GIAC Security Leadership Certificate (GSLC)

Length: 5 Days

Summary: The GIAC Security Leadership Certification (GSLC) is an intermediate skill level certification and covers topic areas including security management, cryptography, incident handling, web security and vulnerability management.

Course Objectives: Upon completion of this course, students will have learned how to demonstrate competency in the following areas:

- ✓ Cryptographic Applications
- ✓ Cryptography Concepts for Managers
- ✓ Incident Response and Business Continuity
- ✓ Managing a Security Operations Center
- ✓ Managing Application Security
- ✓ Managing Negotiations and Vendors
- ✓ Managing Projects
- ✓ Managing Security Architecture
- ✓ Managing Security Awareness
- ✓ Managing Security Policy
- ✓ Managing System Security
- ✓ Managing the Program Structure
- ✓ Network Monitoring for Managers
- ✓ Network Security and Privacy
- ✓ Networking Concepts for Managers
- ✓ Risk Management and Security Frameworks
- ✓ Vulnerability Management

Who Should Attend: Security Professionals with managerial or supervisory responsibility for information security staff.

Prerequisites: None

COURSE CONTENT

802.11

- Airborn viruses (ie. Cabir)
- Securing and Protecting wireless best practices
- Security Technologies (WPA, 802.11i, 802.1x, and EAP)
- Types of wireless and their frequencies
- WEP Weaknesses
- Wireless Threats (Eavesdropping, Wardriving, Masquerading, DoS, Rogue AP)

ACCESS CONTROL AND PASSWORD MANAGEMENT

- Access control models (DAC, MAC, RBAC)
- Best Practices (implicit deny, least privilege, separation of duties, job rotation)
- Centralized Access Control Technologies (Active directory, RADIUS)
- Fundamentals of Biometrics
- Password cracking
- Passwords, Hashes and limitations of windows hashes
- Strong Password Policy (what it is and why it's needed)
- Terminology (identity, authentication, authorization, least privilege, need to know, separation of duties, rotation of duties, data owner, single sign on)

BUILDING A SECURITY AWARENESS PROGRAM

- General approach to training
- Know what NIST SP 800 - 50 is
- Metrics for Security Awareness Programs
- Security Awareness Goals (changing user behavior)

BUSINESS SITUATIONAL AWARENESS

- Budgeting Approaches (top down, bottom up, negotiated, devolving)
- Factors that reduce business situational awareness
- Several important objectives: employees with 20 objectives are not accountable
- Temet Nosce: know your strengths and weaknesses
- Time Management
- To align security with the needs of the business, you must know company financials and products, you must know the business

CHANGE MANAGEMENT AND SECURITY

- Implementing change management
- Indicators of change management problems
- Relationship between undocumented changes and network instability
- Repeatable builds
- Tracking unplanned work

COMPUTER AND NETWORK ADDRESSING

- Broadcast addresses
- CIDR Addressing
- IP addresses and Subnet masks (network and host portion)
- MAC Addresses and OUIs (MACs built into NIC, only last for one hop)
- Private Addresses Strongly Recommended

CRYPTOGRAPHY ALGORITHMS AND CONCEPTS

- AES
- Concepts in crypto (computational complexity, intractable problems, public scrutiny)
- Crypto Attacks (known plaintext, chosen plaintext, adaptive chosen plaintext, ciphertext only, chosen ciphertext, chosen key)
- DES (56 bit key space considered insecure, symmetric block cipher)
- ECC usage and vulnerabilities
- Quantum cryptography concepts
- RSA vs. DES (asymmetric vs. Symmetric) characteristics

CRYPTOGRAPHY APPLICATIONS, VPNS AND IPSEC

8. Client and Server Side Certificate uses
9. Encrypting and Decrypting email with PGP
10. IPSEC Headers (AH and ESP)
11. IPSEC modes (transport and tunnel)
12. Key Management (public key distribution, private key storage)
13. PKI CA Hierarchy
14. PKI Problems (revocation is biggest issue)
15. PPP Basics
16. VPN components and placement issues
17. VPN technologies (SSL, SSH)
18. VPN types (site to site, client VPN)
19. Web of Trust (such as Linkedin, Facebook or people you know)

CRYPTOGRAPHY FUNDAMENTALS

9. Depend on secrecy of the key NOT the algorithm
10. Key management is weakest link
11. OPSEC problems (ie. Enigma Purple defeated by poor operations)
12. ROT-13
13. Stream and block cipher characteristics
14. Techniques must be combined carefully to produce strong crypto (substitutation, permutation, hybrid)
15. XOR operations

