Zertifikatsprogramm - Modul Z214

Netzsicherheit I: IT-Sicherheit von Netzwerken

- Netzwerktechnik und IT-Sicherheit
- Angriffs- und Sicherheitskonzepte
- Identitäts- und Zugriffsmanagement
- Angriffe auf Netzwerkprotokolle
- Sicherheit von virtuellen Netzwerken

Tobias Scheible, M.Eng.

Open C³S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Modul Z-214

Netzsicherheit I: IT-Sicherheit von Netzwerken

Studienbrief 1: Netzwerktechnik und IT-Sicherheit

Studienbrief 2: Angriffs- und Sicherheitskonzepte

Studienbrief 3: Identitäts- und Zugriffsmanagement

Studienbrief 4: Angriffe auf Netzwerkprotokolle

Studienbrief 5: Sicherheit von virtuellen Netzwerken

Autor:

Tobias Scheible, M.Eng.

---

2. Auflage

Hochschule Albstadt-Sigmaringen

Hochschule Albstadt-Sigmaringen
Zertifikatsprogramm
Poststraße 6
72458 Albstadt

2. Auflage (2022-01-11)

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Satz	S
Übung	Ü

II. Zu dem Autor

Tobias Scheible ist begeisterter Informatiker und interessiert sich für Computer, solange er sich zurückerinnern kann. Neben den technischen Aspekten der IT interessieren ihn vor allem auch der Faktor Mensch und das Thema Wissensvermittlung. So faszinieren ihn besonders die Benutzungsfreundlichkeit, Informationsarchitektur und die Auswirkung neuer Technologien. Außerdem bereitet es ihm Freude, sein Wissen mit anderen zu teilen.

Tobias Scheible ist als Cyber-Security- und IT-Forensik-Sicherheitsforscher und -Dozent an der Hochschule Albstadt-Sigmaringen tätig. Dort arbeitete er zuerst als Modulentwickler im Forschungsprojekt Open Competence Center for Cyber Security und entwickelte Studieninhalte zu den Bereichen Cloud Computing und Internettechnologien mit dem Fokus auf die IT-Sicherheit. Danach engagierte er sich als Autor und E-Tutor im berufsbegleitenden Masterstudiengang Digitale Forensik und leitete im Bachelorstudiengang IT Security Praktika rund um das Thema Informationssicherheit und digitale Forensik. Derzeit ist er als Dozent am Institut für Wissenschaftliche Weiterbildung (IWW) der Hochschule im berufsbegleitenden Zertifikatsprogramm tätig. Dort unterrichtet er berufstätige Teilnehmer in speziellen Einzelmodulen in Online-Kursen. Seine Forschungsschwerpunkte liegen in den Bereichen Sicherheit von Web-Anwendungen, Web Browser Forensics, Pentest-Hardware und benutzerzentrierte Didaktik.

Überdies hält er Vorträge und Workshops für Verbände und Unternehmen, u. a. auch offene Veranstaltungen für den VDI. Mit viel Leidenschaft schreibt er in seinem Blog scheible.it über IT-Sicherheitsthemen. Des Weiteren veröffentlicht er Artikel in verschiedenen Fachzeitschriften.

Aktuelle und ehemalige Lehrveranstaltungen

- Netzsicherheit I: IT-Sicherheit von Netzwerken *Hochschulzertifikatsprogramm*
- Grundlagen der digitalen Forensik *Masterstudiengang IT GRC Management*
- Digitale Forensik *Bachelorstudiengang IT Security*
- Industrieprojekt *Bachelorstudiengang IT Security*
- Einführung in die Informatik *Masterstudiengang Digitale Forensik*
- Internet Grundlagen *Masterstudiengang Digitale Forensik*
- Betriebssystemforensik *Masterstudiengang Digitale Forensik*
- Praktikum IT Security 2 *Bachelorstudiengang IT Security*
- Seminar IT Security 2 *Bachelorstudiengang IT Security*
- Informationssicherheit-Praktikum *Bachelorstudiengang Wirtschaftsinformatik*
- Digitale Rechnersysteme *Studium Initiale*
- Einführung Algorithmen und Programmierung *Studium Initiale*
- Wissenschaftliches Arbeiten *Studium Initiale*
- Cloud Technologies and Cloud Security Architectures *IT GRC Management*
- Internettechnologien *Hochschulzertifikatsprogramm*

Profil | Blog | Twitter | Linkedin | Xing

III. Modullehrziele

Die Lehrveranstaltung „Netzsicherheit I: IT-Sicherheit von Netzwerken“ gibt Ihnen einen Überblick über die Bedrohungen und Angriffe gegen Netzwerke. Ferner lernen Sie die eingesetzten Technologien von Rechnernetzen und die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Datennetzen kennen. Es werden die zentralen Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Verteidigungsmaßnahmen erläutert. In Übungen im virtuellen Labor führen Sie selbst Angriffe durch, um im Anschluss Bedrohungsszenarien nachvollziehen und einordnen zu können.

Im ersten Studienbrief „Netzwerktechnik und IT-Sicherheit“ werden Grundlagen in den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit behandelt, um vorhandenes Wissen zu reaktivieren und eine gemeinsame Ausgangsbasis für dieses Modul zu schaffen.

Im zweiten Studienbrief „Angriffs- und Sicherheitskonzepte“ erlernen Sie, wie generelle Sicherheitskonzepte für Netzwerke realisiert werden. Anhand realitätsnaher Angriffsszenarien und relevanter Verteidigungsmaßnahmen werden Sicherheitseigenschaften von Netzwerktechnologien praxisorientiert vorgestellt.

Im dritten Studienbrief „Identitäts- und Zugriffsmanagement“ wird ein Überblick über das Thema Zugriffsteuerung gegeben. Die Anmeldung und Autorisierung einzelner Benutzer und Systeme stellen ein wichtiger Grundpfeiler für den sicheren Betrieb von Netzwerkdiensten dar. Es werden etablierte Protokolle und Systeme behandelt und wie diese sicher betrieben werden.

Im vierten Studienbrief „Angriffe auf Netzwerkprotokolle“ werden konkrete Angriffsmethoden und Sicherheitslösungen der LAN/WAN-Netze anhand des Schichtenmodells vorgestellt. Sie lernen konkrete Bedrohungen für verschiedene Netzwerkprotokolle kennen und welche Schutzmaßnahmen gegen diese Angriffe realisiert werden können.

Im letzten Studienbrief „Sicherheit von virtuellen Netzwerken“ wird ein Ausblick auf flexible und softwaregesteuerte Netzwerktechniken gegeben. Anhand verschiedener Konzepte und Protokolle werden die Grundlagen von virtualisierten Netzwerken erläutert.

Nach erfolgreichem Abschluss des Moduls haben Sie Kenntnisse über die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Netzwerken und können die verwendeten Sicherheitskonzepte einordnen. Sie sind in der Lage, Bedrohungen und Angriffe gegen Netzwerke einzuordnen, und haben sich Wissen über die Anwendung von Programmen angeeignet, um die Möglichkeiten und Grenzen dieser Tools selbst einzuschätzen zu können. Damit sind Sie in der Lage, Maßnahmen zur Verbesserung der Netzsicherheit umzusetzen.

IV. Literaturempfehlungen

Das Modul wurde so realisiert, dass die Studienbriefe genügend Materialien in Form von Hinweisen, Übungen und Abbildungen bieten, um sich die Modulinhalte selbstständig und ohne weitere Literatur erarbeiten zu können. Zusätzlich erfolgen immer wieder Verweise auf frei verfügbare externe Quellen, um spezifische Aspekte näher zu erläutern oder mit individuellen Beispielen zu verdeutlichen.

