Schwachstellenanalyse in der Kommunikation von Medizingeräten am Beispiel von B. Braun Infusionspumpen

Bachelorarbeit
Zur Erlangung des Grades Bachelor of Science
des Fachbereichs Informatik und Medien der
Technischen Hochschule Brandenburg

Vorgelegt von:
Tino Nicksch

Betreuer: Prof Dr. Pilgermann
Zweitgutachter: Prof. Dr. Purohit

Brandenburg an der Havel, 20. Dezember 2022

I Kurzfassung

Der Einfluss von Technik in der Medizin wird immer deutlicher. Hierbei steigt auch im gleichen Maß die Bedrohung auf das Gesundheitswesen durch Cyberkriminalität. [1] Diese Arbeit umfasst eine Schwachstellenbetrachtung und Analyse der Kommunikation zweier B. Braun Infusionspumpen und dem dazugehörigen Konfigurationswerkzeug, der „Online-Suite“. Hierbei wurde ein Fokus auf vor allem drei Untersuchungsmethoden gelegt: 1. Ein Portscan mittels „Nmap“, welcher bereits erste, leicht einsehbare Informationen über die verwendeten Ports und Dienste aufdecken sollte. 2. Ein Schwachstellenscan durchgeführt mit „GVM/OpenVAS“, welcher die einzelnen Schwachstellen der Dienste und Software an Hand von einem „CVSS-Wert“ bewertet. 3. Eine Betrachtung des Netzwerkverkehrs in Wireshark, um den Aufbau der Kommunikation zu analysieren. Hierbei ergaben sich diverse Sicherheitsrisiken und Probleme. Diese können im schlimmsten Fall auch die Sicherheit des Patienten beeinflussen. Besonders häufig wurden hierbei Schwachstellen gefunden, welche durch veraltete und nicht weiter unterstützte Software bedingt waren.

Schlüsselwörter

Schwachstellenscan, Medizingeräte, Infusionspumpen, Sicherheit, Patientensicherheit

II Abstract

The influence of technology on medicine is growing rapidly. Simultaneously, the threat of cyber crime in medicine is growing to the same extent. [1] Part of this thesis is a vulnerability consideration and analysis of the communication between two B. Braun infusion pumps and their configuration tool, the “Online-Suite”. This thesis focuses primarily on three methods of analysis: First, a port scan using “Nmap”, which’s main task is to discover all open ports as well as identifying the services running on these ports. Secondly, a vulnerability scan with “GVM/OpenVAS”, which evaluates the vulnerabilities of the used services based on their “CVSS-Score”. Lastly, an analysis of the network traffic and its structure using “Wireshark”. This results in various security risks and issues being found. These may lead up to compromised safety for the patient. Particularly common were vulnerabilities which were caused by deprecated software.

Keywords

Vulnerability Scan, Medical Devices, Infusion Pumps, Security, Patient Safety

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

Die Digitalisierung ist ein immer weiter fortschreitender Prozess und beeinflusst mittlerweile jeden Aspekt unseres Lebens. Dazu gehören auch Fortschritte im Gesundheitswesen. Gleichzeitig erhöht sich jedoch dabei auch die Gefahrenlage und das Risiko in solchen Bereichen.

Laut einer Einschätzung der „European Union Agency for Cybersecurity“ (ENISA) handelt es sich beim Gesundheitswesen um einen der am meisten betroffenen Sektoren, wenn es um die reine Anzahl an Vorfällen von Cyberbedrohungen geht. Weiter vorne sind hierbei nur Sektoren wie die der öffentlichen Verwaltung, generelle öffentliche Dienste oder digitale Dienstleister. [2]

Hierbei entsteht nun die Frage, wie sicher das Gesundheitswesen ist bzw. wie sicher die dort benutzten Gerätschaften sind. Diese Arbeit soll am Beispiel von B. Braun Infusionspumpen (Infusomat Space) eine Schwachstellenanalyse durchführen und auswerten. Hierbei steht die Kommunikation dieser Medizingeräte im Vordergrund und weniger die Hardware der Produkte selber. Die Kommunikation der Geräte beruht größtenteils auf Kommunikation innerhalb des Netzwerks sowie dem Informationsaustausch mit einer „Online-Suite“. Diese dient als Konfigurationswerkzeug und erweitert die Bedienung der Infusionspumpen.

Ziel der Arbeit ist es, eine Sicherheitsbetrachtung und Analyse der Kommunikation zwischen den Pumpen und der Online-Suite durchzuführen. Hierzu gehören vor allem auch die benutzten Dienste, Ports oder weitere Software, welche in einem Netzwerk kommunizieren. Im gleichen Maße soll dabei sowohl der Aufbau und die Struktur der Kommunikation als auch die dabei entstehenden Sicherheitsrisiken erläutert und thematisiert werden.

1.1 Zielsetzung

Wie bereits beschrieben, ist das Ziel der Arbeit eine genaue Untersuchung des Netzwerkverkehrs medizinischer Geräte am Beispiel von zwei B. Braun-Pumpen. Hierfür soll diese mit einem Fokus auf Datensicherheit analysiert und beschrieben werden.

Das bedeutet, dass zunächst eine detaillierte Beschreibung und Erfassung des Netzwerks bzw. der Pumpen erfolgen wird. Diese beinhaltet verschiedene Aspekte wie einen Netzwerk- und Portscan. Danach folgt eine ähnliche Erfassung zu den benutzten Diensten mittels eines

Schwachstellenscans. Dies deckt erste mögliche Sicherheitsrisiken auf. Dies schafft dann Grundlagen für das weitere Vorgehen.

Der dritte Hauptteil dieser Arbeit besteht dann aus einer Untersuchung und Aufschlüsselung des Netzwerkverkehrs mittels eines „Packet-Analysers“. Hierfür werden vor allem Netzwerkprotokolle und der Aufbau weiter untersucht.

1.2 Aktueller Stand der Literatur

Aktuell gibt es nur wenige Arbeiten, die genau dieses Thema abdecken. Hierbei sticht vor allem eine ähnliche Arbeit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus dem Jahr 2020 heraus.

Unter dem Projektnamen „ManiMed“ untersuchte das BSI stichprobenartig Medizinprodukte aus verschiedenen Kategorien und testete diese auf Schwachstellen. Hierbei wurden insgesamt 150 Probleme festgestellt. Diese sind jedoch nicht nur auf Lücken in der Kommunikation, sondern auf alle Aspekte zurückzuführen. Das schließt auch Softwarefehler wie z.B. Bufferoverflows ein, welche keinen direkten Bezug zur Kommunikation des Gerätes besitzen. Untersucht wurden die Medizingeräte ebenfalls mithilfe eines Penetrationstests. Das BSI selber schrieb im Abschnitt 7 des Papers, dass sie jedoch keinen Anspruch auf Vollständigkeit erheben. [3]

Weitere verwandte Literatur findet sich im ERNW Whitepaper 66, welches bereits 2018 eine rein theoretische Analyse des Sicherheitsstands verschiedener Medizinprodukten durchführte. Hier wurden jedoch selber keine Tests oder Untersuchungen angeführt. Auch hier wurde festgestellt, dass Sicherheitsschwachstellen existieren und diese eine Gefahr für den Patienten darstellen. Außerdem wurde festgestellt, dass das Risiko und die Gefährdung jährlich zunimmt. Gleichzeitig konnte jedoch nicht nachgewiesen werden, dass alle diese Probleme durch ungenügende Sicherheitsstandards bedingt sind. [4] Es könnte demnach auch durch andere Ursachen bedingt sein.

1.2.1 Genereller Stand der IT-Sicherheit in Deutschland

Die Gefährdung der IT-Sicherheit in Deutschland nimmt in den letzten Jahren immer mehr zu. Dies wird auch durch das BSI in ihrem Lagebericht zur IT-Sicherheit in Deutschland 2021 bestätigt. So beschreibt das BSI die Gefahrenlage in Deutschland als angespannt bis kritisch. Im Vergleich zum letzten Jahr stiegen die Anzahl der täglich neuen Schadprogramm-Varianten

um 22% zum Jahr 2020. Besonders häufig vertreten waren hierbei Cyber-Erpressungsmethoden. Dazu gehören vor allem Löse-, Schutz- und Schweigegelderpressungen. Die Jahre 2020 sowie 2021 stellten schwere Herausforderungen für viele Behörden, Organisationen und Unternehmen. Durch die Umstellung auf das Arbeiten im Homeoffice kam es zu einer Zunahme von Cyber-Angriffen. [5] Laut einer Umfrage zum Thema IT-Sicherheit im Homeoffice aus dem Jahr 2020 hat dies besonders kleine Unternehmen getroffen. 25% der Unternehmen mit weniger als 50 Beschäftigten erfuhren sehr schwere bis existenzbedrohende Folgen aus Cyberattacken während des Homeoffice. [6]

