Fachhochschule Nordwestschweiz
Hochschule für Technik

Drehbuch

für

cysL

Cyber Security Labor

Verfasser: *Martin Gwerder*

Modulanlass: H*S/2025*

Version: 1 / 11.03.24

Inhaltsverzeichnis

Datum	Wer	Was
16.09.25	GwM	Initiale Version zum Semesterstart

1 Funktion im Rahmen der Gesamtausbildung

1.1 Leitidee

Die Studenten sollen die Kenntnisse aus netsi und kry praktisch anwenden und vertiefen können.

Sie sind in der Lage gängige Internet-Systeme wie DNS, Web oder Mail auf Sicherheitsprobleme zu analysieren und die Resultate der Analyse bezüglich Sicherheit zu bewerten. Sie können Lokale Attacken erkennen, analysieren und entsprechende Schutzszenarien entwerfen. Die Studenten kennen „State-of-the-Art"-Mechanismen der Cyber-Defense

1.2 Voraussetzungen / Vorkenntnisse

Fundierte Grundkenntnisse in der Administration von Linux-Systemen sowie Kenntnisse bezüglich Funktion und Aufbau von Netzwerkprotokollen.

Es wird erwartet, dass der Student einen einfachen, unbekannten Service nach Anleitungen im Internet selbständig und zeitnah Aufbauen kann.

1.3 Outcome-Kompetenzen der Studierenden (KISA)

Kompetenzen	Indikatoren	Standard	Assessment
Die Studierenden können einfache statische Systeme anhand von Logfiles analysieren und Anomalien im Bereich der Systemstabilität und der Privilegieneskalation erkennen.	Sie können entsprechende Aufgabenstellungen lösen.	K4 Analysieren	Entsprechende Aufgaben lösen.
Studenten können einfache Netzbasierte Angriffe erkennen, klassifizieren und abwehren.	Sie können entsprechende Aufgabenstellungen lösen und entsprechende Schutzszenarien entwerfen.	K5 Beurteilen	Entsprechende Aufgaben lösen.
Studenten können einen beliebigen Mail und Webdienst installieren, diagnostizieren und absichern.	Sie können entsprechende Aufgabenstellungen lösen und die Begriffe Arbeit, Leistung und Energie erklären.	K3 Anwenden	Entsprechende Aufgaben lösen und mindestens ein Produkt mit Sachverstand handhaben.
Die Studenten kennen speziell beliebte Angriffsvektoren für DNS, Web und Mailserver. Können diese beobachten, die Beobachtungen interpretieren und adäquate Massnahmen ergreifen	Sie können entsprechende Aufgabenstellungen lösen und Berechnungsmodelle programmieren.	K5-K6 Beurteilen - Erschaffen	Entsprechende Aufgaben im lösen.

2 Unterrichtsorganisation

2.1 Lern- und Arbeitsformen

Die Studenten bereiten das Material jeweils vor der Lektion auf. Ergänzendes und vertiefendes Wissen wird während 21h Kontaktunterricht vermittelt. Die Lektionen 1, 6 und 13 sind reine Theorieblöcke. In allen weiteren Lektionenblöcken findet zuerst ein Theorieblock zur Vertiefung von 1h statt und anschliessend wird das Wissen im Labor umgesetzt. Das Labor ist mindestens während 4h nutzbar.

Es gilt keine Präsenzpflicht. Im Durchschnitt muss für Selbststudium während der Unterrichtsfreien Zeit noch einmal mit 45h Lern- und Nachbearbeitungsaufwand gerechnet werden.

Stoff wird vorgängig via Web (Inside-Gruppe) zur Verfügung gestellt und durch den Modulverantwortlichen gepflegt.

2.2 Zeitaufwand für Studierende (summarisch)

Kontaktunterricht KS:	21h
Begleitetes Selbststudium BSS:	6h
Unbegleitetes Selbststudium während Unterrichtszeit USS:	18h
Unbegleitetes Selbststudium während unterrichtsfreier Zeit	45h
Gesamtaufwand:	90h

2.3 Leistungsbeurteilung

Assessments

Die Erfahrungsnote wird über 2 Berichte (einzureichen am Tag vor der 8. Lektion und zwei Arbeitstage vor der 14. Lektion) ermittelt. Fehlende Berichte werden mit der Note 1 bewertet. Die Berichte werden anhand der eingereichten Dokumente an der gebauten Infrastruktur bewertet. Der Event 7 und 14 sind Pflichtveranstaltungen. Ansonsten gibt es keine Präsenzpflicht.

Modulschlussprüfung

Dieses Fach hat keine Modulschlussprüfung.

Arbeitsmittel

Sicherheitsbuch	
ergänzende Literatur	Weblinks
von Dozierenden abgegebene Arbeitsmittel	Foliensatz Linksammlung
spezielle Informatikmittel	Cyberlab-Infrastruktur
weitere Arbeitsmittel	Internet

3 Themen der Unterrichtsblöcke

3.1 Theorieblock “Netzgestützte und lokale Attacken (technisch und nicht-technisch)“

Lernziele

- Die Studierenden kennen die Arbeitsweise im Labor
- Die Studierenden kennen den Aufbau des cysL-Modules
- Die Studenten kennen die Grundlagen der Informationssicherheit
- Die Studierenden können Lokale Attacken aufzählen und klassifizieren

Inhalte

- Klassifizierungen von Angriffen
- Beliebte lokale, technische Angriffe
- Beliebte, nicht technische Angriffe