Darüber hinaus können Sie aus dem Netzwerk der Hochschule Albstadt-Sigmaringen (auch per VPN) auf folgende E-Books kostenfrei zugreifen:

- IT-Sicherheit für TCP/IP- und IoT-Netzwerke : Grundlagen, Konzepte, Protokolle, Härtung | Steffen Wendzel | Springer Vieweg, Wiesbaden | ISBN 9783658334239 | https://doi.org/10.1007/978-3-658-33423-9
- Netzsicherheit : Grundlagen & Protokolle; mobile & drahtlose Kommunikation; Schutz von Kommunikationsinfrastrukturen | Günter Schäfer; Michael Roßberg | dpunkt.verlag, Heidelberg | ISBN 9783864901157 | https://ebookcentral.proquest.com/lib/hsalbsig-ebooks/detail.action?docID=1764755
- IT-Sicherheit: Konzepte – Verfahren – Protokolle | Claudia Eckert | De Gruyter, Oldenbourg | ISBN 9783110551587 | https://www.degruyter.com/viewbooktoc/product/490352
- Kryptographie und IT-Sicherheit | Stephan Spitz; Michael Pramateftakis; Joachim Swoboda | Springer Vieweg, Wiesbaden | ISBN 9783834881205 | https://doi.org/10.1007/978-3-8348-8120-5

Das Folgende Buch kann zur Unterstützung im Bereich Grundlagen der Netzwerktechnik hinzugezogen werden:

- Computernetzwerke | Andrew S. Tanenbaum; David J. Wetherall | Pearson, München | ISBN 9783868941371 | https://www.pearson-studium.de/computernetzwerke.html

Zusätzlich kann noch die folgende Online-Quelle zur Unterstützung genutzt werden:

- IT-Grundschutz des BSI - NET: Netze und Kommunikation | https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_Uebersicht_node.html

V. Inhalte

Elemente, die als *Exkurs* gekennzeichnet sind, gehen über die eigentliche Zielsetzung des Modul hinaus, verdeutlichen aber den Zusammenhang und stellen einen Praxisbezug her. Diese Elemente sind daher *nicht prüfungsrelevant*.

Studienbrief 1 Netzwerktechnik und IT-Sicherheit

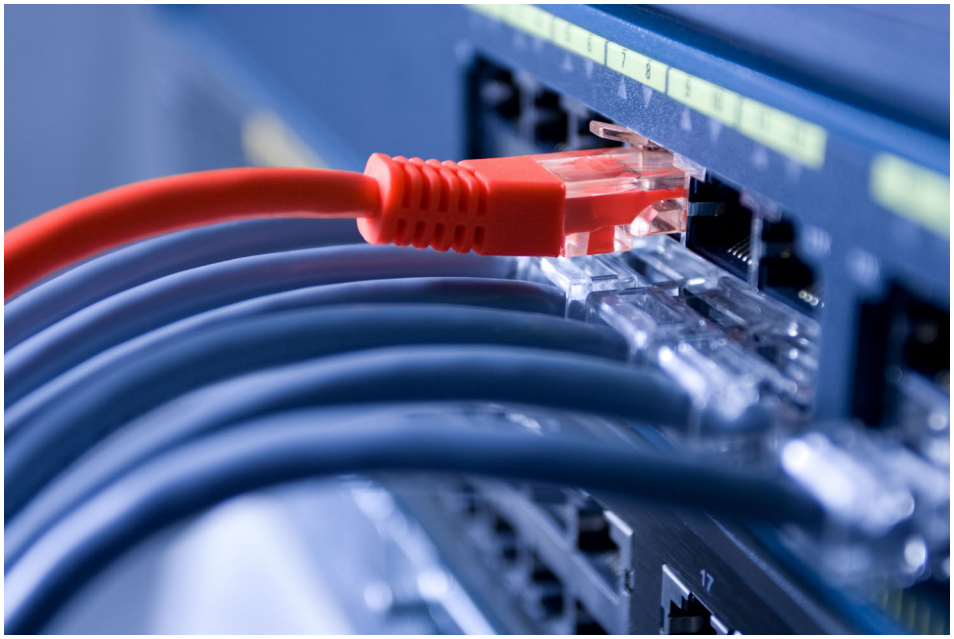
1.1 Advance Organizer

Dieser erste Studienbrief legt die Grundlagen für das weitere Verständnis des Themas Netzsicherheit. Die Inhalte werden nicht in den Online-Vorlesungen behandelt, sondern dienen im Selbststudium zur Wiederholung respektive Reaktivierung des Wissens aus den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit. In den folgenden Studienbriefen werden diese Grundlagen mit konkreten Anwendungsszenarien verknüpft.

1.2 Lernergebnisse

Nach Abschluss dieses Studienbriefs können Sie grundlegende Begriffe der Netzwerktechnik einordnen und wissen, welche Komponenten in Netzwerken verwendet werden. Sie können die verschiedenen Netzwerktopologien und -architekturen beschreiben und den Aufbau der Referenzmodelle nachvollziehen. Sie besitzen das Wissen, um kryptografische Konzepte einzuordnen und können verschiedene Algorithmen und Protokolle situationsbezogen einschätzen. Weiterhin sind Sie in der Lage, die Kernelemente der IT-Sicherheit zu erläutern.

Studienbrief 2 Angriffs- und Sicherheitskonzepte



2.1 Lernergebnisse

Sie können einerseits die für Netzwerke relevanten Sicherheitskonzepte beschreiben und andererseits die dafür bedeutsamen Bereiche identifizieren. Sie kennen die häufigsten Angriffsarten auf Netzwerke und ihre Auswirkungen. Außerdem können Sie die Konzepte von verschiedenen Verteidigungsmaßnahmen beschreiben.

2.2 Advance Organizer

In diesem Studienbrief werden die Angriffskonzepte auf und Sicherheitsprinzipien von Rechnernetzen allgemein behandelt, hierzu werden diese vorgestellt und exemplarisch erklärt. In den weiteren Studienbriefen wird auf diese Erläuterungen aufgebaut und daran konkrete Angriffsszenarien abgeleitet.

Ü

Übung 2.1: Wireshark – Netzwerkanalyse

Arbeiten Sie sich in das Tool *Wireshark* ein. Ein entsprechendes Tutorial finden Sie auf Ilias.

a) Starten Sie Wireshark und beginnen Sie mit der Aufzeichnung. Öffnen Sie danach das Terminal und führen Sie jeweils einen einzelnen Ping durch. Wechseln Sie wieder zu Wireshark und stoppen Sie die Aufnahme. Analysieren Sie die Aufzeichnung. Welcher Typ von ICMP wird jeweils verwendet? Verwenden Sie den folgenden Befehl, um einen einzelnen Ping zu senden.

```
$ ping 2130706433 -c1
$ ping 202.61.237.58 -c1
```

b) Starten Sie nun erneut die Aufzeichnung und führen einen einzelnen Ping der Domain *cyber-security-lab.net* durch. Finden Sie die entsprechende Übermittlung der Antwort der DNS-Abfrage mit der IP-Adresse.

c) Führen Sie nun die Analyse einer HTTP-Verbindung durch. Starten Sie dazu die Aufnahme in Wireshark, öffnen Sie den Firefox-Webbrowser und rufen Sie die Domain *server.lab* auf. Sie werden sehr viele Abfragen sehen, die von Firefox selbst und der Eingabe in der Adresszeile verursacht wurde. Nutzen Sie den untenstehenden Filter, um nur die Übertragungen des lokalen Netzwerkes angezeigt zu bekommen. Wie viele Anfragen gibt es? Ist der Name des Webservers erkennbar?

```
ip.src==10.0.0.0/24 and ip.dst==10.0.0.0/24
```

Ü

Übung 2.2: Zenmap – Netztopologieplan

Verschaffen Sie sich als Erstes einen Überblick über das lokale Netzwerk. Führen Sie dazu einen einfachen Scan des kompletten lokalen Netzwerkes mit dem Tool *Zenmap* durch. Geben Sie dazu in das Feld *Target* das aktuelle Subnetz „10.0.0.*“ ein und wählen Sie das *Profil* „Ping scan“ aus. Starten Sie den Vorgang mit dem Button „Scan“. Wechseln Sie zum Tab „Topology“ und speichern Sie den entstandenen Netztopologieplan.

```
# Start von Zenmap per Terminal:
$ sudo zenmap-kbx
```

a) Welche anderen Systeme konnten im lokalen Netzwerk gefunden werden?

b) Welche Informationen können Sie dem Netztopologieplan entnehmen?