Der Lagebericht des BSI zur IT-Sicherheit in Deutschland 2022 legte zusätzlich auch einen besonderen Fokus auf den russischen Angriffskrieg gegen die Ukraine. Das BSI fand hierbei eine Reihe von kleineren Vorfällen, jedoch wird keine größere Angriffskampagne gegen deutsche Ziele erwartet. [7] Konträr dazu, steigen jedoch die Trends der vergangen Jahre weiter an. Besonders die bereits aufgezeigten Bedrohungen der Cyber-Erpressung steigen weiter an. Dazu gehörten in diesem Jahr sowohl die Anzahl der Opfer solcher Erpressungen, als auch die gezahlten Geldsummen. Hierbei wurden vor allem umsatzstarke Unternehmen Ziel dieser Angriffe. Jedoch blieb es nicht nur bei diesen, sondern es kam auch zu Angriffen auf mehrere Kommunen, welche über Monate mit Störungen zu kämpfen hatten. [8]

1.2.2 Stand der IT-Sicherheit von Medizingeräten

Ähnlich wie auch in *1.2.1 Genereller Stand der IT-Sicherheit in Deutschland* ist auch der Stand der Medizingeräte selber alarmierend. So gab es bereits in der Vergangenheit schon Rückrufe von wichtigen Medizingeräten wie Herzschrittmachern, da diese fatale Sicherheitslücken aufwiesen. Dazu gehörten u. a. auch die Steuerung der Batterie (Akku). Behoben wurde dies durch ein Firmware-Update beim Arzt. Bereits hierbei wird deutlich, dass ein hoher Grad an Sicherheit nur durch regelmäßiges Aktualisieren der Software garantiert werden kann. Veraltete Software riskiert sowohl die Sicherheit des Patienten als auch die Vertraulichkeit der persönlichen Daten. [9] Außerdem ist zu beachten, dass das Gesundheitswesen besonders häufig zum Opfer für Cyberkriminalität wird. Hierbei haben bis zu 94% aller medizinischen Einrichtungen in den letzten zwei Jahren einen Datendiebstahl gemeldet. Hierzu gehören vor allem der Diebstahl von medizinischen Akten, Abrechnungen sowie Versicherungsdokumente. [1] Eine weitere Untersuchung ergab außerdem, dass einige der untersuchten Geräte offene Sicherheitsrisiken besitzen, wie das Nutzen von Standardanmeldeinformationen („default

credentials“), welches bereits durch ordnungsgemäße Schulung des Personals vermieden werden könnten. [10]

2. Methodik

Dieser Teil der Arbeit behandelt das methodische Vorgehen und stellt im Folgenden die verwendeten Programme und Werkzeuge vor. Die Arbeit orientiert sich in ihren ersten Schritten an einem traditionellen Penetrationstest, jedoch weicht sie ab von den klassischen Endphasen eines Penetrationstests.

2.1 Ablauf eines Penetrationstests

Zur Analyse und methodischen Suche nach Schwachstellen in den Gerätschaften wurden verschiedene Technologien genutzt. Diese unterscheiden sich u. a. durch die Phasen in welchen sie benutzt werden. Ein allgemeiner Penetrationstest unterteilt sich in der Regel in fünf Phasen, wobei je nach Quelle die Phasen auch anders benannt werden. Ein traditioneller Penetrationstest verläuft üblicherweise über folgende Phasen:

Phase eins ist die Informationsbeschaffung (Reconnaissance). Hierbei werden zunächst Informationen über das Ziel beschafft. Je nach Perspektive gehört hier jedoch noch keine Scanning-Aktivitäten dazu, sondern lediglich eine Informationsbeschaffung über Google-Anfragen oder Literaturrecherchen. Im speziellen Fall dieser Arbeit zählt jedoch auch das Scannen von z.B. Netzwerken zur ersten Phase. [11] Dafür eignet sich ein vor allem ein „Network-Scanner“.

Phase zwei geht hierbei nahtlos über und kann durchaus auch Teile von Phase eins beinhalten. Spätestens hier kommen Network-Mapper ins Spiel, um verschieden Informationen wie offene Ports, Dienste, Softwareversionen oder andere mögliche Schwachstellen zu ermitteln. Weiterhin werden hier auch Schwachstellenscanner benutzt, um einen ersten Eindruck vom Gesamtsystem zu erhalten. [11]

Phase drei nutzt nun die in Phase eins und zwei ermittelten Schwachstellen aus und versucht so, je nach Ziel des Angriffes, unerlaubten Zugriff zu erhalten, Dienste zu stören oder vertrauliche Daten zu entwenden. [11]

Phase vier versucht versteckte Hintereingänge (Backdoors) zu erstellen, um im Anschluss jederzeit wieder in das System eindringen zu können. [11]

In Phase fünf wird versucht, die Spuren zu verwischen und alle möglichen Beweise zu eliminieren. [11]

Diese Arbeit unterscheidet sich jedoch besonders zum Ende in großen Teilen von einem traditionellen Penetrationstest. Das Ziel dieser Arbeit ist es, eine Analyse der Phase eins und zwei zu erstellen und diese auszuwerten. Phase drei, vier und fünf verfolgen ein anderes Ziel und werden deswegen in dieser Arbeit nicht weiter thematisiert.

2.2 Vorstellung der Software-Werkzeuge

Im folgenden werden die wichtigsten Werkzeuge und Begriffe vorgestellt und erklärt, welche in den aufgezeigten Phasen verwendet werden.

2.2.1 Nmap – Vorstellung

Bei Nmap handelt es sich um ein Open-Source-Programm, welches spezialisiert für das Scannen von Netzwerken entwickelt wurde. [12] Nmap ist besonders geeignet, wenn es um Port-Scanning geht. Dabei untersucht Nmap das gesamte Netzwerk und schickt an jeden Port eine Anfrage, um auf diese Weise zu ermitteln, welche Ports offen sind. Auf diese Weise können auch Dienste (Services) und auch Versionen ermittelt werden, die auf den einzelnen Ports laufen. [13]

2.2.2 OpenVAS / GVM - Vorstellung

Bei dem Programm OpenVAS handelt es sich um einen Sicherheitsschwachstellenscanner. Hierbei werden durch verschiedene Datenbanken generische Testangriffe auf ein Gerät oder ein Programm vollzogen, um zu prüfen, ob es offene Schwachstellen gibt. [14] Mittlerweile ist OpenVAS bekannt unter Greenbone Vulnerability Manager (GVM) und wird täglich erweitert. Hierbei werden unter anderem jeden Tag neue „Network Vulnerability Tests“ (NVTs) zur Verfügung gestellt. Die Gesamtanzahl beläuft sich auf über 50.000 (Stand 2020). [15]

2.2.3 Wireshark – Vorstellung

Bei Wireshark handelt es sich um ein Netzwerkprotokoll-Analysierer. Wireshark ermöglicht das Nachvollziehen und Analysieren von Netzwerkverkehr auf Protokoll-Ebene. [16] Diese

Daten werden in Form von einzelnen Paketen dargestellt und dann durch Wireshark in Segmente, mittels Farben, eingeteilt. Verschiedene Filter ermöglichen eine tiefgreifende Analyse des Netzwerkverkehrs. [17] Um Netzwerkverkehr mit aufzuzeichnen wird in dieser Arbeit, in Form eines PacketSquirrels, eine „man-in-the-middle“-Lösung verwendet.

2.2.4 PacketSquirrel – Vorstellung

Beim PacketSquirrel handelt es sich um ein physisches Hosentaschen großes „man-in-the-middle“-Gerät. Dies ermöglicht das Zwischenschalten zwischen zwei kommunizierenden Geräten und die Aufzeichnung dieses Verkehrs. [18] Der in dieser Arbeit verwendete PacketSquirrel speichert die aufgezeichneten Daten in Form eines „tcpdumps“ (tcpdump ist ein Packet-Analyzer bzw. Packet-Sniffer [19]). Angeschlossen wird der PacketSquirrel zwischen den Pumpen und dem Internetzugang. Diese Datei kann dann anschließend in einem passenden Programm, in diesem Fall Wireshark, analysiert werden.

2.2.5 CVSS – Begriffserklärung

Das „Common Vulnerability Scoring System“ (CVSS) stellt eine Metrik zum Messen für allgemeine Sicherheitsschwachstellen von Software dar. Die Auswertung ergibt ein numerisches Ergebnis von null bis zehn. Hierbei steht die Null für kein und die Zehn für das größtmögliche Risiko. Diese Bewertung ergibt sich dann aus verschiedenen Variablen wie z.B. Schweregrad des Risikos oder die Wahrscheinlichkeit, dass ein Angreifer diese Lücke ausnutzt. Dieses Ergebnis kann dann noch weiter beeinflusst werden durch zeitlich und umgebungsvariable Einflüsse. [20] Diese Arbeit verwendet ebenfalls zu Teilen das CVSS und beurteilt so Teile der Analyse der GVM-Scans.