DEFENSE-IN-DEPTH

10. Architectural Process, zones, checkpoints
11. Information-centric DiD
12. Protected Enclaves DiD
13. Risks Associated with Connecting USB or Portable Devices or Using Them as Copying Devices
14. Role Based Access Control
15. Security Architect
16. Terminology (risk, threat, attack surface)
17. Uniform Protection DiD (least important type)
18. Vector Oriented DiD

DEFENSIVE OPSEC

11. 3 key laws of OPSEC
12. Employee issues (monitoring, screening, agreements, need to know, least privilege)
13. OPSEC Defined
14. Sensitive information (labeling, handling, and access)

DISASTER RECOVERY / CONTINGENCY PLANNING

11. BCP (definition and components)
12. Business Impact Analysis
13. DRP (definition and components)
14. Key Elements of continuity planning
15. Top BCP/DRP Planning Mistakes

DNS

12. Cache Poisoning - dangers of attacker controlling namespace
13. Cybersquatting
14. Domain Hijacking -- procedural and technical controls to prevent
15. gethostby name and gethostbyaddr
16. Hierarchy
17. Host Table (how it can be used against you or to protect you)
18. Nslookup forward and reverse lookups
19. Protecting Domain Names
20. Uses and misuses of the HOSTS table

ENDPOINT SECURITY

- 3rd party applications - ie. Secunia PSI
- Anti-virus has reached its limit
- Browser defense, plugins, testing
- Endpoint White list
- Risks associated with connecting USB or Portable devices, or using them as copying devices

FACILITIES AND PHYSICAL SECURITY

- Cooling, Hot Spots
- Detection of unauthorized access
- Lock types (traditional, cipher lock, magnetic cards, smart cards, biometric)
- Physical Security basics
- Power Basics
- Smoke and Fire basics - detective and suppressive controls

GENERAL TYPES OF CRYPTOSYSTEMS

- Goals of each type of crypto system (CIA + non-repudiation)
- One way hash functions
- Public Key Crypto (Asymmetric/two key crypto)
- Secret Key Crypto (symmetric/one key crypto)

HONEYPOTS, HONEYNETS, HONEYTOKENS, TARPITS

- Benefits and Drawbacks of using Honeypots
- Honeypots defined and types (host, network, service, honey token)
- Legal Issues
- Technologies (Virtualization, honeynet project, labrea tarpit)

INCIDENT HANDLING AND THE LEGAL SYSTEM

- Chain of Custody
- Evidence collection (real, direct, best, relevant, reliable, integrity, sign and seal)
- Search and Seizure (with and without a warrant)
- Types of laws (regulatory, criminal, civil)
- US Title 18 Section 30

INCIDENT HANDLING FOUNDATIONS

- Common Incident Handling Mistakes
- Containment Phase - how to contain the incident in detail (make a backup)
- Detecting and recognizing incidents (if you detect zero, maybe you are not recognizing incidents)
- Identification Phase - steps to recognize an incident in detail
- Incident Handling and Incidents defined
- Preparation Phase - how to in detail
- Six Step Incident Handling Process Defined

INFORMATION WARFARE

- Asymmetry
- Currency Destabilization
- Cybermilitia
- Malicious Code Blitz
- Perception Management
- Predictable Response

IP TERMINOLOGY AND CONCEPTS

- Application Layer Security Protocols
- Encapsulation
- ICMP
- IP and Important Fields
- Packets vs Frames
- Ping, Traceroute/Tracert and their uses
- Server and Client Ports
- Sniffers
- TCP 3 Way Handshake and connection establishment
- UDP
- What is a network protocol

LOGGING

- Raid 5, raid 10
- Syslog
- Thin and fat events, referential data

MALICIOUS SOFTWARE

- Malicious Browser Content and Hybrid Threats (browser was never designed to be a security gateway)
- Malware Defense Techniques
- Propagation techniques
- Trojan Horse characteristics
- Virus types and characteristics (require user action to spread)
- Worm characteristics (does not require user action to spread)

MANAGER'S GUIDE TO ASSESSING NETWORK ENGINEER

- Ask them about embedded protocol and to read the fields
- Done at job interview
- Give them the handout and sample packet
- You have the "teacher's edition" to check their work

MANAGERIAL WISDOM

- Key Concepts from Good to Great (First Who, then What, Hedgehog Concept, Flywheel, Level 5 leader)
- Know the 7 Habits of Highly Effective People