Ü

Übung 2.3: Zenmap – Traceroute

Nachdem Sie nun einen Überblick über das lokale Netzwerk haben, analysieren Sie die Internetverbindung. Verwenden Sie dazu die Funktion Traceroute. Fügen Sie in das Feld *Command* den folgenden Befehl ein und ersetzen Sie jeweils den Platzhalter *DOMAIN* durch die unten jeweils genannte Domain:

```
$ nmap -sn -Pn --traceroute DOMAIN
```

Dokumentieren Sie jeweils die Ausgabe und erstellen Sie am Ende einen neuen Netztopologieplan.

a) Analysieren Sie die Verbindung zum Server mit der Domain *hs-albsig.de*

b) Analysieren Sie die Verbindung zum Server mit der Domain *cyber-security-lab.net*

Ü

Übung 2.4: Rechnernetz-Scan

Als Nächstes untersuchen Sie das lokale Netzwerk intensiver. Nutzen Sie *Nmap,* um das lokale Netz der Testumgebung zu scannen. Recherchieren Sie dafür die Funktionsweise von *Nmap* und experimentieren Sie mit verschiedenen Parametern. Führen Sie mindestens vier verschiedene Scans des kompletten Netzwerkes mit unterschiedlicher Tiefe (unauffällig <=> maximale Informationen) durch. Das Ziel ist es, möglichste viele Informationen (offene Ports, eingesetzte Software und verwendete Versionen) zu erlangen.

```
$ nmap 10.0.0.*
```

a) Welche zusätzlichen Informationen können gewonnen werden?

b) Wie können mit einem Scan möglichst schnell möglichst viele Informationen gewonnen werden?

Ü

Übung 2.5: DoS-Angriff

Führen Sie mit dem Tool *hping3* einen *DoS-Angriff* gegen den *Server* durch. Recherchieren Sie dafür die Funktionsweise von *hping3* und experimentieren Sie mit verschiedenen Parametern. Sie können z. B. die Ports 22 (SSH) und 80 (HTTP) als Angriffsziele verwenden und parallele Angriffe mit mehreren Terminal-Tabs oder -Fenstern durchführen. Versuchen Sie, während die Angriffe laufen, mit dem Client auf den Server zuzugreifen (HTTP). Analysieren Sie die Auslastung des Servers mit den Tools *htop, EthStatus* und *bmon*.

```
$ htop
$ ethstatus -i enps4 -S 100m
$ bmon
```

a) Wie sieht die Auslastung des Kali-Linux-Systems während des Angriffes aus?

b) Ist es möglich, den Server komplett auszulasten? Mit welchen Parametern und wie vielen Verbindungen?

Studienbrief 3 Identitäts- und Zugriffsmanagement

3.1 Lernergebnisse

Sie können die wichtigsten Begriffe und Konzepte des Identitäts- und Zugriffsmanagements einordnen und wiedergeben. Sie wissen, welche Protokolle und Systeme für die Realisierung verwendet werden und welche Sicherheitsaspekte zu beachten sind. Zusätzlich können Sie anhand von Beispielen den konkreten Einsatz beschreiben und wie typische Angriffsszenarien ablaufen.

3.2 Advance Organizer

In diesem Studienbrief werden die Methodiken in den Bereichen Identitäts- und Zugriffsmanagement beschrieben und erläutert. Dazu werden die in den vorherigen Studienbriefen beschriebenen Technologien herangezogen und auf Angriffskonzepte übertragen. In den folgenden Studienbriefen werden diese dann mit Angriffen auf der Netzwerkprotokollebene verknüpft.

3.6 Übungsaufgaben

Das Bestehen der Übungen (unbenotete Prüfungsleistung) ist obligatorisch für die Zulassung zur Abschlussprüfung. Die Abgabe muss rechtzeitig über Ilias erfolgen, die Termine stehen auf Ilias. Dokumentieren Sie Ihre Ausarbeitung mit Screenshots und kurzen Beschreibungen. Gegebenenfalls anfallende Protokolle oder Aufzeichnungen geben Sie als Anhang mit ab.

Ü

Übung 3.1: HTTP Basic Authentication – bekannte Passwörter

Auf dem Webserver des Servers ist der Unterordner */secure* mit einem Passwortschutz per HTTP Basic Authentication versehen. Setzen Sie hierzu das Tool *Ncrack* ein, um den Login anzugreifen. Verwenden Sie dazu den Benutzernamen „httpuser“ und die in Kali Linux integrierte Passwortliste *rockyou.txt*.

a) Wie lautet das Passwort?

b) Welche Methoden gibt es, um den Vorgang zu beschleunigen?

Ü

Übung 3.2: HTTP Basic Authentication -– Tool-Vergleich

Auf dem Webserver gibt es im bereits bekannten passwortgeschützten Ordner http://10.0.0.100/secure/ einen weiteren Benutzer mit dem Namen *httpuser3*. Versuchen Sie das Passwort dieses Accounts zu knacken, indem Sie die Passwortliste linkedin.txt nutzen. Verwenden Sie dazu die Tools *Ncrack, Patator, Hydra* und *M edusa*. Optimieren Sie die Ausführungszeit und messen Sie die Ausführungsdauer mit dem Tool *time*.

a) Wie lautet das Passwort?

b) Wie schnell sind die jeweiligen Tools?

Ü

Übung 3.3: FTP – generierte Passwörter

Erstellen Sie im ersten Schritt mit dem Tool *cewl* eine eigene Passwortliste, indem Sie dazu die Website des Servers verwenden. Erweitern Sie anschließend die generierte Passwortliste mit dem Tool *Mentalist*. Tauschen Sie alle „a“ durch ein „@“, alle „i“ durch ein „!“ und fügen Sie jedem Eintrag Zahlen zwischen 0 und 1000 hinzu. Verwenden Sie anschließend das Tool *Medusa*, um den FTP-Service des Server anzugreifen. Ihr Ziel ist der Benutzer „ftpuser“.

a) Wie lautet das Passwort?

b) Welche Methoden gibt es, um den Vorgang zu beschleunigen?

Ü

Übung 3.4: SSH – Brute-Force-Methode

Greifen Sie als Nächstes den SSH-Log-in des Servers an. Verwenden Sie dazu das Tool *Hydra* und generieren Sie damit Passwörter mit Kleinbuchstaben und Zahlen. Verwenden Sie hier den Benutzernamen „sshuser“.

a) Wie schnell werden die Versuche durchgeführt (Passwörter pro Sekunde)?

b) Welche Methoden gibt es, um den Vorgang zu beschleunigen?