3. Durchführung

Dieser Teil der Arbeit beschreibt die genaue Zielsetzung und Durchführung. Daraus ergibt sich, dass dieser Teil sich mit der genauen Beschreibung der Vorgehensweise beschäftigt. Dies schließt sowohl die ersten Schritte des Penetrationstests ein, als auch die Analyse dessen. Um die Durchführung einfacher verständlich zu machen, stellt *3.1 Aufbau des Experiments* die Eckdaten des Aufbaus weiter vor.

3.1 Aufbau des Experiments

Um die Beziehungen der einzelnen Komponenten deutlicher zu visualisieren, stellt Abbildung 1 einen Netzplan der wichtigsten Elemente dar.

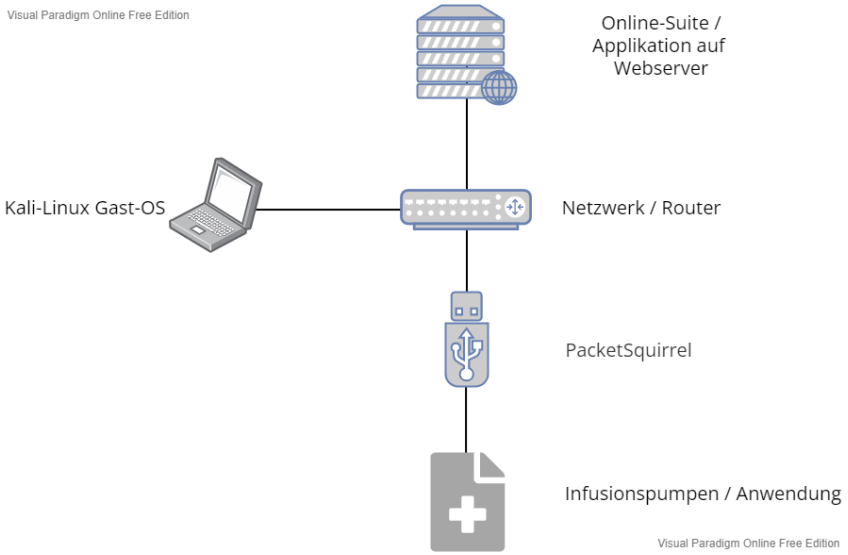


Abbildung 1: Netzplan des Versuchs

Hierbei kommunizieren die Infusionspumpen über das (i. d. R. öffentliche) Netzwerk mit der Online-Suite. In den Versuchen dieser Arbeit wurde hierfür zwischen dem Netzwerk und den Infusionspumpen der PacketSquirrel geschaltet, wodurch jeglicher Verkehr, sowohl von als auch zu den Pumpen aufgezeichnet werden konnte. Sowohl die Portscans, als auch die Schwachstellenscans wurden über einen Windows-Laptop mit einer virtuellen Kali-Linux Maschine durchgeführt. Dieser Laptop befand sich hierbei im selben, öffentlichen Netzwerk wie die Infusionspumpen.

Bei der Online-Suite handelt es sich um eine Applikation auf einem Webserver, für eine einheitliche gebündelte Plattform für alle internen Anwendungen im Krankenhaus. Hierbei ermöglicht die Installation auf einem Server die Bedienung der Online-Suite von jedem Netzwerk-internen Krankenhaus-Webbrowser und damit auch die Steuerung von z.B. jeder verbundenen Infusionspumpe. Die Online-Suite ist dabei ein Konfigurationswerkzeug sowie ein Bündel von Managersystemen. Ein Beispiel hierfür ist der „Drug Library Manager“ (zu deutsch: Medikamentendatenbank Manager), welcher die zentrale Verwaltung von Medikamentendatenbanken ermöglicht. [21]

Die Infusionspumpen selber sind hierbei i. d. R. nur das ausführende Gerät der Online-Suite. Obwohl es auch möglich ist, kleinere Einstellungen an den Infusionspumpen selber anzupassen, benötigt der Nutzer für die zentrale Verwaltung sowie das Einstellen der Medikamentendatenbanken die Online-Suite.

Zuletzt listet die folgende Tabelle alle verwendeten Hard- und Softwarewerkzeuge mit der jeweiligen Version auf:

Name	**Version**	**Anwendung**
Windows 11	Windows 11, version-22h2	Host für das Kali-Linux-System
Kali-Linux	Kali Linux 2022.2 virtualbox-amd64 (Debian 64-Bit)	Gast-OS für die Port- sowie die Schwachstellenscans
Nmap	Nmap-version-7.92	Portscanner
GVM/OpenVAS	GVM-21.4.3	Schwachstellenscanner
GVM Datenbanken	NVT: 20220905T1012 SCAP: 20220905T0444 CERT: 20220905T0643 GVMD_DATA: 20220804T1333	Datenbanken zum Finden von Sicherheitsschwachstellen
PacketSquirrel	PacketSquirrel hergestellt von hak5	Gerät zum Mitschneiden von Netzwerkverkehr
Wireshark	Version-3.6.8-gd25900c51508	Netzwerkprotokollanalyse

Tabelle 1: Auflistung aller verwendeten Hard- und Softwarewerkzeuge

3.2 Portscans

Die Tests begannen mit verschiedenen Portscans, durchgeführt mit Nmap. Insgesamt durchgeführt wurden acht Scans, aufgeteilt auf sowohl die Pumpen als auch die Online-Suite. Die Scans unterschieden sich in Bezug auf die Zielsetzung. Alle Scans wurden lokal vor Ort auf einer virtuellen Kali-Linux Maschine auf einem Windows Host durchgeführt.

Begonnen wurde mit einem Standard TCP-Scan. Dieser wurde mit dem Befehl „sudo nmap –p- bbraunspacecom.th-brandenburg.de“ bzw. mit „sudo nmap –p- mzi-bbraun-th-

brandenburg.de*“* auf der Kali-Kommandozeile gestartet. Dieser Befehl besteht aus mehreren Parametern, angefangen mit *sudo*. Sudo stand ursprünglich für *super user do* und vermittelt Linux, dass der folgende Befehl mit Administratorrechten ausgeführt werden soll. *Nmap* startet einen standardmäßigen TCP-Portscan und würde ohne weitere Parameter lediglich die 1000 meistgenutzten TCP-Ports scannen. Hierbei unterscheidet Nmap dann gefundene Ports in sechs verschiedene Zustände: offen, geschlossen, gefiltert, ungefiltert, offen | gefiltert oder geschlossen | gefiltert. Außerdem ist hierbei zu beachten, dass Nmap die Ports lediglich so unterscheidet, wie Nmap sie selber sieht, nicht zwangsweise wie sie wirklich sind. Das bedeutet, dass Nmap innerhalb eines Netzwerkes den Zielport als offen ansehen kann und gleichzeitig außerhalb dieses Netzwerks als gefiltert. [22] Der Parameter *–p-* weist Nmap an alle Ports von 1 bis 65535 zu scannen. [23] Zum Schluss muss noch eine Zieladresse angegeben werden. Hier wird entweder *bbraunspacecom.th-brandenburg.de* für die Pumpen angegeben oder *mzi-bbraun-th-brandenburg.de* für die Online-Suite. Ein Ausschnitt des TCP-Scans sowohl der Pumpen als auch der Online-Suite ist im Anhang 1.1 zu finden.

Als die TCP-Scans abgeschlossen waren, wurden als nächstes UDP-Scans durchgeführt. Ähnlich wie beim TCP-Scan wurden hier wieder mit dem fast gleichen Nmap Befehl gearbeitet. Eine genauere Erklärung erübrigt sich damit. Lediglich zwei wichtige Veränderungen wurden getätigt. Es wurde ein weiterer Parameter hinzugefügt (*-sU*), welcher den Scan-Modus auf UDP wechselt. Außerdem wurde der Parameter *–p-* diesmal weggelassen. Auch der UDP-Scan von Nmap scannt nur die am häufigsten benutzten 1000 Ports in seiner Standardauswahl, braucht jedoch bereits auch dafür erheblich länger als ein TCP-Scan im selben Netzwerk. [24] Während der TCP-Scan der Pumpen 22 Sekunden brauchte, waren es beim UDP-Scan bereits 18 Minuten. Bei einem gleichbleibenden durchschnittlichen Zeitverbrauch würde ein gesamter Scan aller möglichen UDP-Scans weit über 16 Stunden gehen und war damit nicht vor Ort realisierbar. Ein Ausschnitt der UDP-Scans sowohl der Pumpen als auch der Online-Suite ist im Anhang 1.2 zu finden.

Mit Abschluss der UDP-Scans wurden als nächstes „OS-Detection“-Scans („Operating System“ englisch für Betriebssystem) durchgeführt. Hierbei schickt Nmap verschiedene TCP- und UDP-Pakete an das Ziel und analysiert die Antwort. Durch ein Abgleich mit der internen Datenbank kann Nmap so mit einer gewissen Wahrscheinlichkeit ein Betriebssystem bzw. auch die Version des Betriebssystems ermitteln. Aktiviert wird der OS-Detection-Scan mit dem Parameter *–O.* [25] Ein Ausschnitt der OS-Detection-Scans sowohl der Pumpen als auch der Online-Suite ist im Anhang 1.3 zu finden.

