ITSec Foundation — Syllabus

State: released - ID: 107 - Topic: ITSec - Version: 1 - language: deutsch - valid from 2017-10-01
Anzahl der Prüfungsfragen: 30
Schulungszeit in Minuten: 1440

Die verpflichtende Zeitvorgabe für die dazugehörige Schulung ist 3 Tage à min. 8 Stunden mit je 60 Minuten (= 1440 Minuten).

Für den Erhalt des ITSec Foundation Prüfungszertifikates muss die im Multiple-Choice-Verfahren gehaltene Prüfung erfolgreich bestanden werden.

- Sprache: Deutsch/Englisch
- Prüfungsdauer: 45 Minuten
- Format: Multiple Choice-Fragen; mit zwei oder drei Antwortmöglichkeiten, von denen eine, zwei oder auch alle drei Antworten korrekt sein können.
- min. Punkte: 20 von 30
- Jede komplett richtig beantwortete Frage gibt einen Punkt. Bei falsch beantworteten Fragen gibt es 0 Punkte (aber keinen Punktabzug). Als falsch beantwortet gilt eine Frage wenn eine falsche Antwort markiert ist, oder nicht alle richtigen angekreuzt wurden.

Die hier beschriebenen Werte sind eine Kopie der Prüfungsordnung. Sollten sich Prüfungsordnung und dieser Lehrplan widersprechen, gelten die in der Prüfungsordnung angegebenen Prüfungsformate und Definitionen.

Der vorliegende Lehrplan ist keine Agenda. Die Schulungsorganisation ist frei in der Reihenfolge der Inhaltsvermittlung. Die vorgegebenen Zeiten zu den Kapitel sollten eingehalten werden.

1. Voraussetzung

Severity: 5.00% — Minutes: 72 — Min/avg/max number of questions: 1.0/1.5/2.0

Grundkenntnisse in den folgenden Themen werden vorausgesetzt:

- https://de.wikipedia.org/wiki/Ethernet
- https://de.wikipedia.org/wiki/Internet_Protocol
- https://de.wikipedia.org/wiki/IPv4
- https://de.wikipedia.org/wiki/Address_Resolution_Protocol
- https://de.wikipedia.org/wiki/Ping_(Datenübertragung)
- https://de.wikipedia.org/wiki/Internet_Control_Message_Protocol
- https://de.wikipedia.org/wiki/User_Datagram_Protocol
  https://de.wikipedia.org/wiki/Transmission_Control_Protocol
- https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports
  FTP(20/21); SSH (22); TELNET (23); SMTP (25); HTTP (80); NTP (123) HTTPS /n/r(443); IMAP (143); IMAPS (993); POP3S (995); POP3 (110)

2. Vorgehen & wichtige Begriffe

Severity: 10.00% — Minutes: 144 — Min/avg/max number of questions: 2.5/3.0/3.5

Hacker, Cracker & Skriptkiddies

- https://de.wikipedia.org/wiki/Hacker
- https://de.wikipedia.org/wiki/Hacker_(Computersicherheit)
- https://de.wikipedia.org/wiki/Cracker_(Computersicherheit)
- https://de.wikipedia.org/wiki/Skriptkiddie
- https://de.wikipedia.org/wiki/Computerkriminalit%C3%A4t

Ablauf eines Angriffs

- Informationsgewinnung (passiv/aktiv)
  https://de.wikipedia.org/wiki/Footprinting

- Angriff
  o Zugriff erlangen
  o Rechte erweitern
  o permanenten Zugang einrichten
  o Spuren verwischen

Penetration Test und ISMS Audit - Abgrenzung und Zusammenspiel

- https://de.wikipedia.org/wiki/Penetrationstest_(Informatik)
- https://de.wikipedia.org/wiki/ISO/IEC_27001
- https://de.wikipedia.org/wiki/Audit

weitere Begriffe

- https://de.wikipedia.org/wiki/Hackerethik
- http://www.ccc.de/hackerethics?language=de
- https://de.wikipedia.org/wiki/Passwort
- https://de.wikipedia.org/wiki/Salt_(Kryptologie)
- https://de.wikipedia.org/wiki/Denial_of_Service & DDOS
- https://de.wikipedia.org/wiki/Botnet

- https://de.wikipedia.org/wiki/Exploit
- https://de.wikipedia.org/wiki/Computer_Emergency_Response_Team
- https://de.wikipedia.org/wiki/Logging
- https://de.wikipedia.org/wiki/Firewall
- https://de.wikipedia.org/wiki/Intrusion_Detection_System
- https://de.wikipedia.org/wiki/Schadprogramm Maleware
- https://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm)
- https://de.wikipedia.org/wiki/Computervirus
- https://de.wikipedia.org/wiki/Backdoor
- https://de.wikipedia.org/wiki/Spyware
- https://de.wikipedia.org/wiki/Scareware
- https://de.wikipedia.org/wiki/Ransomware
- https://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit)
- https://de.wikipedia.org/wiki/Identit%C3%A4tsdiebstahl
- https://de.wikipedia.org/wiki/Sniffer
- https://de.wikipedia.org/wiki/WLAN-Sniffer

3. Informationsbeschaffung & Angriff

Severity: 45.00% — Minutes: 648 — Min/avg/max number of questions: 11.0/13.5/16.0

Google Hacking

- https://en.wikipedia.org/wiki/Google_hacking

OS Fingerprinting

- https://de.wikipedia.org/wiki/OS-Fingerprinting

Schwachstellenprüfung mit Vulnerability Scannern

- https://de.wikipedia.org/wiki/Vulnerability_Scanner
- https://de.wikipedia.org/wiki/Vulnerability_Scan