Ü

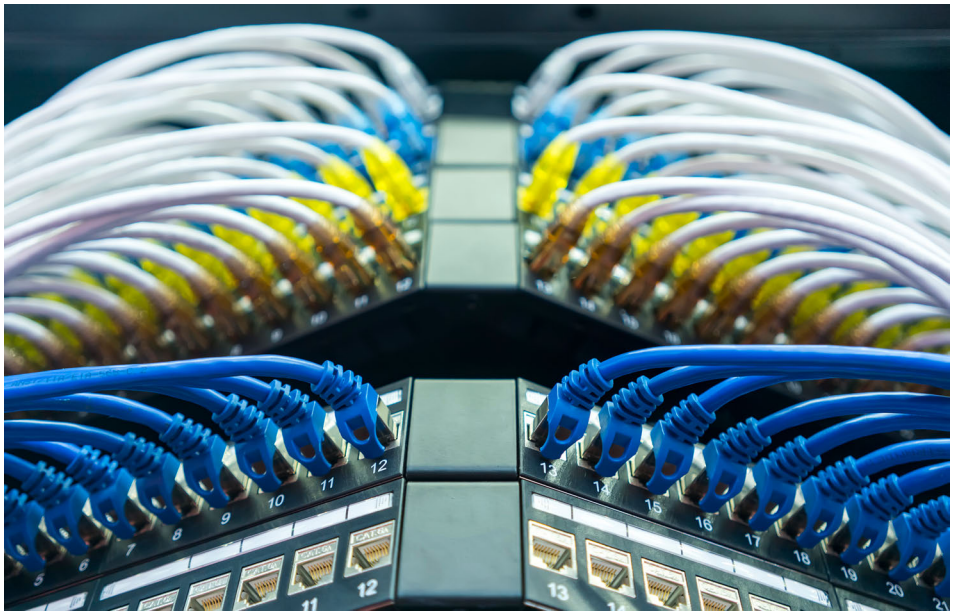
Übung 3.5: LDAP Angriff

Auf dem Server ist eine LDAP-Installation aktiv.

a) Analysieren Sie diese erneut mit dem Tool *nmap* und nutzen Sie die *Nmap Scripting Engine (NSE)*. Recherchieren Sie, welches Script für eine Analyse geeignet ist. Welche Informationen können Sie gewinnen?

b) Führen Sie einen Angriff auf den LDAP-Server durch, um die Log-ins zu knacken. Verwenden Sie dazu das Tool *patator*. Generieren Sie als Erstes mit dem Tool *crunch* eine eigene Passwortliste (1 bis 4 Zeichen mit Zahlen und Kleinbuchstaben) und setzen Sie diese ein, um das Passwort eines LDAP-Benutzers zu knacken.

Studienbrief 4 Angriffe auf Netzwerkprotokolle



4.1 Lernergebnisse

Sie verstehen die Architektur von LAN/WAN-Netzen anhand des Schichtenmodells. Sie können beschreiben, auf welcher Schicht welche Angriffsarten zu erwarten sind und wie entsprechende Sicherheitskonzepte aussehen, um diese Angriffe abzuwehren. Sie haben Kenntnisse über die konkreten Bedrohungen gegen etablierte Netzwerkprotokolle und wie Schutzmaßnahmen gegen diese Angriffe realisiert werden können.

4.2 Advance Organizer

Dieser Studienbrief verknüpft das Wissen aus den vorherigen Studienbriefen, überträgt die behandelten Konzepte auf konkrete Angriffe und zeigt entsprechende Schutzmaßnahmen auf.

4.9 Übungsaufgaben

Das Bestehen der Übungen (unbenotete Prüfungsleistung) ist obligatorisch für die Zulassung zur Abschlussprüfung. Die Abgabe muss rechtzeitig über Ilias erfolgen, die Termine stehen auf Ilias. Dokumentieren Sie Ihre Ausarbeitung mit Screenshots und kurzen Beschreibungen. Gegebenenfalls anfallende Protokolle oder Aufzeichnungen geben Sie als Anhang mit ab.

Übung 4.1: ARP-Spoofing — URLs und Parameter abfangen

Ü

Starten Sie einen ARP-Spoofing-Angriff mit dem Kali-System auf dem Client. Leiten Sie dazu den gesamten Datenverkehr zwischen Router und Client über das Kali-System um. Analysieren Sie die URL-Aufrufe mit dem Tool *urlsnarf*.

a) Welche Einträge sind im ARP-Cache des Clients vorhanden?

b) Wie lauten die URLs, die übertragen werden?

c) Wie lautet das Passwort, das als GET-Parameter übertragen wird?

Übung 4.2: ARP-Spoofing — Log-in-Daten abfangen

Ü

Ändern Sie den ARP-Spoofing-Angriff so ab, dass der Datenverkehr zwischen Client und Server über das Kali–Linux-System umgeleitet wird. Verwenden Sie das Tool *dsniff*, um die übertragenen Zugangsdaten abzufangen.

a) Für welche Dienste werden Log-ins genutzt?

b) Wie lauten die Benutzernamen und die Passwörter?

Übung 4.3: DNS-Spoofing — Aufruf einer Domain umleiten

Ü

Anstatt nur passiv mitzulesen, greifen Sie nun aktiv in die Verbindungen ein. Sorgen Sie dafür, dass der Aufruf der Domain *cyber-security-lab.net* auf dem Client auf den lokalen Webserver des Kali-Systems umgeleitet wird. Verwenden Sie dazu das Tool *Ettercap*.

Hinweis: Leeren Sie den Browser- und DNS-Cache, bevor Sie mit der Aufgabe starten.

Ü

Übung 4.4: DoS-Angriff auf den HTTP-Server

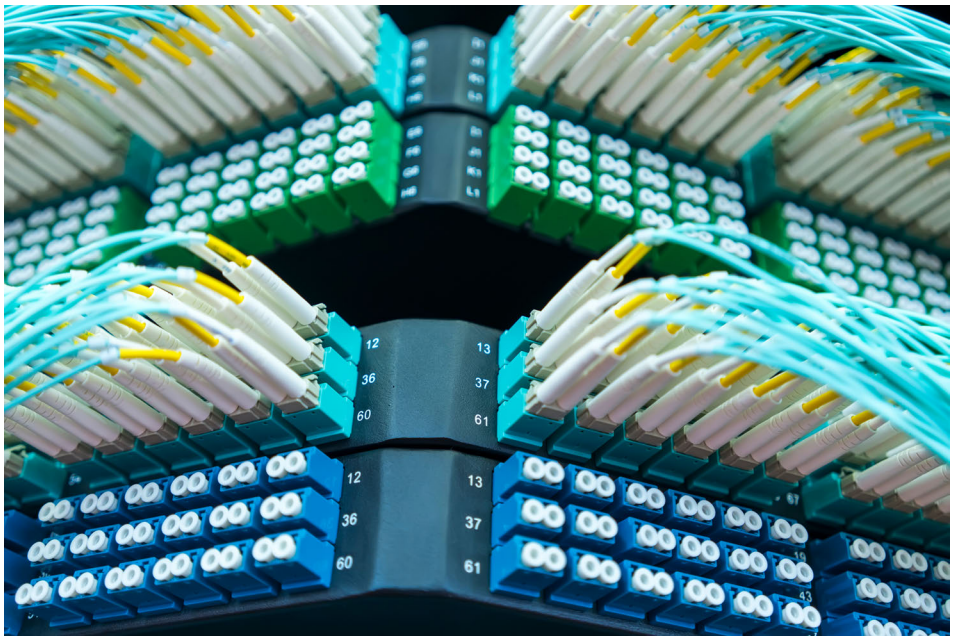
Greifen Sie mit dem Kali-System den HTTP-Server des Servers per DoS an. Verwenden Sie dazu das Tool *slowloris*; es ist bereits im Verzeichnis des Benutzers „hsas“ installiert. Mit dem Parameter -s können Sie bestimmen, wie viele gleichzeitige Verbindungen verwendet werden. Überwachen Sie die Systemauslastung auf dem Server mit den bereits behandelten Tools (inkl. *Linux Dash* auf Port 81) und auf dem Kali-Linux-System mit dem Tool *System Monitor*.

a) Wie viele gleichzeitige Verbindungen sind notwendig, damit der Webserver nicht mehr erreichbar ist?

b) Gibt es einen Unterschied in der Erreichbarkeit des Servers zwischen dem Client und dem Kali-System?

b) Wie ist die Auslastung auf dem Server? Wie ist die Auslastung auf dem Kali-System?

Studienbrief 5 Sicherheit von virtuellen Netzwerken



5.1 Lernergebnisse

Sie können die Grundlagen und Konzepte von flexiblen und softwaregesteuerten Netzwerken erläutern. Zudem können Sie darstellen, welche Protokolle für virtualisierte Netzwerke eingesetzt werden, und sie können erläutern, wie konkrete Anwendungsszenarien aussehen. Ferner können Sie die Methoden zur Absicherung von virtualisierten Netzwerken einordnen.

