices and communications

Control systems security for applications

Control systems security for hosts

Credential management

Cryptographic tokens

Cyber physical system administration

Cyberspace operations

Data center security

Database security

Designing for security

Device access control

Disabling unnecessary accounts

Disabling unnecessary services

Disabling unused features on devices

Disaster recovery

Discretionary Access Control (DAC)

DLP

DMZ

Elements of security metrics

Encryption/Decryption

Fail-safe defaults

Federated identities and access control

FIPS

Firewall

Firewall rules

Flood guards

Full device encryption

Full disk data encryption

Group policy enforcement

Group-based privilege

Hard drive encryption

Hardware security

HIDS

High availability

History-based Access Control (HBAC)

Honeypot

Host isolation

Host patch management

Host-based firewalls

Hot site

HSM

HTTPS

Identification vs. authentication vs. authorization

Identity-based Access Control (IBAC)

Implicit deny

Incident management

Initial baseline configuration

IPSec

IPv6

ISO 17799

Kerberos

Key escrow

Key management

Knowledge-based authentication

Layered security/Defense in depth

LDAP

Least privilege

Lockout

Logical access control

MAC limiting and filtering

Management controls

Mandatory access

Mandatory Access Control (MAC)

Mobile device encryption

Mobile device management

Multifactor authentication

Network administration

Network firewall

Network security

Network segmentation

Network separation

Network switch

Non-Discretionary Access Control

Norm and rule violation

NTLM

NTLMv2

OCSP

One-time passwords

Operating system security and settings

Operational controls

Organization-based Access Control (OrBAC)

OS account management

OSI relevance

Passively testing security controls

Password complexity policy enforcement

Password iteration count

Password protection

Password storage

Patching

PCI/DSS

PEAP

Personal device tracking

Personal identification verification card

PGP/GPG

Physical access control

Physical data security

Physical security

Pop-up blockers

Port 143

Port 21

Port 3389

Port security

Privacy preserving protocols

Privacy settings

Private key

Proxies
Public key
Rack level security
RADIUS
Recovery point objective
Remote access
Remote wiping
Removable media encryption
Role-based Access Control (RBAC)
Router
Rule-based Access Control (RAC)
Rule-based management
Safety controls
SCP
Screen locks
Secret key (symmetric) cryptography
Secret sharing protocols
Secure architecture design
Secure LDAP
Secure router configuration
Security administration
Security layers
Security policy
Sender authentication
Separation of duties
Seven domains of a typical IT infrastructure
SFTP
SHA
Single sign-on
SLA
Smart card
SNMP
Spam
SSH
SSL
Stream cipher
Strong vs. weak ciphers
Supply chain security
Symmetric vs. asymmetric encryption
System hardening
System image capture
TACACS+
TCP/IP
Technical controls
Time of day restrictions
TLS
Transitive access
Transitive trust/authentication
Transport encryption
Transport-layer protocols
Trusted OS
Type and classifications of analytic tools and techniques

Unified threat management
URL filter
USB encryption
Use of algorithms/protocols with transport encryption
Use of proven technologies
User rights and permissions review
User-assigned privilege
Virtualization patch compatibility
Virtualization security control testing
VLAN management
Voice over IP (VoIP)
VPN (over open wireless)
VPN concentrator
Warm site
Web application firewall
Web security gateways
WEP
WEP vs. WPA/WPA2 and pre-shared key
Whitelisting vs. blacklisting applications
WPA
WPA2
XTACACS

TAWG 2, Domains: Awareness and Training and Business Environment

SIG 5 (LO 879) Learning Objective **Understand and align security function to goals, mission and objectives of the organization**

Certification Domain **Information Security Governance & Risk Management**

CISSP - Certified Information Systems Security Professional (ISC)2

Responsibility Area **Assess and manage risk**

CONCEPTS

Application hardening
Background of cybersecurity in control systems
Business impact analysis
BYOD Privacy
Calculating risk of threat vs. likelihood
Compare and contrast alternative methods to mitigate security risks in Android
Compare and contrast alternative methods to mitigate security risks in embedded systems
Compare and contrast alternative methods to mitigate security risks in game consoles
Compare and contrast alternative methods to mitigate security risks in mainframe
Compare and contrast alternative methods to mitigate security risks in SCADA
Control redundancy and diversity
Cyber Resilience Review self-assessment
Cyber threats, attacks, and mitigations to control systems
Cybersecurity Evaluation Tool (CSET)
Data integrity
Defensive techniques and measures
Detective controls
Deterrent controls
Handling Big Data
Identification of critical systems and components
Identify lack of security controls
Identity theft
Information classification
Insider threat
PII
Privacy policy
Probability/threat likelihood
Public cloud
Quantitative vs. qualitative risk
Removing single points of failure
Risk assessment
Risk avoidance, transference, acceptance, mitigation, deterrence
Risk awareness
Risk impact
Risk likelihood
Risk management
Risks associated with cloud computing and virtualization
Routine audits
Site surveys
SLE
Strategic implications of escalation and deterrence
SWOT Analysis
Threat assessment

Vulnerability assessment
War chalking
Wireless technology

TAWG 3, Domains Information Protection Processes and Procedures and Response Processes

SIG 6 (LO 1741) Learning Objective **Understand the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and "lessons learned" meetings.**

Certification Domain **Incident Handling: Recovering and Improving Capabilities**

GCIH - GIAC Certified Incident Handler (GIAC)

SSCP - Systems Security Certified Practitioner (ISC)2

Responsibility Area **Respond to intrusions**

CONCEPTS

Addressing privacy breaches

Digital forensics

Incident response

Zero-day exploits

Responsibility Area **Understand and demonstrate real-world impact of threats and vulnerabilities**

CONCEPTS

Botnet

Cyber terrorism

Cyber-assisted crimes

Cyber-focused crimes

Cybersecurity, privacy, and global human rights

Cyberspace as a sovereign domain

Global economic implications of cybersecurity

Global governance in cybersecurity

Implications of stolen root certificates

National economic implications of cybersecurity

Pharming

Phishing and social engineering

Ransomware

Spear phishing

Spyware

The dark web

Threat of free/open WiFi networks

Unethical hacking criminal penalties

Vishing

Whaling

Worm

TAWG 3, Domains Information Protection Processes and Procedures and Response Processes

SIG 7 (LO 1738) Learning Objective **Understand what incident handling is, why it is important, and the best practices to take in preparation for an incident**

Certification Domain **Incident Handling Overview and Preparation**

GCIH - GIAC Certified Incident Handler (GIAC)

SSCP - Systems Security Certified Practitioner (ISC)2

Certification Domain **IDS/IPS Management and Architecture Issues**

GCIA - GIAC Certified Intrusion Analyst (GIAC)

Responsibility Area **Log security incidents**

CONCEPTS

Cyber threats, attacks, and mitigations to control systems

Monitoring access logs

Monitoring audit logs

Monitoring event logs

Monitoring security logs

Network tracking

Reported alerts

Security monitoring

Responsibility Area **Implement security monitoring**

CONCEPTS

Anomaly-based NIDS/NIPS

Application firewall

Continuous security monitoring

Heuristic NIDS/NIPS

Host-based intrusion detection

IDS

IDS vs. IPS

Intrusion Detection System (IDS)

Intrusion Protection System (IPS)

Network security

Network traffic analysis

OS performance monitoring

Security monitoring

Signature-based NIDS/NIPS

Web traffic tracking

Wireless technology