Nachdem die OS-Detection-Scans abgeschlossen waren, wurden „SV-Detection“-Scans („Service and Version“-Scans) durchgeführt. Ähnlich wie beim OS-Detection-Scan werden hierbei verschiedene Dienste und Versionen ermittelt, indem Antworten des Ziels interpretiert, analysiert und mit einer Datenbank intern verglichen werden. Gestartet wird ein SV-Detection-Scan mit dem Parameter *–sV*. [26] Ein Ausschnitt der SV-Detection-Scans sowohl der Pumpen als auch der Online-Suite ist im Anhang 1.4 zu finden.

Nicht erkannte Dienste werden in Form eines Fingerabdrucks und einer URL ausgegeben und können dann bei Nmap gemeldet werden, sofern der Dienst oder das Betriebssystem bekannt ist. Dies erweitert Nmaps Datenbank und verbessert so das Detektieren von Diensten, Versionen und Betriebssystemen. [26] Anhang 1.4 zeigt verschiedene nicht erkannte Dienste und deren Fingerabdrücke.

3.3 Schwachstellenanalyse

Während den Portscans wurden ebenfalls die Schwachstellenscans mit OpenVAS eingeleitet. Die Datenbanken wurden hierbei nur wenige Tage zuvor aktualisiert und die Tests wurden vor Ort durchgeführt. Analysiert wurden hierbei lediglich die Pumpen, denn auch bei wiederholten Versuchen war es nicht möglich einen OpenVAS-Scan bei der Online-Suite zu starten. Wie auch beim Mitschneiden des Netzwerkverkehrs wurden in zwei Phasen Scans durchgeführt. Ein Scan wurde vor der Aktualisierung des Pumpensystems durchgeführt und einer danach. Die vollständigen Ergebnisse befinden sich im angehängten Ordner.

Bei den Scans ergaben sich außerdem noch einige wichtige Anmerkungen. Zum einen wurden verschiedene Ergebnisse direkt herausgefiltert und somit gar nicht erst angezeigt. Dazu gehören:

Resultate, die als „Log“ gekennzeichnet sind, beinhalten in der Regel sehr detaillierte Beschreibungen und Informationen. Oftmals sind hierhinter Name eines Dienstes oder dessen Versionsnummer versteckt. [27]

Ist ein Ergebnis mit „Debug“ gekennzeichnet, so enthält es Informationen, welche für das Debuggen des Systems wichtig sein können. [28]

Ein Ergebnis, welches als „False Positive“ gekennzeichnet ist, weist eine Schwachstelle auf, welche nicht existiert. [27]

Des Weiteren ist für die weitere Bearbeitung und im Besonderen für die Vorstellung der Ergebnisse ein weiterer Parameter wichtig. Der „Quality of Detection“-Wert (QoD) gibt die Genauigkeit sowie die Art der Verifizierung der Schwachstelle an. Bei einem hohen QoD-Wert findet der Scan ggf. nicht alle Schwachstellen, schließt dafür aber auch zu einer größeren Wahrscheinlichkeit Fehler, wie z.B. ein falsch-positives Ergebnis, aus. Ein QoD von 100% liefert nur Ergebnisse, welche durch einen Exploit detektiert wurden und somit vollständig verifiziert sind. Ein QoD von 70%, wie auch beim Scan der Infusionspumpen, führt einige Überprüfungen durch, garantiert aber keine vollständige Verifizierung. Trotz des Filters von einem QoD von 70%, wird für jedes Resultat des Scans nochmals der QoD-Wert angegeben. [29]

3.4 Netzwerkverkehr aufzeichnen

Abschließend wurden Teile des Netzwerkverkehrs mitgeschnitten mittels des PacketSquirrel. Hierfür wurde zwischen der Dockingstation der Pumpen und dem Netzwerkkabel das Gerät zwischengeschaltet und ermöglichte es so den gesamten Netzwerkverkehr aufzuzeichnen. Hierbei wird an den PacketSquirrel ein USB-Stick angeschlossen, welcher die aufgezeichneten Daten speichert. Nachdem alles angeschlossen ist, benötigt das Gerät einige Zeit zum Hochfahren und konnte dann, sobald dieses startbereit war, für circa fünf Minuten pro Durchlauf den Netzwerkverkehr aufzeichnen. Hierbei wurden verschieden Versuche durchgeführt. Bei jedem Versuch wurde der PacketSquirrel zuvor eingeschaltet und im Anschluss wieder ausgeschaltet. Somit ergeben sich für jeden Versuch eigene Dateien. Im Folgenden werden jedoch nur die relevanten Durchgänge erläutert und auch ausgewertet.

Angefangen wurde mit dem Aufzeichnen im ausgeschalteten Zustand (Standby-Modus). Hierbei war das Gerät noch an eine Stromquelle angeschlossen und wurde lediglich über die „Power“-Taste ausgeschaltet. Es war sichtlich erkennbar, dass der Bildschirm noch zu Teilen eingeschaltet war.

Zwei weitere Versuche behandelten das Einlegen sowohl einer Spritze als auch eines Tropfenreglers. Nach dem jeweiligen Einlegen wurden außerdem noch verschiedene Parameter eingestellt. Die Spritze erhielt als Rate 5ml/h, als Volumen 11ml/h und sollte für circa zwei Stunden laufen. Zusätzlich ertönte zuvor ein Erinnerungsalarm nach ungefähr zwei Minuten. Dies ist zurückzuführen auf das zu langsame Einführen der Spritze. Der Tropfenregler wurde mit denselben Parametern eingestellt. Bei diesem ertönte jedoch kein Erinnerungsalarm.

Einige Tage, nachdem alle Versuche abgeschlossen waren, wurde ein neues Sicherheitsupdate auf den Geräten installiert. Aus diesem Grund wurde ein Teil der Versuche wiederholt, um einen Vergleich zu ermöglichen.

Zunächst ist es wichtig zu erwähnen, dass während der Gesamtheit aller Tests, die nach dem Sicherheitsupdate durchgeführt wurden, eine dunkelgelbe, leicht rot leuchtende LED an dem PacketSquirrel leuchtete. Bei einer fehlerfreien Aufzeichnung sollte diese LED lediglich gelb leuchten. Ein rotes Leuchten signalisiert ein Fehler beim Aufzeichnen der Daten. Ein dunkelgelbes, leicht rotes Leuchten ist nicht in der Dokumentation des PacketSquirrel zu finden. [30] Trotzdem erzeugte der PacketSquirrel eine Wireshark-funktionsfähige Datei.

Wieder wurden hier beide Pumpen parallel geschaltet. Diesmal wurden jedoch keine Parameter direkt eingegeben, sondern über die Medikamentendatenbank der Online-Suite heruntergeladen. Diese musste zunächst erneut in den Standby-Modus gebracht werden, bevor sie den Eintrag herunterladen konnten. Hierbei wurde der Tropfenregler mit den Werten 20mg/1ml als Rate und 5ml/h als Volumen eingestellt. Die Spritze erhielt denselben Wert für die Rate und ein Volumen von 4ml/h.

4. Ergebnisse

Dieser Teil der Arbeit präsentiert die erzielten Ergebnisse der zuvor beschriebenen Versuche. Hierbei werden die Ergebnisse, wie zuvor auch in der Durchführung, eingeteilt in die drei Kategorien der Erhebungen. Begonnen wird hierbei ebenfalls mit den Portscans.

4.1 Ergebnisse der Portscans

Die Ergebnisse der Portscans teilen sich untereinander auf die verschieden getätigten Scans auf. Diese sind dann ein weiteres Mal in die Scans der Pumpen und die Scans der Online-Suite unterteilt. Im Folgenden werden jeweils nur Ausschnitte der Ergebnisse vorgestellt. Die vollständigen Ergebnisse befinden sich im Anhang 1.

4.1.1 Ergebnisse der TCP-Scans

Der TCP-Scan der Pumpen ergab insgesamt fünf offene Ports: Port 80, Port 443, Port 1500, Port 4001 und Port 4002. Alle anderen Ports sind geschlossen. Abbildung 2 zeigt hierbei einen Ausschnitt der Ergebnisse.

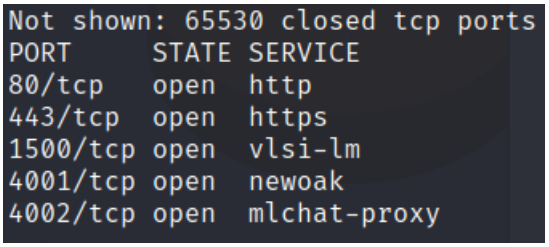


Abbildung 2: Ausschnitt der Ergebnisse des TCP-Scans der Pumpen

Zunächst finden sich hierbei die folgenden beiden Ports: Port 80 und Port 443. Auf diesen läuft standardmäßig http und https. Dieser Standard ist zum einen weit verbreitet sowie auch offiziell von der „Internet Assigned Numbers Authority“ (IANA) vergeben. Auch bei Port 1500 und Port 4001 handelt es sich um registrierte Ports. Bei „vlsi-lm“ handelt es sich zusätzlich um den „VLSI License Manager“. Port 4002 ist standardmäßig nach den Vorgaben der IANA an einen anderen Dienst vergeben. [31]

Der Scan der Online-Suite fand vier geöffnete Ports: Port 80, Port 443, Port 3389 und Port 7680. Alle anderen TCP-Ports konnten nicht weiter bestimmt werden, da diese keine Antwort lieferten. Nmap kennzeichnete diese als „filtered“. [22] Abbildung 3 zeigt hierbei einen Ausschnitt der Ergebnisse.