5.2 Advance Organizer

Dieser Studienbrief gibt einen Ausblick auf die Protokolle von virtualisierten Netzwerken. Es wird gezeigt, welche Konzepte in Rechenzentren, Cloud-Umgebungen und großen Unternehmen eingesetzt werden. Hierbei wird auch aufgezeigt, welche Aspekte der Netzwerksicherheit sich daraus ergeben.

5.8 Übungsaufgaben

Das Bestehen der Übungen (unbenotete Prüfungsleistung) ist obligatorisch für die Zulassung zur Abschlussprüfung. Die Abgabe muss rechtzeitig über Ilias erfolgen, die Termine stehen auf Ilias. Dokumentieren Sie Ihre Ausarbeitung mit Screenshots und kurzen Beschreibungen. Gegebenenfalls anfallende Protokolle oder Aufzeichnungen geben Sie als Anhang mit ab.

Die Übungsaufgaben werden in digitaler Form auf Ilias bereitgestellt.

Übung 5.1: Segmentierung

Ü

Führen Sie einen *Nmap*-Scan des lokalen Netzwerkes durch. Deaktivieren Sie beim Kali-Linux-System die Netzwerkverbindung *LAN* und aktivieren Sie die Netzwerkverbindung *EXT*. Führen Sie einen erneuten Scan mit *Nmap* durch. Vergleichen Sie die beiden Scans miteinander.

a) Welche IP-Konfiguration hat das Kali-System in den beiden unterschiedlichen Netzwerken?

b) Welche Systeme sind innerhalb des EXT-Netzwerks erreichbar?

Übung 5.2: VPN

Ü

Führen Sie erneut einen ARP-Spoofing-Angriff durch, um mit dem Kali-System die Aufrufe der URLs des Clients abzufangen. Aktivieren Sie nun auf dem Client die VPN-Verbindung zum Router.

```
start:
$ sudo wg-quick up vpn
stop:
$sudo wg-quick down vpn
```

a) Funktioniert die VPN-Verbindung trotz des ARP-Spoofing-Angriffs?

b) Können die URLs nach Aktivierung der VPN-Verbindung weiterhin abgefangen werden?

Ü

Übung 5.3: Tor-Netzwerk – Browser

Auf dem Kali-System ist der Tor-Browser installiert. Mit ihm kann komfortabel das Overlay-Netzwerk Tor genutzt werden und Websites können anonym oder im Tor-Netzwerk aufgerufen werden.

a) Starten Sie den Tor-Browser und rufen Sie die Website `https://cyber-security-lab.net` auf. Wie lautet Ihre öffentliche IP-Adresse? Welche Route nehmen die Datenpakete?

b) Rufen Sie die beiden Darknet-Seiten `http://3g2upl4pq6kufc4m.onion` und `http://vfqnd6mieccqyiit.onion` auf. Welche Informationen finden Sie hier?

Ü

Übung 5.4: Tor-Netzwerk – systemweit

Mit dem Tor-Browser können nur Websites angezeigt werden. Um systemweit das Tor-Netzwerk zu nutzen, kann das Tool *torghost* verwendet werden. Es ist bereits im Heimverzeichnis des Kali-Linux-Benutzers abgelegt.

a) Starten Sie *torghost* und überprüfen Sie Ihre Internetverbindung.

b) Testen Sie verschiedene Verbindungsarten. Gibt es Einschränkungen bei den verschiedenen Netzwerkdiensten?

Liste der Lösungen zu den Kontrollaufgaben

Lösung zu Kontrollaufgabe 1.1 auf Seite 18

Die Stern-Topologie ist heute die übliche Topologie, die am häufigsten Anwendung findet. Von „kleinen“ Sternen innerhalb eines Büros bis hin zu „großen“ Sternen, die sich über ein ganzes Gebäude erstrecken.

Lösung zu Kontrollaufgabe 1.2 auf Seite 22

Services können zentral von nur einem Server für mehrere Clients angeboten werden, wodurch Ressourcen gespart werden können.

Lösung zu Kontrollaufgabe 1.3 auf Seite 27

Ein Broadcast wird immer nur von einem Sender durchgeführt.

Lösung zu Kontrollaufgabe 1.4 auf Seite 29

RFCs werden durch allgemeine Akzeptanz und Gebrauch als Standard eingesetzt, ohne dass sie von Normungsgremien verabschiedet worden sind.

Lösung zu Kontrollaufgabe 1.5 auf Seite 31

Damit wird die Komplexität reduziert und einzelne Techniken können gesondert betrachtet werden oder einfach ausgetauscht werden.

Lösung zu Kontrollaufgabe 1.6 auf Seite 34

Das TCP/IP-Schichtenmodell ist im Gegensatz zum ISO/OSI-Referenzmodell ein aus der Praxis hervorgegangener Protokollstapel. Das ISO/OSI-7-Schichtenmodell wurde von der International Organization for Standardization (ISO) als Standard veröffentlicht und repräsentiert die Netzwerkkommunikation im Allgemeinen.

Lösung zu Kontrollaufgabe 1.7 auf Seite 37

Virtuelle Netzwerke, sogenannte VLANs, verwenden Tagged-MAC-Frames für die Übermittlung des VLAN-Tags. Dieser beinhaltet neben einer Priorisierung die eigentliche VLAN-ID, womit mehrere VLANs unterschieden werden können.

Lösung zu Kontrollaufgabe 1.8 auf Seite 38

Da die Informationen per Funk übertragen werden, sind diese nicht einfach auf einen räumlichen Bereich beschränkt. Bei einem Netzwerk per Kabel müsste der Angreifer erst in ein Gebäude eindringen, um eine Manipulation vorzunehmen. Bei einem WLAN, das über das Gebäude hinausgeht, kann ein Angreifer sich im öffentlichen Bereich auf der Straße befinden.

Lösung zu Kontrollaufgabe 1.9 auf Seite 41

Mittels ARP werden IP-Adressen mit den dazugehörigen MAC-Adressen verknüpft. Jeder Rechner legt mittels des ARP-Protokolls sogenannte ARP-Tabellen

(auch Mapping-Tabellen genannt) an, welche die besagte Abbildung zwischen Netzwerk- und Hardwareadresse repräsentieren.

Lösung zu Kontrollaufgabe 1.10 auf Seite 43

IP-Adressen dienen der eindeutigen Zuordnung von Netzwerkteilnehmern.

Lösung zu Kontrollaufgabe 1.11 auf Seite 56

Hash-Algorithmen werden in der Netzwerktechnik u. a. dazu eingesetzt, die Integrität einer Übertragung sicherzustellen.

Lösung zu Kontrollaufgabe 1.12 auf Seite 60

Die symmetrisch Verschlüsselung kann schnell durchgeführt werden. Die asymmetrische Verschlüsselung bietet Vorteile bei dem Schlüsselaustausch.

Lösung zu Kontrollaufgabe 1.13 auf Seite 72

Bei einem derartig unprofessionellen Vorgehen werden prinzipiell alle Schutzziele verfehlt, abhängig von den Berechtigungen des Accounts. Ein potenzieller Angreifer kann dadurch beispielsweise beliebige Daten einsehen, verändern und unwiderruflich entfernen. Des Weiteren könnte beliebige Schadsoftware installiert werden, die den Rechner dauerhaft ausspionieren würde.

Lösung zu Kontrollaufgabe 1.14 auf Seite 72

Zwei Kommunikationspartner können einen geheimen Schlüssel erzeugen, der nicht von einem Angreifer abgefangen werden kann, auch wenn er die komplette Kommunikation abhört.

Lösung zu Kontrollaufgabe 2.1 auf Seite 79

Eine Risikoanalyse kann entweder nach der Realisierung der weiterführenden Sicherheitsmaßnahmen durchgeführt werden, um nicht abgedeckte Bereiche zu analysieren. Zum Teil wird nach der Schutzbedarfsfeststellung die Risikoanalyse durchgeführt, um eine Priorisierung der Maßnahmen zu erhalten.