Transfer

- Die Studierenden arbeiten Material zu Angriffen auf.
- Die Studierenden Studieren einfache Angriffe via abgegebenem Material.
- Die Studierenden diskutieren das erhaltene Material untereinander

3.2 Labor „Lokale Attacken“

Lernziele

- Die Studierenden erkennen einen Buffer Overflow
- Die Studierenden erkennen Anzeichen von DoS-Attacken und können diese präventiv unterbinden
- Die Studierenden können lokale Attacken aufzählen und klassifizieren

Inhalte

- Theorieblock „OS Boundaries“
- Aufgabenblatt Buffer Overflow und System-Hardening

Transfer

- Via Einführender Theorie und anschliessender Laborarbeit

3.3 Labor „Lokale Schad-Aktivitäts-Erkennung“

Lernziele

- Die Studierenden können Logs und andere Quellen auf verdächtige Aktivitäten durchforsten.

Inhalte

- Theorieblock „Hidden activities and files“
- Aufgabenblätter Log-Analyse und System-Analyse

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.4 Labor „Remote Attacken auf Webservices“

Lernziele

- Die Studierenden erkennen die Attacken XSS, Logic Bomb, Taversal sowie Injection-Attacken und können geeignete Schutzszenarien anwenden.

Inhalte

- Theorieblock „Webgestützte Attacken“
    - Ressourcen-Attacken auf Webservices
    - Traversal-Attacken auf Webservices
    - Injection-Attacken auf Webservices

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.5 Labor „Remote-Attacken Webservices 2“

Lernziele

- Die Studierenden können eine einfache Attacke auf einen Server via schlecht abgesicherten Webseiten anhand einer Anleitung nachvollziehen.

Inhalte

- SQL-Injektion
- Schlecht gesicherte Webdienste und gehashte Passworte

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.6 Theorieblock „Mail und DNSSEC“

Lernziele

- Die Studenten verstehen die Funktion von DNSSEC
- Die Studenten sind in der Lage die notwendigen Schritte für DNSSEC durchzuführen
- Die Studenten kennen die Grundlagen des Mailprotokolls

Inhalte

- Theorieblock „DNSSEC“
    - Funktion eines DNS-Servers mit Master- und Slave-Zonen
    - Grundsätzliche Funktion von DNSSEC
    - Umgang mit ZSK und KSK
- Theorieblock „Mail“ (2h)
    - Mailserver und grundsätzliche funktionsweise
    - Internes Queuing
    - Unterscheidung der Funktionen SMTP und SMTPd
    - Verschlüsselung und Voraussetzungen

Transfer

- Die Studierenden arbeiten Material zu Mail und DNSSEC auf.
- Die Studierenden diskutieren das erhaltene Material untereinander

3.7 Labor „DNSSEC“

Lernziele

- Die Studierenden können eine bestehende DNS-Implementation mit DNSSEC ergänzen

Inhalte

- Theorieblock „DNSSEC“
    - Umgang mit rndc und dynamischen Zonen
    - BCP für das Schlüsselmanagement

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.8 Labor „Mailserver (Normal and Backup)”

Lernziele

- Die Studierenden können einen Mailserver mit zugehöriger Backup-Queue aufsetzen

Inhalte

- Theorieblock „Mailservice am Beispiel von Postfix“
    - Inhalte der Konfigurationsfiles
    - Kaskadierte Queue-Strukturen
    - Mail-Proxies
    - Mail-Filter

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.9 Labor „DKIM/SPF“

Lernziele

- Die Studenten kennen die DNS-Basierten Authentisierungsdienste.
- Die Studenten können SPF einsetzen.

Inhalte

- Theorieblock „DNS-Basierte Mailserver-Authentisierung“
  - SPF
  - DKIM

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.10 Labor „Bayes“

Lernziele

- Die Studierenden können einen bayes-basierten Dienst installieren.
- Die Studierenden sind in der Lage geeignete Szenarien für Trainings-Sets zu machen.

Inhalte

- Theorieblock „Bayes scanning mit Amavis und Spamassassin“

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.11 Labor „Greylisting“

Lernziele

- Die Studierenden kennen die Vor und Nachteile eines listenbasierten Systems und können sie entsprechend einsetzen

Inhalte

- Theorieblock „Bayes scanning mit Amavis und Spamassassin“

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

3.12 Labor Catchup und Endspurt (2x)

Inhalte

- Abschliessen der Infrastruktur

Transfer

- Via einführender Theorie und anschliessender Laborarbeit

4 Drehbuch

Woche / KW	Inhalt	KS	BSS	USS	Tot
1 / 38	Einführung (Allgemeine Infos zur Arbeit im cysL) Netzgestützte und lokale Attacken (technisch und nicht-technisch)	3			3
2 / 39	Labor lokale Attacken	1	2		3
3 / 40	Labor lokale Schad-Aktivitäts-Erkennung	1	2		3
4 / 41	Labor Remote Attacken und Webservice	1	2		3
5 / 42	Labor DoS-Attacken	1	2		3
6 / 43	Theorieblock Mail (SMTP(s)) und DNSSEC	3			3
7 / 44	Labor	1	2		3
8 / 45	Labor	1	2		3
9 / 46	Labor DKIM/SPF	1	2		3
10 / 47	Labor Baynes	1	2		3
11 / 48	Labor Tarpit	1	2		3
12 / 49	Labor Greylisting	1	2		3
13 / 50	Labor		3		3
14 / 51	Labor Arbeitspräsentation		3		3
UFZ	Studium der Theorie und Arbeiten			48	48
	Total	**16**	**26**	**48**	**90**