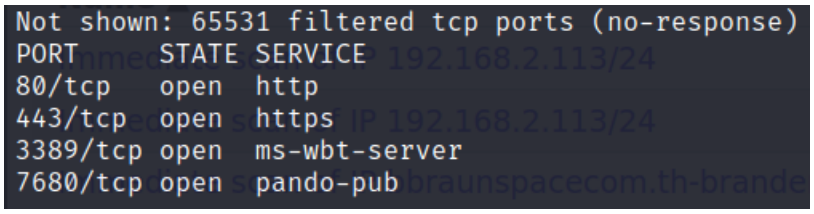


Abbildung 3: Ausschnitt der Ergebnisse des TCP-Scans der Online-Suite

Die ersten beiden Ports, sind hierbei erneut standardmäßig „http“ und „https“. Auf Port 3389 läuft „ms-wbt-server“. Hierbei handelt es sich um die „Microsoft Windows Based Terminal Server“. Diese Portnummer ist ebenfalls, wie Port 80 und Port 443, durch die IANA vergeben und standardisiert. [32] Genutzt wird dieser Port in der Regel für „Remote Desktop Services“ (RDS), was es ermöglicht eine Verbindung über Fernzugriff (Remote Desktop Connection) zu initialisieren. Häufig wird dies für virtuelle Maschinen oder andere Desktopanwendungen aus der Cloud verwendet. [33] Der letzte offene Port ist Port 7680 und dieser ist auch als einziger der vier nicht offiziell von der IANA vergeben. [32] Auf diesem Port läuft „pando-pub“, bei welchem es sich um eine Applikation für das Senden und Empfangen von Dateien handelt. Besonders häufig wird Pando verwendet, wenn es sich um Dateien handelt, welche eigentlich zu groß zum Verschicken sind. [34]

4.1.2 Ergebnisse der UDP-Scans

Die UDP-Scans der Pumpen ergaben lediglich einen offenen Port: Port 68. Abbildung 4 zeigt hierbei einen Ausschnitt der Ergebnisse.

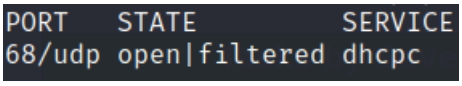


Abbildung 4: Ausschnitt der Ergebnisse des UDP-Scans der Pumpen

Entgegen der Resultate der bisherigen Ports ist dieser auf „open | filtered“ gesetzt und damit nicht sicher offen. Ein solches Ergebnis liegt im Regelfall vor, wenn Nmap nicht in der Lage war zu ermitteln, ob ein Port offen oder gefiltert ist. Dies könnte entweder ein Resultat daraus sein, dass der geöffnete Port keine Antwort gegeben hat oder dass der Packet-Filter die Antwort verloren hat. [22] Beim laufenden Service handelt es sich um den „Dynamic Host Configuration Protocol client“ (DHCPC). Dieser bildet das Gegenstück zum DHCP, welcher die Server-Seite darstellt. Hierdurch kann der Client Parameter wie IP-Adressen, Netzwerkmasken, Domain-Namen oder Gateways automatisch vom Server beziehen. [35]

Die UDP-Scans der Online-Suite ergaben keine geöffneten Ports. Hierbei resultierten alle Ports in dem Status „open | filtered“, was in diesem Fall dafür steht, dass keine Antwort gegeben wurde. Abbildung 5 zeigt einen Auschnitt dieser Ergebnisse.

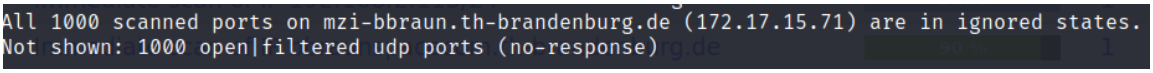


Abbildung 5: Ausschnitt der Ergebnisse des UDP-Scans der Online-Suite

Hierbei kam es, konträr zu Abbildung 4, trotz gleichem Status zu keinen Ergebnissen. Während beim UDP-Scan der Pumpen noch ein Dienst erkannt werden konnte, lieferte der UDP-Scan der Online-Suite keine Informationen.

4.1.3 Ergebnisse der OS-Detection-Scans

Die OS-Detection-Scans der Pumpen ergaben erneut die geöffneten TCP-Ports, als auch diverse Spezifikationen der Pumpen. Abbildung 6 zeigt einen Auschnitt dessen.

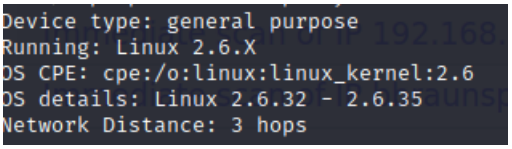


Abbildung 6: Ausschnitt der Ergebnisse der OS-Detection-Scans der Pumpen

Hierbei kam es zu verschiedenen Resultaten. Zum einen wurde ein Geräte-Typ (device type) festgestellt, welcher mit „general purpose“ (engl. für allgemeiner Zweck/Gebrauch) bezeichnet wurde. Unter Geräte-Typ unterscheidet Nmap zwischen z.B. Router, Drucker oder Firewall. Im Beispiel der Pumpen steht „general purpose“ für Betriebssysteme wie Windows oder Linux, da diese für fast alle Anwendungen genutzt werden können. [36] Im Weiteren grenzt Nmap dann das Betriebssystem noch weiter ein und benennt auch die Versionsnummer, sofern möglich. In diesem Fall handelt es sich um Linux 2.6.X. Gefolgt davon wird die „Common Platform Enumeration“ (CPE) angegeben. Diese bezeichnet eine einheitliche Namenskonvention und dient der Vergleichbarkeit von z.B. Sicherheitsschwachstellen. [37] Als Nächstes werden noch weitere Details zum Betriebssystem angegeben. Hierbei wird dieses Feld in der Regel dafür benutzt, um Freitext anzuzeigen, welcher ggf. menschenlesbar ist. [38] Im Fall der Infusionspumpen wird hier die Version des Betriebssystems weiter eingegrenzt. Darauf folgend kann Nmap außerdem auch noch die Zeit, welche das System schon erreichbar ist, angeben. Im Fall der Pumpen fehlt diese. Nmap lässt dies aus verschieden Gründen teilweise aus. Dazu gehöhren Gründe wie eine fehlende Antwort seitens des Ziels, fehlende Zeitstempel in den Packeten, ein nicht Erkennen der Zeitstempel oder eine suspekte Angabe. Die letzte Erkenntnis des Scans ist die Netzwerkdistanz. Diese gibt die Anzahl an Routern an, welche zwischen dem scannenden System und dem Ziel liegen. Im Falle der Infusionspumpen ist dies drei. Nmap ist zudem auch in der Lage noch zwei weitere Parameter zu bestimmen: „TCP Sequence Prediction“ sowie „IP ID sequence generation“. [38] Diese kommen jedoch nicht in den Ergebnissen dieser Arbeit vor und wurden nur der Vollständigkeit erwähnt.

Die OS-Detection-Scans der Online-Suite ergaben ähnlich wie die Scans der Infusionspumpen neben den TCP-Ports diverse Spezifikationen des Systems. Dies ist in Abbildung 7 dargestellt.