Lösung zu Kontrollaufgabe 2.2 auf Seite 81

Das Konzept Defense-in-Depth sieht den koordinierten Einsatz mehrerer Sicherheitsmaßnahmen auf verschiedenen Ebenen vor, um einen mehrstufigen Sicherheitsansatz zu realisieren.

Lösung zu Kontrollaufgabe 2.3 auf Seite 83

Mit Zero Trust wird ein Sicherheitskonzept verfolgt, bei dem generell jedem Vorgang, unabhängig von seiner Herkunft, misstraut wird. Es basiert auf dem Grundsatz, keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks zu vertrauen.

Lösung zu Kontrollaufgabe 2.4 auf Seite 87

Mit einem Scan kann ermittelt werden, welche Rechner in einem Netzwerksegment aktiv sind. Bei einzelnen Rechnern kann ermittelt werden, welche Dienste aktiv sind. Mit einem aggressiven Scan kann die Version eines Dienstes herausgefunden werden.

Lösung zu Kontrollaufgabe 2.5 auf Seite 91

Bei einem DoS-Angriff versucht ein Angreifer, einen Server mit einer großen Anzahl von Anfragen zu überlasten. Dabei verfolgt der Angreifer das Ziel, mit möglichst wenig Aufwand möglichst viele Anfragen zu generieren. Ein DoS-Angriff wird von einem oder nur wenigen Rechnern ausgeführt. Ein DDoS-Angriff hingegen wird von einer Vielzahl von verteilten Rechnern ausgeführt, die sich an verschiedenen Standorten befinden.

Lösung zu Kontrollaufgabe 2.6 auf Seite 95

Die meisten Tools sind sehr klein und können dadurch einfach transportiert und unauffällig platziert werden. Gleichzeitig sind sie oft einfach zu bedienen und arbeiten autark, dadurch müssen sie z. B. nur angeschlossen und später wieder mitgenommen werden.

Lösung zu Kontrollaufgabe 2.7 auf Seite 97

Das Ziel ist hierbei die Isolation von potenziellen Angreifern. Nach einem erfolgreichen Angriff können nur die Rechner innerhalb des Segmentes erreicht werden.

Lösung zu Kontrollaufgabe 2.8 auf Seite 99

Ein IDS kann Angriffe erkennen und protokollieren. IPS hingegen kann auch auf einen Angriff reagieren und z. B. mit der Firewall interagieren, um einen Angreifer zu blockieren.

Lösung zu Kontrollaufgabe 3.1 auf Seite 111

Beispiele für Besitz: neuer Personalausweis, SIM-Karte im Smartphone, Hardware-Sicherheitsmodule (Smartcard, USB-Stick, ...) usw.

Lösung zu Kontrollaufgabe 3.2 auf Seite 113

Wenn die Daten für ein biometrisches Merkmal gestohlen wurden, können sie nicht abgeändert werden. Wurde ein Fingerabdruck gestohlen, ist dieser theoretisch nicht mehr sicher genug, um ihn weiterhin zu verwenden.

Lösung zu Kontrollaufgabe 3.3 auf Seite 116

Ein Angreifer probiert bei einem Brute-Force-Angriff systematisch alle möglichen Kombinationen von Passwörtern durch.

Lösung zu Kontrollaufgabe 3.4 auf Seite 116

Wird immer dasselbe Passwort bei mehreren Diensten verwendet, besteht eine beträchtliche Gefahr, wenn die Daten eines Dienstes illegal veröffentlicht werden. Angreifer probieren die erbeuteten Zugangsdaten zum Teil automatisiert bei anderen Diensten aus.

Lösung zu Kontrollaufgabe 3.5 auf Seite 118

Die Übertragung des zusätzlichen Faktors muss auf einem weiteren Kanal erfolgen. Der weitere Faktor muss dabei nur einmal gültig sein und entspricht somit einem Einmalpasswort.

Lösung zu Kontrollaufgabe 3.6 auf Seite 121

Identity Management ist notwendig, um die digitalen Identitäten, deren Attribute und deren Berechtigungen für IT-Systeme sowie IT-Dienste zu erzeugen, nutzen, pflegen und löschen zu können.

Lösung zu Kontrollaufgabe 3.7 auf Seite 123

Da es ein auf TCP/IP basierendes Protokoll ist, müssen keine aufwendigen Implementierungen des kompletten Netzwerkstacks erfolgen. Dadurch ist LDAP insgesamt leichtgewichtiger und auch für schwächere Clients mit weniger Ressourcen geeignet.

Lösung zu Kontrollaufgabe 3.8 auf Seite 124

Da beim LDAP Channel Binding die TLS-Verbindung und die LDAP-Anwendungsschicht miteinander verbunden werden, ist LDAPS für die verschlüsselte TLS-Verbindung erforderlich. Das heißt, LDAP Channel Binding baut auf LDAPS auf und kann nicht losgelöst verwendet werden.

Lösung zu Kontrollaufgabe 3.9 auf Seite 125

Es muss die Funktionen Authentifizierung, Autorisierung und Accounting bereitstellen.

Lösung zu Kontrollaufgabe 4.1 auf Seite 135

Diese werden als Metadaten oder Metainformationen bezeichnet und sind strukturierte Daten, die Informationen über die Kommunikationsverbindung enthalten.

Lösung zu Kontrollaufgabe 4.2 auf Seite 138

Als zentrales Mittel wird eine Ausnahmeliste (Allowlist/Whitelist) mit MAC-Adressen gepflegt, die auf das Netzwerk zugreifen dürfen. Alle anderen Geräte ohne registrierte MAC-Adressen werden geblockt. Zusätzlich wird die Freigabe auf wenige physische Ports beschränkt. Um dies zu realisieren, ist ein gewisser Auf-

wand notwendig. Gleichzeitig können MAC-Adressen sehr einfach geklont werden.

Lösung zu Kontrollaufgabe 4.3 auf Seite 140

Der Angreifer kann mit ARP-Spoofing einen Man-in-the-Middle-Angriff durchführen und den Netzwerkverkehr umleiten. Dadurch kann der Angreifer die komplette Kommunikation abhören oder auch manipulieren.

Lösung zu Kontrollaufgabe 4.4 auf Seite 143

Der Angreifer sendet eine hohe Anzahl von IP-Paketen mit dem gesetzten More-Fragments-Flag (MF) an ein Zielsystem. Dadurch muss der Empfänger die Daten zwischenspeichern, bevor er sie verwerfen kann; damit wird der Speicher des Empfängers geflutet.

Lösung zu Kontrollaufgabe 4.5 auf Seite 148

Bei einem ICMP-Flood-Angriff ist die Bandbreite des Angreifers ausschlaggebend für das Gefährdungspotenzial. Bei einem Smurf-Angriff hingegen werden unbeteiligte Maschinen mit eingebunden und damit der Angriff verstärkt.

Lösung zu Kontrollaufgabe 4.6 auf Seite 151

Ein Angreifer sendet einem der beiden Kommunikationspartner ein Paket der angeblich anderen Seite mit neuer Sequenznummer. Dadurch sind schließlich beide Seiten der Meinung, von ihrem Gegenüber andere Sequenznummern erhalten zu müssen. Ist dies der Fall, bricht ein sogenannter Ack Storm aus, da jede Seite ihre Bestätigungen sendet.

Lösung zu Kontrollaufgabe 4.7 auf Seite 151

SYN-Cookies sind eine Gegenmaßnahme gegen DoS-Angriffe. Dabei speichert der Server selbst keinerlei Informationen über ein SYN-Paket in der Backlog-Queue, sondern sendet ein Cookie an den Client. Wenn dieser nicht antwortet, hat der Server lediglich ein wenig Rechenzeit investiert. Antwortet der Client, kommt das Cookie wieder zurück und der Server kann anhand der darin enthaltenen Informationen errechnen, dass er mit diesem Client bereits gesprochen hat.