Sessionübernahme

- https://de.wikipedia.org/wiki/Session_Hijacking

DNS-Spoofing/Cache Poisoning

- https://de.wikipedia.org/wiki/Cache_Poisoning

Spoofing - ARP und IP

- https://de.wikipedia.org/wiki/ARP-Spoofing
- https://de.wikipedia.org/wiki/IP-Spoofing

Manipulation von URL-Parametern

- https://en.wikipedia.org/wiki/Semantic_URL_attack

Directory Traversal

- https://de.wikipedia.org/wiki/Directory_Traversal

Cross-Site-Scripting

- https://de.wikipedia.org/wiki/Cross-Site-Scripting

SQL-Injection

- https://de.wikipedia.org/wiki/SQL-Injection

Drive-by-Downloads

- https://de.wikipedia.org/wiki/Drive-by-Download

Man-in-the-Middle Angriffe

- https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff

WLAN Hacking

- https://de.wikipedia.org/wiki/Wired_Equivalent_Privacy
- https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access

mindestens 2 Demonstrationen

Beispiel:
Passive Informationsbeschaffung via Google - Die wichtigsten Optionen (http://www.ceilers-news.de/serendipity/249-Google-Hacking,-ganz-einfach.html)

- ""-Doppelte Anführungsstriche sorgen dafür, dass nach genau dem zwischen den Anführungszeichen angegebenen String gesucht wird und nicht nach einem Vorkommen der Wörter in beliebiger Reihenfolge.
- intitle: sucht nach dem angegebenen Begriff im Titel der Seiten.
- allintitle: sucht nur nach Seiten, die alle angegebenen Begriffe im Titel enthalten.
- intext: sucht nur im Text der Seiten nach dem angegebenen Begriff
- allintext: funktioniert wie bei allintitle:, nur das hier alle Begriffe im Text der Seite vorkommen müssen.
- inurl: sucht nach dem angegebenen Begriff im URL der Seiten.
- site: beschränkt die Suche auf eine bestimmte Website.

mindestens 6 praktisch Übungen gefordert

für die Übungen müssen mindestens 60% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.

Beispiele:

•
Übung Portscan/OS-fingerprinting mit https://de.wikipedia.org/wiki/Nmap
•
Übung mit https://de.wikipedia.org/wiki/OpenVAS
OpenVAS (Open Vulnerability Assessment System) ist ein Software-Framework aus verschiedenen Diensten und Werkzeugen und bildet eine Lösung für Schwachstellen-Scanning und Schwachstellen-Management. OpenVAS wurde von Nessus abgespalten.
•
Übung mit "Social Engineering Toolkits"
https://www.trustedsec.com/social-engineer-toolkit/
SET is an open-source Python-driven tool aimed at penetration testing around Social-Engineering
•
Übung mit mit dem Exploit Framework "Metasploit"
https://en.wikipedia.org/wiki/Metasploit_Project
The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.. Its best-known sub-project is the open source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.)

4. Kryptologie

Severity: 20.00% — Minutes: 288 — Min/avg/max number of questions: 5.0/6.0/7.0

Kryptologie - https://de.wikipedia.org/wiki/Kryptologie

- Abgrenzung Kryptographie und Kryptoanalyse
- Prinzip von Kerckhoff https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip

Kryptographie - https://de.wikipedia.org/wiki/Kryptographie

- Symmetrisches, Asymmetrisches & Hybride Verschlüsselung
  https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem
  https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem
- Kryptologische Hashfunktionen (MD5 und SHA)
  https://de.wikipedia.org/wiki/Kryptologische_Hashfunktion
- Caesar und ROT13-Verschlüsselung
  https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung
  https://de.wikipedia.org/wiki/ROT13
- Kryptoanalyse
  https://de.wikipedia.org/wiki/Kryptoanalyse
  https://de.wikipedia.org/wiki/W%C3%B6rterbuchangriff
  https://de.wikipedia.org/wiki/Brute-Force-Methode
  https://en.wikipedia.org/wiki/Password_cracking

mindestens 1 Demonstration

Beispiel:
• entschlüsseln einer Linux passwd-Datei, Windows LM-Hash oder ähnliches

mindestens 2 praktisch Übungen gefordert

für die Übungen müssen mindestens 30% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.
Beispiel:
• verschlüsseln eines Plain-Textes mit dem Cäsar Verfahren (händisch)
• entschlüsseln eines mit einem Cäsar Verfahren verschlüsselten Textes

5. Grundsätze der IT-Forensik

Severity: 20.00% — Minutes: 288 — Min/avg/max number of questions: 5.0/6.0/7.0

BSI Leitfaden IT-Forensik Version 1.0.1
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/Leitfaden_IT-Forensik_pdf.pdf?__blob=publicationFile

- Seite 8 - Definition IT Forensik nach BSI
- Seite 13 bis 16 - Begriffsfindung und Einordnung der IT-Forensik
- Seite 22 bis 23 - Anforderungen an eine forensische Untersuchung/Ermittlungsprozess
- Seite 24 bis 25 - Allgemeine Vorgehensweise bei einer forensischen Untersuchung nach BSI (6 Stufen)
- Seite 26 bis 28 - Die beweissichere Anfertigung eines Datenträgerabbilds (forensische Duplikation)
- Seite 29 bis 32 - Die CERT-Taxonomie im Rahmen einer forensischen Untersuchung

mindestens 1 praktische Übungen gefordert

für die Übungen müssen mindestens 30% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.

Beispiel:

- Angriff aufgrund eines gegebenen Logfile Inhaltes analysieren