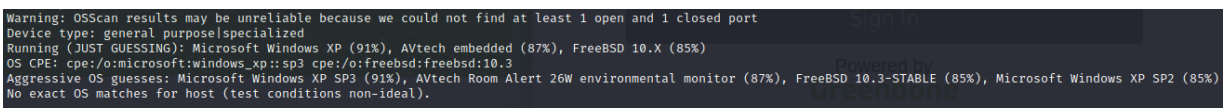


Abbildung 7: Ausschnitt der Ergebnisse der OS-Detection-Scans der Online-Suite

Wie bereits in 4.1.1 Ergebnisse der TCP-Scans aufgezeigt, hat Nmap lediglich entweder geöffnete Ports erkannt oder keine Antwort erhalten. Hierbei wurde kein einziger geschlossener Port gefunden. Der OS-Detection-Scan warnt aus diesem Grund vor eventueller Ungenauigkeit. Bei dem Geräte-Typ der Online-Suite handelt es sich um „general purpose | specialized“. Hierbei fällt die Online-Suite sowohl in die Kategorie „general purpose“ als auch „specialized“. Letzteres stellt eine ebenfalls allgemeine Obergruppe dar. Zu dieser gehören alle Systeme, welche nicht genau zugeordnet werden können, weil diese zu speziell sind. Beispiele dafür sind z.B. Uhren, Oszilloskope oder andere Sensoren. [39] Als Betriebssystem-Typ konnte Nmap, aufgrund der Ungenauigkeit und der fehlenden Informationen, nur Schätzungen abgeben. Nmap sieht hierbei vier verschiedene Betriebssysteme als wahrscheinlich an: Windows XP (91%), Avtech embedded (87%) und FreeBSD 10.X (85%). Diese Schätzungen sind weiter unter „Aggressive OS guesses“ ausgeführt und außerdem um ein viertes Betriebssystem ergänzt: „Microsoft Windows XP SP2 (85%)“. Dieses Feld ist eigentlich für „OS Details“ vorgesehen, jedoch tauscht Nmap diese Felder aus, falls es mehrere sehr wahrscheinliche Treffer gibt und damit keine eindeutige Antwort gegeben werden kann. [38]

4.1.4 Ergebnisse der Service-Detection-Scans

Die letzten Iterationen der Portscans sind die Service-Detection-Scans. Diese ergaben nur teilweise Resultate. Abbildung 8 stellt einen Ausschnitt dieser dar.

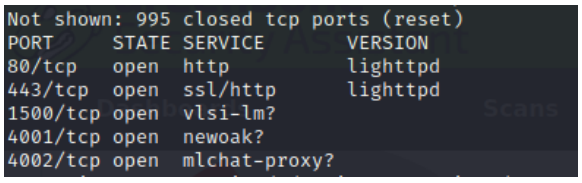


Abbildung 8: Ausschnitt der Ergebnisse der SV-Detection-Scans der Pumpen

Hierbei ist zu erkennen, dass sowohl der TCP-Port 80 als auch TCP-Port 443 „lighttpd“ benutzen. Bei „lighttpd“ handelt es sich um einen open-source Webserver ähnlich wie Apache, welcher besonders für Umgebungen optimiert ist, bei welchem die Geschwindigkeit eine große Wichtigkeit erhält. [40] Die restlichen drei Ports ergaben keine Treffer in der Erkennung der Software. Außerdem ergaben sich hierbei zum ersten Mal nicht erkannte Daten. Wie bereits erwähnt, werden diese von Nmap als „Fingerabdruck“ ausgegeben und können dann so bei Nmap eingereicht werden. Die Ergebnisse der Fingerabdrücke befinden sich im Anhang 1.4 unter Abbildung 26.

Die Ergebnisse der Service-Detection-Scans der Online-Suite ergaben keine Treffer. Es wurden erneut lediglich die generellen Dienste gefunden, zu sehen in Abbildung 9.

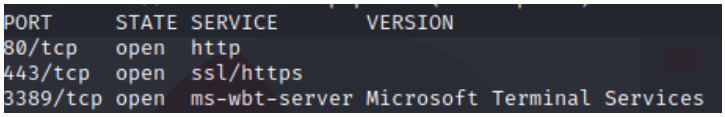


Abbildung 9: Ausschnitt der Ergebnisse der SV-Detection-Scans der Online-Suite

Des Weiteren ergaben sich zwei weitere „Fingerabdrücke“. Diese befinden sich ebenfalls im Anhang 1.4 unter Abbildung 27 sowie Abbildung 28.

4.2 Ergebnisse der Schwachstellenanalyse mittels OpenVAS / GVM

Eingeleitet wurde der erste Schwachstellenscan lokal vor Ort. Der zweite Scan wurde aufgrund von technischen Schwierigkeiten remote durchgeführt. Beide Scans wurde ebenfalls auf einer virtuellen Kali-Linux Maschine durchgeführt. Außerdem filterten beide Scans, wie bereits in *3.3 Schwachstellenanalyse* ausgeführt, hierbei standardmäßig mehrere Ergebnisse bereits zuvor heraus.

4.2.1 Ergebnisse des ersten Schwachstellenscans

Nach dem Filterungsprozess des Scans ergaben sich insgesamt noch sechs verbleibende Resultate. Hierbei wurden 63 Ergebnisse aussortiert. In der Übersicht ergaben sich zwei Schwachstellen mit einem hohen Bedrohungsgrad, drei mit einem mittleren und eine Schwachstelle mit einem niedrigen Bedrohungsgrad. Jedoch sind diese teilweise Duplikate. Abbildung 10 zeigt hierbei einen Auschnitt der GVM-Übersicht. In diesem sind die Schwachstellen nach ihrem QoD-Wert sortiert und der Bedrohungsgrad ist farblich verdeutlicht.

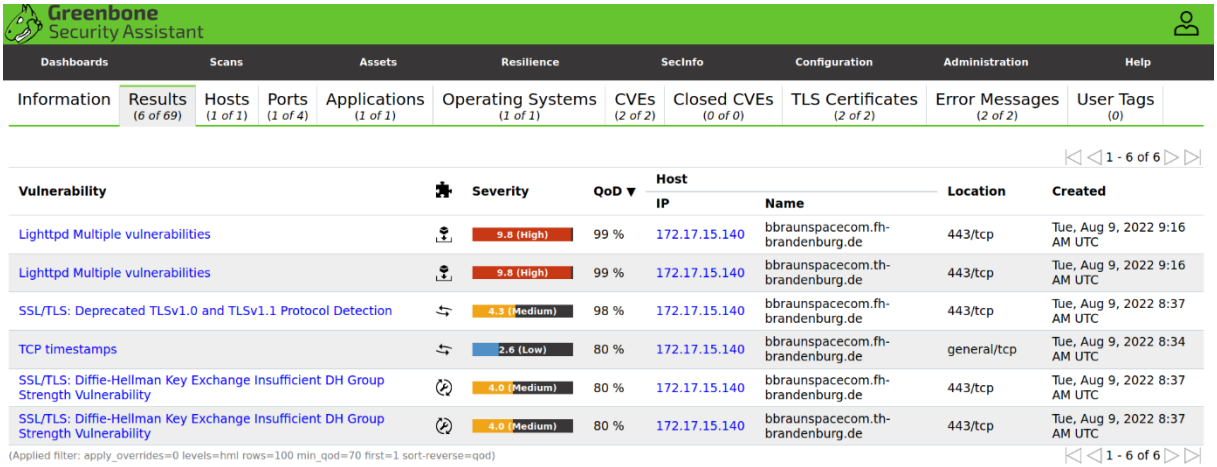


Abbildung 10: Ausschnitt der ersten Schwachstellenanalyse der Infusionspumpen

Zunächst ergibt sich hierbei eine Schwachstelle im Port 443. Mit einem CVSS-Wert von 9.8 ist diese die Schwachstelle mit dem größten Gefahrengrad. GVM benennt diese als „Lighttpd Multiple vulnerabilities“. Mit einem QoD-Wert von 99% wurde diese Schwachstelle durch aktives Prüfen (Ausführen von externem Code, SQL-Injektion etc. [27]) verifiziert und zeigt damit eindeutig die Existenz dieser Schwachstelle. Ein falsch-positives Ergebnis ist damit ausgeschlossen. Als Folge dieses Exploits besteht hierbei die Möglichkeit für einen Angreifer willkürlich SQL-Kommandos auszuführen oder verschiedene Dateien zu lesen. Der „Lighttpd“-Dienst wurde bereits in Abbildung 8 aufgezeigt und läuft sowohl auf Port 80 als auch 443. GVM führt außerdem an, dass es sich hierbei um einen Exploit, der lediglich in alten „Lighttpd“-Versionen vorhanden ist, handelt. Eine Aktualisierung des Dienstes auf die Version 1.4.35 oder spätere würde das Problem beheben.

Die nächste Schwachstelle ergibt sich mit einem CVSS-Wert von 4.3 und befindet sich ebenfalls auf dem Port 443. Bezeichnet wird diese als „SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection“. Mit einem QoD-Wert von 98% ist die Verifizierung ähnlich wie bei der Lighttpd-Schwachstelle zuvor durch aktives Prüfen bestätigt worden. [27] Hierbei setzen die Pumpen auf ein veraltetes und nicht weiter unterstütztes TLS (Transport Layer Security) Protokoll. TLS ist weit verbreitet und wird im Regelfall für kryptographische Kommunikation im Internet verwendet und dient damit der sicheren Verschlüsselung von Daten. [41] Veraltete TLS Versionen sind anfällig gegenüber man-in-the-middle-Angriffe (unbemerkt in eine Kommunikation von zwei oder mehr Partner eindringen [42]) und bergen so ein hohes Risiko gegenüber der Vertraulichkeit der Daten. Außerdem ist das Protokoll soweit veraltet, dass es keine weiteren Sicherheitsupdates erhält. Hier wäre erneut die beste Lösung

das Deaktivieren von allen TLSv1.0 sowie TSLv1.1 Protokollen und im gleichen Zug das Austauschen dieser für TLS Versionen 1.2 oder spätere.