Lösung zu Kontrollaufgabe 4.8 auf Seite 154

Mit der ersten Anfrage des Clients an den Server werden die ursprüngliche Initialisierung („Client Hello“-Nachricht) und die notwendigen Informationen für die Verschlüsselung bei TLS 1.3 zusammengefasst.

Lösung zu Kontrollaufgabe 4.9 auf Seite 157

Um die Integrität einer DNS-Anfrage abzusichern, steht DNSSEC zur Verfügung.

Um zusätzlich die Vertraulichkeit zu gewährleisten, kann entweder DNS over TLS (DoT) oder DNS over HTTPS (DoH) verwendet werden.

Lösung zu Kontrollaufgabe 4.10 auf Seite 159

Bei einer DHCP Starvation Attack simuliert ein einziger Client viele verschiedene Anfragen an den DHCP-Server mit dem Ziel, den kompletten zur Verfügung stehenden IP-Bereich zu reservieren. Dadurch bekommen weitere Clients keine IP-Adresse mehr zugewiesen.

Lösung zu Kontrollaufgabe 5.1 auf Seite 168

Für die Konfiguration von VLANs werden nur 12 Bits verwendet, wodurch die maximale Anzahl auf 4096 begrenzt ist. Mit VXLAN sind insgesamt 16.777.215 (24 Bits) Varianten möglich, die ihrerseits wieder jeweils 4096 VLANs beinhalten können.

Lösung zu Kontrollaufgabe 5.2 auf Seite 171

Floating IPs werden eingesetzt, wenn nach außen hin eine öffentliche IP-Adresse benötigt wird, die intern flexibl unterschiedlichen Servern zugewiesen werden kann. Dies wird häufig bei Failover-Szenarien verwendet.

Lösung zu Kontrollaufgabe 5.3 auf Seite 175

Der Aufbau von WireGuard ist einfacher, es werden nur wenig verschiedene Algorithmen zugelassen und die Geschwindigkeit ist höher.

Lösung zu Kontrollaufgabe 5.4 auf Seite 177

Durch eine flexiblere Unterteilung kann eine Segmentierung besser erfolgen und die Administration ist systematischer und meist zentralisierter. Gleichzeitig kann damit schneller auf Veränderung, wenn etwa mehr Bandbreite benötigt wird, reagiert werden.

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

VI. Sätze

VII. Tabellen

VIII. Literatur

[1] Steffen Wendzel. *IT-Sicherheit für TCP/IP- und IoT-Netzwerke - Grundlagen, Konzepte, Protokolle, Härtung*. Springer-Verlag, Berlin Heidelberg New York, 2. edition, 2021.

[2] Jürgen Scherff. *Grundkurs Computernetzwerke - Eine kompakte Einführung in Netzwerk- und Internet-Technologien*. Springer-Verlag, Berlin Heidelberg New York, 2010.

[3] DE-CIX Frankfurt statistics. https://www.de-cix.net/en/locations/germany/frankfurt/statistics. Letzter Zugriff: 07.01.2022.

[4] Patrick-Benjamin Bök, Andreas Noack, Marcel Müller, and Daniel Behnke. *Computernetze und Internet of Things - Technische Grundlagen und Spezialwissen*. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.

[5] The Internet Standards Process. https://tools.ietf.org/html/bcp9. Letzter Zugriff: 07.01.2022.

[6] Larry L. Peterson and Bruce S. Davie. *Computernetze - eine systemorientierte Einführung*. Dpunkt-Verlag, Köln, 2008.

[7] Luigi Lo Iacono Christoph Sorge, Nils Gruschka. *Sicherheit in Kommunikationsnetzen*. Oldenbourg Wissenschaftsverlag, München, 2013.

[8] Claudia Eckert. *IT-Sicherheit - Konzepte - Verfahren - Protokolle*. Walter de Gruyter GmbH und Co KG, Berlin, 10. edition, 2018.

[9] Einwegfunktion. https://de.wikipedia.org/wiki/Einwegfunktion. Letzter Zugriff: 07.01.2022.

[10] Joachim Swoboda Stephan Spitzer, Michael Pramateftakis. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. Springer Fachmedien Wiesbaden, 2011.

[11] The ECB Penguin. https://blog.filippo.io/the-ecb-penguin/. Letzter Zugriff: 07.01.2022.

[12] Claudia Eckert. *IT-Sicherheit - Konzepte - Verfahren - Protokolle*. Walter de Gruyter GmbH und Co KG, Berlin, 7. edition, 2012.

[13] IT-Grundschutz-Bausteine. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html. Letzter Zugriff: 07.01.2022.

[14] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile. Letzter Zugriff: 07.01.2022.

[15] Moving Beyond "Blinky Box" Security to Defense-in-Depth Security. https://ussignal.com/blog/moving-beyond-blinky-box-security-to-defense-in-depth-security. Letzter Zugriff: 07.01.2022.

[16] Heise Medien GmbH und Co. K. iX extra - Security. https://www.heise.de/ix/downloads/05/2/7/7/6/8/3/1/ix.2019.10.extra.pdf. Letzter Zugriff: 07.01.2022.

[17] Steffen Wendzel. *IT-Sicherheit für TCP/IP- und IoT-Netzwerke - Grundlagen, Konzepte, Protokolle, Härtung*. Springer-Verlag, Berlin Heidelberg New York, 2018.

[18] Ronald Eikenberg. Hackerangriff auf WhatsApp. https://www.heise.de/security/meldung/Hackerangriff-auf-WhatsApp-1974342.html. Letzter Zugriff: 07.01.2022.

[19] Sicherheitslücke in Realtek-Chips wird angegriffen. https://www.golem.de/news/ddos-sicherheitsluecke-in-realtek-chips-wird-angegriffen-2108-159092.html. Letzter Zugriff: 07.01.2022.

[20] DDoS-Attacken: Angreifer fordern Bitcoin von verschiedenen E-Mail-Anbietern. https://www.heise.de/news/DDoS-Attacken-Angreifer-fordern-Bitcoins-von-verschiedenen-E-Mail-Anbietern-6229016.html. Letzter Zugriff: 07.01.2022.

[21] Bug in iOS: Bestimmte WLAN-Namen legen Netzwerkfähigkeit von iPhones lahm. https://t3n.de/news/bug-ios-wlan-namen-iphone-1386214/. Letzter Zugriff: 07.01.2022.

[22] T-Pot GitHub. https://github.com/telekom-security/tpotce. Letzter Zugriff: 07.01.2022.

[23] Norbert Pohlmann. *Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer-Verlag, Berlin Heidelberg New York, 2019.

[24] Massive Sicherheitslücke im zentralen Corona-Register legte Daten offen. https://www.derstandard.at/story/2000131971545/massive-sicherheitsluecke-im-zentralen-corona-register-legte-daten-offen.

Letzter Zugriff: 07.01.2022.

[25] Schäuble: Meinen Fingerabdruck kann jeder haben. https://www.sueddeutsche.de/digital/datenschutz-schaeuble-meinen-fingerabdruck-kann-jeder-haben-1.276913. Letzter Zugriff: 07.01.2022.

[26] Hacker kopieren Fingerabdruck der Verteidigungsministerin. https://www.dw.com/de/hacker-kopieren-fingerabdruck-der-verteidigungsministerin/a-18154212. Letzter Zugriff: 07.01.2022.

[27] Passwort gegen Brute-Force-Angriff. https://www.mahr-edv.de/passwort-gegen-brute-force-angriff. Letzter Zugriff: 07.01.2022.

[28] Have I Been Pwned. https://haveibeenpwned.com. Letzter Zugriff: 07.01.2022.

[29] Die Handvenenerkennung - Personen berührungslos und sicher identifizieren. https://www.handvenenerkennung.com. Letzter Zugriff: 07.01.2022.

