Certified Vulnerability Assessor

Código: CVA-001

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 24 Horas

El curso “Certified Vulnerability Assessor” ayuda a los estudiantes a entender la importancia de la evaluación de vulnerabilidades.
Brinda habilidades y conocimientos especiales en evaluaciones de vulnerabilidades. Prepara al estudiante para aplicar estos conocimientos, y practicar estas habilidades en el interés de los demás. Ayuda a entender la importancia de la evaluación de vulnerabilidades y como puede ayudar a prevenir importantes intromisiones a su empresa.

AUDIENCIA

Este curso está dirigido a:

- Organizadores de Sistemas de Información
- Analistas
- Ethical Hackers
- ISSO’s
- Gestores de Seguridad Cibernética
- Ingenieros informáticos

PRE REQUISITOS

- Comprensión básica de redes

OBJETIVOS

- Identifique cualquier defecto esencial en los marcos que podrían permitir el acceso a intrusos digitales
- Describir y redactar una evaluación de vulnerabilidad
- Base de datos de evaluación de vulnerabilidades Implementación
- Capacitación e instrucción de líderes para administradores de sistemas

CERTIFICACIÓN DISPONIBLE

- Certificación oficial de **COGNOS**.

CONTENIDO

1.39. COST OF A COUNTERMEASURE
1.40. CAN YOU GET RID OF ALL RISK?
1.41. MANAGEMENT'S RESPONSE TO IDENTIFIED RISKS
1.42. LIABILITY OF ACTIONS
1.43. POLICY REVIEW (TOP-DOWN)
1.44. METHODOLOGY
1.45. DEFINITIONS
1.46. POLICY TYPES
1.47. POLICIES WITH DIFFERENT GOALS
1.48. INDUSTRY BEST PRACTICE STANDARDS
1.49. COMPONENTS THAT SUPPORT THE
1.50. SECURITY POLICY
1.51. POLICY CONTENTS
1.52. WHEN CRITIQUING A POLICY
1.53. TECHNICAL (BOTTOM-UP)
1.54. METHODOLOGY
1.55. REVIEW

2. MODULO 2 - VULNERABILITY TYPES

2.1. OVERVIEW
2.2. CRITICAL VULNERABILITIES
2.3. CRITICAL VULNERABILITY TYPES
2.4. BUFFER OVERFLOWS
2.5. URL MAPPINGS TO WEB APPLICATIONS
2.6. IIS DIRECTORY TRAVERSAL
2.7. FORMAT STRING ATTACKS
2.8. DEFAULT PASSWORDS
2.9. MIS CONFIGURATIONS
2.10. KNOWN BACKDOORS
2.11. INFORMATION LEAKS
2.12. MEMORY DISCLOSURE
2.13. NETWORK INFORMATION
2.14. VERSION INFORMATION
2.15. PATH DISCLOSURE
2.16. USER ENUMERATION
2.17. DENIAL OF SERVICE
2.18. BEST PRACTICES
2.19. REVIEW
2.20. LAB

3. MODULO 3 - ASSESSING THE NETWORK

3.1. OVERVIEW
3.2. NETWORK SECURITY ASSESSMENT
3.3. PLATFORM
3.4. VIRTUALIZATION SOFTWARE

3.5. OPERATING SYSTEMS
3.6. EXPLOITATION FRAMEWORKS
3.7. INTERNET HOST AND NETWORK
3.8. ENUMERATION
3.9. QUERYING WEB & NEWSGROUP
3.10. SEARCH ENGINES
3.11. FOOTPRINTING TOOLS
3.12. BLOGS & FORUMS
3.13. GOOGLE GROUPS/USENET,
3.14. HACKING
3.15. GOOGLE AND QUERY OPERATORS
3.16. DOMAIN NAME REGISTRATION
3.17. WHOIS, WHOIS OUTPUT
3.18. BGP QUERYING
3.19. DNS DATABASES
3.20. USING NSLOOKUP
3.21. DIG FOR UNIX / LINUX
3.22. WEB SERVER CRAWLING
3.23. AUTOMATING ENUMERATION
3.24. SMTP PROBING
3.25. NMAP: IS THE HOST ON-LINE
3.26. ICMP DISABLED?
3.27. NMAP TCP CONNECT SCAN
3.28. TCP CONNECT PORT SCAN
3.29. TOOL PRACTICE: TCP
3.30. HALF-OPEN & PING SCAN
3.31. HALF-OPEN SCAN
3.32. FIREWALLED PORTS
3.33. NMAP SERVICE VERSION DETECTION
3.34. ADDITIONAL NMAP SCANS
3.35. NMAP UDP SCANS
3.36. UDP PORT SCAN
3.37. NULL SESSIONS
3.38. SYNTAX FOR A NULL SESSION
3.39. SMB NULL SESSIONS &
3.40. HARDCODED NAMED PIPES
3.41. WINDOWS NETWORKING SERVICES
3.42. COUNTERMEASURES
3.43. REVIEW

4. MODULO 4 - ASSESSING WEB SERVERS

4.1. FINGERPRINTING ACCESSIBLE WEB SERVERS
4.2. IDENTIFYING AND ASSESSING REVERSE PROXY MECHANISMS
4.3. PROXY MECHANISMS
4.4. IDENTIFYING SUBSYSTEMS AND ENABLED COMPONENTS
4.5. BASIC WEB SERVER CRAWLING
4.6. WEB APPLICATION TECHNOLOGIES OVERVIEW

4.7. WEB APPLICATION PROFILING

4.8. HTML SIFTING AND ANALYSIS

BENEFICIOS

- Una vez finalizado el curso, el participante no sólo podrá tomar el examen CVA de manera competente, sino que también podrá comprender e implementar una evaluación básica de la vulnerabilidad.