Als Nächstes ergibt sich eine Schwachstelle in den TCP-Zeitstempel mit einem CVSS-Wert von 2.6. Diesmal ist dieses Problem nicht Port-spezifisch, sondern generell bei allen verfügbaren TCP-Ports vorhanden. Mit einem QoD-Wert von 80% wurde dieser Überprüfung mittels Systemversionen verifiziert. [27] Durch den Scan wurde ermittelt, dass die Pumpen sowohl RFC1323 als auch RFC7323 implementieren. „Request for Comments“ (RFCs) sind eine Reihe von Beiträgen, welche grundlegende Aspekte von Computernetzwerken beschreiben. Hierbei werden z.B. Protokolle vorgestellt und dann für eine Standardisierung vorgeschlagen. Diese erhalten dann einen von sechs verschiedene Status. [43] Bei RFC1323 und RFC7323 handelt es sich um vorgeschlagene Standards („proposed standard“) für eine TCP-Erweiterung für eine verbesserte Performance bei großem Verzögerungs-Bandbreiten-Produkt. [44] [45] Hierbei ist RFC1323 die Vorgängerversion von RFC7323 und wurde durch letzteren obsolet. Ein Nebeneffekt dieser beiden Erweiterungen ist, dass dadurch die Gesamtlaufzeit des Systems ermittelt werden kann. Hierfür schlägt GVM vor, die TCP-Zeitstempel zu deaktivieren. Bei einem Windows Server 2008 oder späteren Versionen ist eine komplette Deaktivierung nicht möglich, jedoch ist bereits durch den Portscan bekannt, dass es sich bei den Pumpen um ein Linuxsystem handelt, in welchem eine Deaktivierung keine Probleme erzeugt.

Bei den letzten beiden Schwachstellen handelt es sich um nur eine Schwachstelle und ein Duplikat. Mit einem CVSS-Wert von 4.0 beinhaltet dies einen größeren Gefahrengrad als die Schwachstelle davor. Erneut wurde auch diese Schwachstelle mit einem QoD-Wert von 80% befunden. Ebenfalls handelt es sich hierbei wieder um ein SSL/TLS-Problem, welches auf dem Port 443 eine Sicherheitsschwachstelle erzeugt. Der Scan ergab, dass der Dienst das „Diffie-Hellman“-Verfahren nutzt, um kryptographische Schlüssel auszutauschen. Die „Diffie-Hellman“-Methode war eine der ersten Möglichkeiten gewesen, zwei Kommunikationspartner auf einen geheimen Schlüssel einigen zu lassen, ohne dass dieser zuvor über einen anderen Weg transportiert werden musste. Hierbei benötigen die beiden Partner kein vorheriges Wissen über den jeweils anderen und es wird auch kein sicherer Kanal benötigt. Auch heute noch wird diese Methode für viele verschiede Dienste im Internet verwendet. [46] Auch wenn bereits seit einigen Jahren der Grad der Sicherheit dieses Verfahren kritisiert wird und es abgeraten wird, die „Diffie-Hellman“-Methode als Basis für sichere Systeme zu nutzen. [47] Zusätzlich ergab der Scan eine ungenügende Länge des Schlüssels. Die Detektion ergab eine Schlüsselgröße von

1024 Bits, während GVM mindestens 2048 Bits empfiehlt. Zum Lösen des Problems gibt GVM zwei verschieden Optionen an: 1. Die „Diffie-Hellman“-Methode austauschen für die „Elliptic-Curve Diffie-Hellman“-Methode. Hierbei handelt es sich um eine verbesserte Version, welche bei kürzeren Schlüssellängen einen gleichen Grad an Sicherheit bietet. [48] [49]. 2. Die Schlüssellänge auf 2048 Bits oder mehr erhöhen.

4.2.2 Ergebnisse des zweiten Schwachstellenscans

Wie bereits erwähnt wurde noch ein zweiter Scan nach dem Sicherheitsupdate der Infusionspumpen durchgeführt. Dieser wurde remote durchgeführt und resultierte in fünf gefundenen Sicherheitsschwachstellen. Hierbei ergaben sich wie bereits im Scan davor auch zwei Duplikate. Abbildung 11 zeigt hierbei einen Auschnitt der GVM-Übersicht. In diesem sind die Schwachstellen erneut nach ihrem QoD-Wert sortiert.

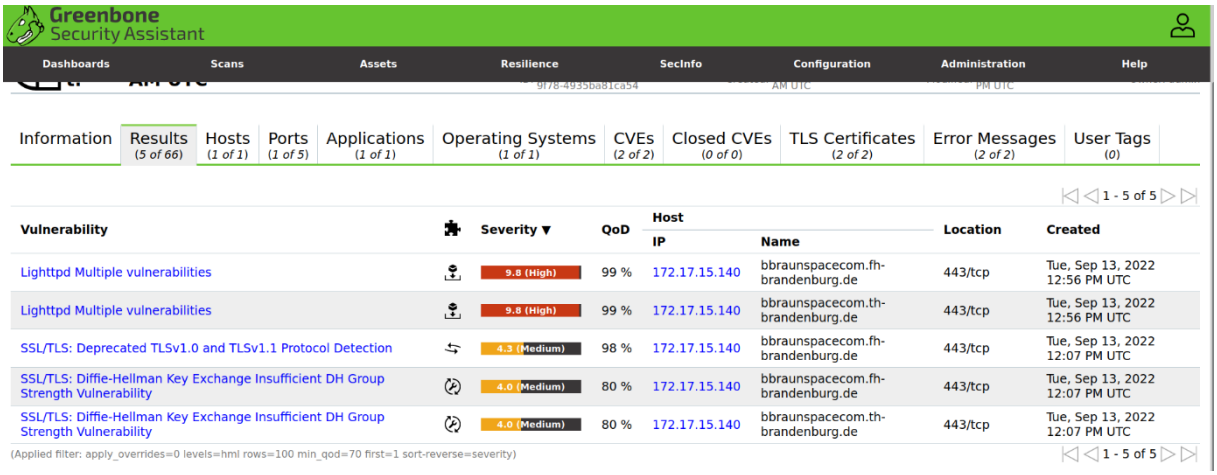


Abbildung 11: Ausschnitt der zweiten Schwachstellenanalyse der Infusionspumpen

Zunächst zeigt sich hier erneut die Schwachstelle „Lighttpd Multiple Vulnerabilities“. Hierbei ist zu erkennen, dass diese immer noch über einen hohen QoD-Wert verfügt. Wie auch schon beim ersten Scan wurde diese Schwachstelle durch aktives Prüfen wie ausführen von externem Code verifiziert und zeigt auch hier wieder die eindeutige Existenz dieser Schwachstelle. [27]

Als Nächstes ergibt der Scan erneut eine bereits zuvor bestehende Schwachstelle. Auch die veralteten SSL/TLS-Protokolle wurden nicht aktualisiert oder deaktiviert. Auch der QoD-Wert von 98% ist identisch zum Wert des ersten Scans.

Als Letztes ergab sich erneut ein Duplikat, welches auch bereits im ersten Scan vorhanden war. Auch hier sind sowohl CVSS- als auch QoD-Wert derselbe, weswegen es sich hierbei auch um dieselbe Schwachstelle handelt.

Die einzige Schwachstelle, welche im zweiten Scan nicht vorhanden ist, ist die TCP-Zeitstempel-Schwachstelle. Das Fehlen dieser lässt daraus schließen, dass diese Schwachstelle im Zuge des Sicherheitsupdates ausgebessert wurde.

4.3 Ergebnisse des Netzwerkverkehr Mitschnitts

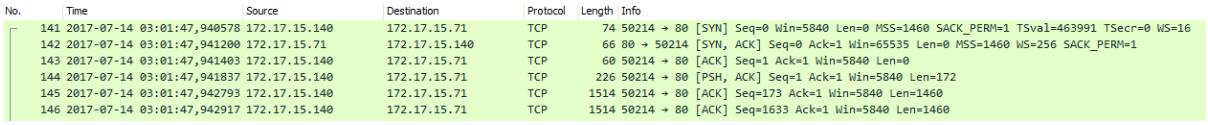
Wie bereits in *3.4 Netzwerkverkehr aufzeichnen* angeführt wurde, ergeben sich mehrere voneinander abgetrennte Wireshark-Dateien, welche zum Auswerten genutzt werden. Begonnen wird hierbei zunächst mit der generellen Struktur und dem Aufbau hinter dem Netzwerkverkehr der Pumpen. Eine genaue Einteilung der Ergebnisse in die einzelnen Versuche ist nicht nötig, da die Struktur und der Aufbau der Kommunikation in jedem Falle gleich sind.