[30] Biometrie: Venen-Scanner schlägt Iris-Messung. https://futurezone.at/science/biometrie-venen-scanner-schlaegt-iris-messung/24.597.953. Letzter Zugriff: 07.01.2022.

[31] Hackerangriff auf Trinkwasser: Immer gleiches Passwort, Windows 7 und Teamviewer. https://heise.de/-5053320. Letzter Zugriff: 07.01.2022.

[32] LDAP und OpenLDAP - Installation und Betrieb unter Linux. https://www.mindux.de/fileadmin/mediapool/pdf/ldap.pdf. Letzter Zugriff: 07.01.2022.

[33] WLAN sichern mit Radius - Individuelle Authentifizierung mit Freeradius unter Linux. https://www.heise.de/ct/artikel/WLAN-sichern-mit-Radius-1075339.html. Letzter Zugriff: 07.01.2022.

[34] Erweiterte Zugangskontrolle fürs LAN - Schlüsselgewalt. https://www.heise.de/select/ix/2018/5/1524882983171288. Letzter Zugriff: 07.01.2022.

[35] Fingbox: ARP-Rowdy mit guten Absichten . https://www.ip-insider.de/fingbox-arp-rowdy-mit-guten-absichten-a-673461/. Letzter Zugriff: 07.01.2022.

[36] Private Auskunft - DNS mit Privacy und Security vor dem Durchbruch. https://www.heise.de/select/ct/2018/14/1530492966691096. Letzter Zugriff: 07.01.2022.

[37] IEEE 802.1Q. https://en.wikipedia.org/w/index.php?title=IEEE_802.1Q&oldid=1058562905. Letzter Zugriff: 07.01.2022.

[38] VLAN Double Tagging Attacks. https://sid-500.com/2017/01/12/vlan-double-tagging-attacks/. Letzter Zugriff: 07.01.2022.

[39] VMware NSX Logical Switch and VXLAN. https://www.oreilly.com/library/view/vmware-nsx-cookbook/9781782174257/7d2a65f0-fadc-4bb9-a507-b25db0886e51.xhtml. Letzter Zugriff: 07.01.2022.

[40] Generic Routing Encapsulation (GRE). https://whatis.techtarget.com/de/definition/Generic-Routing-Encapsulation-GRE. Letzter Zugriff: 07.01.2022.

[41] Harnessing Complex Structures and Collective Dynamics in Large Networked Computing Systems. https://www.researchgate.net/publication/230774628_Harnessing_Complex_Structures_and_Collective_Dynamics_in_Large_Networked_Computing_Systems. Letzter Zugriff: 07.01.2022.

[42] Software-Defined Perimeter: What is It? https://www.appgate.com/blog/what-is-software-defined-perimeter. Letzter Zugriff: 07.01.2022.

[43] Was ist OpenDaylight? https://www.ip-insider.de/was-ist-opendaylight-a-605887/. Letzter Zugriff: 07.01.2022.

[44] LITHIUM OVERVIEW. https://www.opendaylight.org/what-we-do/current-release/lithium. Letzter Zugriff: 07.01.2022.

[45] Was ist OpenFlow? https://www.ip-insider.de/was-ist-openflow-a-605856/. Letzter Zugriff: 07.01.2022.

[46] NTT DATA's Efforts for OpenFlow/SDN. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201211fa9_s.html. Letzter Zugriff: 07.01.2022.

[47] LF Networking Launches Anuket, an Open Source Project to Accelerate Infrastructure Compliance, Interoperability and 5G Deployments. https://www.lfnetworking.org/?p=35978. Letzter Zugriff: 07.01.2022.

[48] What is Network Function Virtualization? https://www.ossline.com/2017/09/what-is-network-function-virtualization-nfv.html. Letzter Zugriff: 07.01.2022.

Stichwörter

Glossar

2FA	Zwei-Faktor-Authentisierung
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CIX	Commercial Internet eXchange
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLR	Distributed Logical Router
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoS	Denial-of-Service
DoT	DNS over TLS
DTLS	Datagram Transport Layer Security
EIAM	Enterprise Identity and Access Management
GAN	Globe Area Network
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communication
HMAC	Hash-based Message Authentication Code
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IXP	Internet Exchange Point
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network

MEC	Mobile Edge Computing
MFA	Multi-Faktor-Authentifizierung
MitM	Man-in-the-Middle-Angriff
NAC	Network Access Control
NFV	Network Function Virtualization
NIC	Network Interface Card
NV	Netzwerk-Virtualisierung
OTP	One-Time-Password
PAN	Personal Area Network
PFS	Perfect Forward Secrecy
PKI	Public-Key-Infrastruktur
PPP	Point-to-Point Protocol
QUIC	Quick UDP Internet Connections
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
SDN	Software Defined Networking
SDP	Software-Defined Perimeter
SIM	Subscriber Identity Module
SMS	Short Message Service
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VXLAN	Virtual eXtensible LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point
WLAN	Wireless Local Area Network

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z214 Netzsicherheit I: IT-Sicherheit von Netzwerken

Die Lehrveranstaltung „Netzsicherheit I: IT-Sicherheit von Netzwerken“ gibt Ihnen einen Überblick über die Bedrohungen und Angriffe gegen Netzwerke. Ferner lernen Sie die eingesetzten Technologien von Rechnernetzen und die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Datennetzen kennen. Es werden die zentralen Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Verteidigungsmaßnahmen erläutert. In Übungen im virtuellen Labor führen Sie selbst Angriffe durch, um im Anschluss Bedrohungsszenarien nachvollziehen und einordnen zu können.

Im ersten Studienbrief „Netzwerktechnik und IT-Sicherheit“ werden Grundlagen in den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit behandelt, um vorhandenes Wissen zu reaktivieren und eine gemeinsame Ausgangsbasis für dieses Modul zu schaffen.

Im zweiten Studienbrief „Angriffs- und Sicherheitskonzepte“ erlernen Sie, wie generelle Sicherheitskonzepte für Netzwerke realisiert werden. Anhand realitätsnaher Angriffsszenarien und relevanter Verteidigungsmaßnahmen werden Sicherheitseigenschaften von Netzwerktechnologien praxisorientiert vorgestellt.

Im dritten Studienbrief „Identitäts- und Zugriffsmanagement“ wird ein Überblick über das Thema Zugriffsteuerung gegeben. Die Anmeldung und Autorisierung einzelner Benutzer und Systeme stellen ein wichtiger Grundpfeiler für den sicheren Betrieb von Netzwerkdiensten dar. Es werden etablierte Protokolle und Systeme behandelt und wie diese sicher betrieben werden.

Im vierten Studienbrief „Angriffe auf Netzwerkprotokolle“ werden konkrete Angriffsmethoden und Sicherheitslösungen der LAN/WAN-Netze anhand des Schichtenmodells vorgestellt. Sie lernen konkrete Bedrohungen für verschiedene Netzwerkprotokolle kennen und welche Schutzmaßnahmen gegen diese Angriffe realisiert werden können.

Im letzten Studienbrief „Sicherheit von virtuellen Netzwerken“ wird ein Ausblick auf flexible und softwaregesteuerte Netzwerktechniken gegeben. Anhand verschiedener Konzepte und Protokolle werden die Grundlagen von virtualisierten Netzwerken erläutert.

Nach erfolgreichem Abschluss des Moduls haben Sie Kenntnisse über die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Netzwerken und können die verwendeten Sicherheitskonzepte einordnen. Sie sind in der Lage, Bedrohungen und Angriffe gegen Netzwerke einzuordnen, und haben sich Wissen über die Anwendung von Programmen angeeignet, um die Möglichkeiten und Grenzen dieser Tools selbst einzuschätzen zu können. Damit sind Sie in der Lage, Maßnahmen zur Verbesserung der Netzsicherheit umzusetzen.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten kön-nen sie auf ein Studium angerechnet werden.

http://zertifikatsprogramm.de