MANAGING ETHICS

- 48 laws of power (concept of amorality: win at any cost)
- Ethical Leadership (managers)
- Ethics Terminology (Ethics, Morals, Policy, Laws, Culture)
- Seven Signs of Ethical Collapse

MANAGING INTELLECTUAL PROPERTY

- Attacks on IP (insider threats, cybersquatting)
- Copyrights (defined, fair use, attacks, defenses)
- Digital Rights Management (Sony XCP, CSS)
- DMCA
- How to protect IP (NDA, non-compete, need-to-know, control publicly released info, label information, monitor outgoing traffic, watermarks, Internet searches, best practices)
- Intellectual Property Valuation
- IP defined
- Patents
- Trade secrets and know how (defined, how to identify)
- Trademarks and Service marks (defined, registration, attacks)

MANAGING IT BUSINESS AND PROGRAM GROWTH IN A GLOBALIZED MARKETPLACE

- 2050 largest economy
- 5 specific cultural points (such as shaking hands)
- Four Ps of Marketing (product, price, promotion, position)
- Key Business Concepts (continuous process improvement, strategic and disruptive innovation)
- Location (physical and virtual)
- Potential barriers to global communication and business
- Three Cs (customer, cost, community)
- Value Added Tax (VAT defined and benefits)

MANAGING LEGAL LIABILITY

- Best Practices for Managing Liability
- Common Damages
- Downstream liability and contributory negligence (related to DiD and due diligence)
- Indicators of Fraud
- Types of Fraud (internal, customer, credit card, accounting, telecom, etc)
- Zublake standard and eDiscovery

MANAGING NEGOTIATIONS

- Negotiation Keys (internalization, change, authority, price vs value, speed, walking away)
- Distributive Bargaining (BATNA, ZOPA, claiming value, anchoring point)
- Good negotiation is win-win.
- Integrative Bargaining (principled, mutual gains, win-win)

MANAGING PDA INFRASTRUCTURE

- Centralized Management versus Individual Device Management
- Security Threats
- Synchronization

MANAGING PRIVACY

- OECD Privacy Principles
- Personally Identifiable Information (PII)
- Privacy Certifications as proof of due diligence (TRUSTe, WebTrust, BBB Online Privacy Seal)
- Significant privacy cases

MANAGING SECURITY POLICY

- Issue-specific policy
- Policy assessment -SMART
- Policy Benefits
- Policy development tools (standards, guidelines, frameworks, mission statement)
- Security Posture and Culture

MANAGING SOFTWARE SECURITY

- Architectural Issues
- Best Practices (safe defaults, modular code, user accountability, error handling)
- Code Review (Manual, Automated, Hybrid, SDLC Integration)
- Understand basics of common implementation flaws at a high level

MANAGING TECHNICAL PEOPLE

- E-mail (business record, retention policy, when to use other comms)
- Encouraging Closure of projects
- Integrity
- Listening to and understanding technical people
- Meeting best practices
- Understand the power dynamic between technical staff and management
- Value of Metrics

MANAGING THE MISSION

- Doctrine
- Goals
- Mission Statement
- Vision Statement

MANAGING THE PROCUREMENT PROCESS

- Difference between price and value
- Negotiating with vendors (vendor honesty and key negotiating points)
- Product Support and Outsourcing
- Trade Show Tips
- Vendor and Product Selection, Ricochet Response

MANAGING THE TOTAL COST OF OWNERSHIP

- Direct costs and Indirect costs
- Depreciation (straight line, sum of years)
- SDLC disposal phase (grave costs)
- TCO (defined, how to calculate)

METHODS OF ATTACK

- Browsing, Enumeration, and Traffic Analysis
- Buffer Overflow key concepts
- Denial of Service (centralized p2p, distributed, physical) (basic forms: resource exhaustion , unexpected value, physical disruption, configuration disruption)
- Google hacking database and Goolag
- Infrastructure attacks (satellite, undersea cables, fiber optic trunks)
- Logic bombs and the Duronio case
- Malicious Code (Trojan horses and trapdoors)
- MITM and Replay attacks

- Phishing and spear phishing
- Physical Attacks
- Race conditions (timing attackes)
- Rootkits
- SPAM and e-mail flooding

MITNICK-SHIMOMURA

- IP address spoofing
- Disable defenses
- DoS so legitimate IP does not alert
- Sequence number prediction

OFFENSIVE OPSEC

- Competitive intel tools and features (whitepages.com, whois.net, nslookup, tracert, geobytes, wayback machine, Dun and Bradstreet)
- Differentiate between espionage and competitive intelligence
- Info on Individuals (google, intelius, credit reporting)
- Key Google searching techniques (ext, intitle, site, link, cache, related, inanchor, info)
- Limiting publicly available info (email and web)
- Sources for researching corporate information
- Using press releases

PROJECT MANAGEMENT FOR SECURITY LEADERS

- Closing out
- Monitor, Control, Conflict Resolution, Change Management
- Phases of project management
- Project Management Terms
- Staying on top of execution is key to bringing tasks to close

QUALITY

- Deming out of crisis
- DemingÕs 14 points
- Process Improvement

RISK MANAGEMENT AND AUDITING

- Acceptable Risk (who decides)
- Acting on the risk (accept, mitigate, transfer, avoid)
- Analysis types (SWOT, Cost Benefit, Weakness Gap, Threat Gap)
- Best Practices (templates, group policy, hotfixes, www.cisecurity.org, etc.)
- Briefing Management
- Calculating Annualized Loss Expectancy (ALE)
- Calculating Single Loss Expectancy (SLE)
- Difference between qualitative and quantitative approaches
- Terminology (Risk, threat, vulnerability, SDLC)
- Types of Risk

SAFETY

- Evacuation preparation and procedures
- Safety first, security second
- Safety walkthrough

SECURITY AND ORGANIZATIONAL STRUCTURE

- Capacity analysis and methods for increasing capacity
- Employee discipline and termination
- Employee performance (measuring, diagnosing causes of failure)
- Employee retention, compensation, and promotion
- Filling positions (requirements, hiring, interviews, 1099)

- Potential conflict of interest for CISO/CSO to report to CIO

SECURITY FRAMEWORKS

- Cobit
- ISO 27001/27002 (formerly ISO 17799) defined
- Understand security's relationship to the organizations mission

SELLING SECURITY

- Selling A Security Program to upper management
- Strategic Information Systems Plan

STEGANOGRAPHY

- Differences between steganography and cryptography and why detection is more difficult
- Methods (injection, substitution, file generation)
- Steganalysis

THE INTELLIGENT NETWORK

- Basic troubleshooting (troubleshooting UTM)
- Data Normalization
- Firewall types and the default rule
- HIPS and NIPS basics
- Ingress/Egress filtering
- IPS and IDS basics, alert types, and importance of detection
- Managing NIDS Costs (deployment and maintenance)
- Signature Analysis, Anomaly Analysis, and Application/Protocol Analysis
- Type 1 and Type 2 Virtualization
- Unified Threat Management (features, drawbacks, selection criteria)

THE NETWORK INFRASTRUCTURE

- Logical and physical topologies
- Network Components
- Network segmentation
- TCP Model
- The OSI Model (frequently used in troubleshooting)
- VLANs and how they support Defense In Depth
- VOIP Basics, Security Implications, availability issues, and threats

VULNERABILITY MANAGEMENT - INSIDE VIEW

- CISecurity.org
- Inside view, tools, approach

VULNERABILITY MANAGEMENT - OUTSIDE VIEW

- Basic Hacker Process
- Exploitation tools versus vulnerability scanners
- How to do a scan, process, dos and don'ts
- Inside view, outside view, user view
- Manager's role in prioritizing remediation
- Risk of not remediating after knowing about vulnerability
- Role of penetration testing in vulnerability management
- Scanning techniques (port, stealth, tcp/udp, passive)
- Threat Concerns
- Threat Vectors - relation to DiD
- Why war dialing is still important, tools

VULNERABILITY MANAGEMENT - USER VIEW

- Awareness and Inoculation
- P2P and IM dangers and controls
- Social Engineering

WEB COMMUNICATIONS AND SECURITY

- CGI and State/Cookie basics
- Cross Site Scripting
- HTTPS security misconceptions
- JavaScript Object Nation
- Protocol basics (HTTP and HTTPS)
- Proxy modification of cookies
- SOA (Exposes business logic)
- SQL Injection (stored procedures and input validation to mitigate)

WIRELESS ADVANTAGES AND BLUETOOTH

- Attacks (bluesnarf, bluejack, sniffing)
- Bluetooth defenses (non-discoverable mode, auditing, pairing in trusted environment, strong PINS)
- Bluetooth protocol fundamentals (PIN, discovery mode)
- Wireless Advantages