4.3.1 Struktur und Aufbau des Netzwerkverkehrs

Zunächst einmal kommuniziert die Pumpen auch im ausgeschalteten Modus (Standby-Modus) weiterhin im Netzwerk. Dies wird jedoch in *4.3.2 Ergebnisse der Mitschnitt* weiter ausgeführt. Zunächst beginnen dann die Infusionspumpen nach der Online-Suite zu suchen und versuchen dann im Folgenden auch eine Verbindung zu etablieren. Eine Verbindung ist deswegen essenziell, weil die Kommunikation zwischen den Pumpen und der Online-Suite ausschließlich über TCP verläuft, welches verbindungsorientiert funktioniert. [50]

TCP verwendet einen „Drei-Wege-Handschlag“ (Three-Way-Handshake) zum initieren einer Verbindung. Diese geht in diesem Fall von den Pumpen aus. Diese senden zuerst ein „[SYN]“ (eine Anfrage zum Synchronisieren bzw. zum Verbindungsaufbau). Als Antwort darauf entgegnet der Server, in diesem Fall die Online-Suite, mit „[SYN, ACK]“. Hierbei bestätigt die Online-Suite, dass sie die Anfrage zum Verbindungsaufbau erhalten hat und auch bereit dafür ist. Zum Schluss bestätigt auch der Client, also die Pumpen, dass diese die zuvor gesendeten „[SYN, ACK]“-Nachricht erhalten haben. [51] Danach entgegnet die Online-Suite noch ein weiteres Mal mit „[PSH, ACK]“. Dies ist eher untypisch und kein Teil des klassischen TCP-Verbindungs-Handschlags. Diese Antwort steht hierbei dafür, dass die Online-Suite einen „Push“ der Daten anfragt. Hierbei kann die Online-Suite kleinere Verzögerungen umgehen, da

die Pumpen nicht warten müssen, bis der Buffer voll ist. [52] Abbildung 12 zeigt diesen Verbindungsaufbau dargestellt in Wireshark. Die zuvor angesprochenen Initierungs-Nachrichten befinden in der rechten Spalten.



No.	Time	Source	Destination	Protocol	Length	Info
141	2017-07-14 03:01:47,940578	172.17.15.140	172.17.15.71	TCP	74	50214 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=463991 TSecr=0 WS=16
142	2017-07-14 03:01:47,941200	172.17.15.71	172.17.15.140	TCP	66	80 → 50214 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
143	2017-07-14 03:01:47,941403	172.17.15.140	172.17.15.71	TCP	60	50214 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
144	2017-07-14 03:01:47,941837	172.17.15.140	172.17.15.71	TCP	226	50214 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=172
145	2017-07-14 03:01:47,942793	172.17.15.140	172.17.15.71	TCP	1514	50214 → 80 [ACK] Seq=173 Ack=1 Win=5840 Len=1460
146	2017-07-14 03:01:47,942917	172.17.15.140	172.17.15.71	TCP	1514	50214 → 80 [ACK] Seq=1633 Ack=1 Win=5840 Len=1460

Abbildung 12: Ausschnitt des Verbindungsaufbaus der TCP-Verbindung

Wireshark ermöglicht eine gruppierte Übersicht über bestimmte Paket-Ströme. Durch das Folgen des TCP-Stroms erhält der Nutzer eine gefilterte und geordnete Übersicht über den gesamten TCP-Nachrichtenaustausch beider Kommunikationspartner. In diesem Fall kann so der Nachrichtenverkehr zwischen den Infusionspumpen und der Online-Suite verfolgt werden.

Zunächst ergibt sich, dass die beiden Parteien XML benutzen um zu kommunizieren. Dies zeigt sich zum einen am XML-Format, welches mittels Start- und End-Tag die Werte markiert. Zum anderen ergibt sich dies aus dem ersten Datenpaket, Paket Nr. 144. Hierbei wird in unverschlüsseltem Hexadezimal die Header-Zeile übertragen. In der Strom-Folgen-Ansicht wird dies auch bereits direkt in menschenlesbaren Text übersetzt.

Aufbauend auf das XML-Format ergibt sich außerdem, dass das „Simple Object Access Protocol“ (SOAP) genutzt wird. [53] Hierbei handelt es sich um ein Protokoll, welches auf Basis von XML Nachrichten kodiert. Hierbei besteht eine SOAP Nachricht immer aus einem „Envelope“-Element (Umschlag-Element), welches noch einen optionalen Header besitzen kann und einen Body besitzen muss. Zudem kann auch noch ein „Fault“-Element (Störungs-Element) mit angegeben werden, welches ggf. Fehler umfasst. [54] Abbildung 13 zeigt hierbei einen Ausschnitt des ersten Netzwerkverkehrmitschnitts der Infusionspumpen. Das „Envelope“-Element beginnt hierbei in der zweiten Zeile mit der Definition des Namensraums (Namespace) und schließt am Ende in der letzten Zeile die SOAP-Nachricht wieder. Ein Header wurde angegeben, jedoch ist dieser ohne Inhalt. Ein „Fault“-Element fehlt gänzlich.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:pcs2="http://www.bbraun.com/HC/RD/AIS/PCS2.5.0">
<soapenv:Header/>
<soapenv:Body>
<pcs2:PCSData crc="33849" version="2.5.0" timestamp="2230872" mac="00-12-21-02-32-4C">
<PointInTime crc="60533" timestamp="2230736" topologyError="NONE">
</PointInTime>
</pcs2:PCSData>
</soapenv:Body>
</soapenv:Envelope>
```

Abbildung 13: Ausschnitt aus einem SOAP-Envelope

Des Weiteren findet sich in keiner der ausgewerteten Wireshark-Dateien ein Bezug auf TLS oder SSL, welches zwischen den Infusionspumpen und der Online-Suite ausgetauscht oder initialisiert wird. Wie in *4.2 Ergebnisse der Schwachstellenanalyse mittels OpenVAS / GVM* bereits festgestellt, nutzen die Pumpen TLS. Auch bei einer veralteten Version von TLS müssten die Daten zuvor verschlüsselt werden, da TLS sich als Sicherheitsprotokoll auf der obersten Schicht des TCP/IP-Referenzmodells, der Anwendungsebene, befindet und so die Daten auch für alle darunter liegende Ebene bereits verschlüsselt. [55] Hierbei müssten demnach die Daten, welche über TCP versendet werden, bereits verschlüsselt und nicht mehr im Klartext lesbar sein.

4.3.2 Ergebnisse der Mitschnitte (vor dem Sicherheitsupdate)

Wie bereits in *4.3.1 Struktur und Aufbau des Netzwerkverkehrs* aufgezeigt, werden alle Daten der Infusionspumpen im Klartext übermittelt. Dazu gehören auch hochsensitive Patientendaten.

Zunächst beginnen die Pumpen mit einer Nachricht an die Online-Suite, dass diese einsatzbereit sind. Dies geschieht durch mehrere Status, die an die Suite übersendet werden. Diese sind in Abbildung 14 dargestellt.

```
<value crc="61925" name="current_device_state">
<arrayValue crc="55707" receptionTime="1214204006">
<enumValue crc="55147" receptionTime="1214204005" value="BOLUS_IS_READY"/>
<enumValue crc="25231" receptionTime="1214204005" value="DEVICE_IS_CONNECTED_TO_MAINS"/>
<enumValue crc="60540" receptionTime="1214204005" value="DEVICE_IS_ON"/>
<enumValue crc="31404" receptionTime="1214204005" value="DRIVE_CLOSED"/>
<enumValue crc="14175" receptionTime="1214204005" value="INFUSION_HAS_BEGUN"/>
<enumValue crc="21523" receptionTime="1214204005" value="KVO_IS_AVAILABLE"/>
<enumValue crc="27099" receptionTime="1214204005" value="PRIMARY_INFUSION_IS_ACTIVE"/>
<enumValue crc="62577" receptionTime="1214204006" value="PUMP_IS_RUNNING"/>
</arrayValue>
```

Abbildung 14: Ausschnitt der Statusmeldung der einsatzbereiten Infusionspumpe

Hierbei ergeben sich verschiedene Meldungen. Zum einen wird hier als erstes übermittelt, dass ein „Bolus“ bereit ist. Bolus steht in der Medizin für eine Dosis von Medikamenten, welche einmalig oder über einen Zeitraum vergeben wird. In der Regel geschieht dies bei einer Infusion oder einer Injektion direkt in die Blutbahn. [56] Weitere wichtige Mitteilungen sind außerdem noch: das Gerät ist verbunden zur Online-Suite, die Infusion hat begonnen und die Infusionspumpe läuft. Darüber hinaus wird auch noch berichtet, welche der beiden Pumpen in Betrieb ist.

Im Anschluss werden die fallspezifischen Daten übermittelt. Hierzu gehören z.B. Durchflussrate, die verbleibende Länge der Infusion oder auch das noch verbleibende Volumen. Ein Ausschnitt dessen ist in Abbildung 15 dargestellt.

```
<value crc="25375" name="current_infusion_flow_rate">
<numberValue crc="700" receptionTime="1214203999" value="500" digits="2" unit="1"/>
</value>
<value crc="39341" name="current_infusion_infused_volume">
<numberValue crc="12528" receptionTime="1214203999" value="0" digits="2" unit="2"/>
</value>
<value crc="17016" name="current_infusion_remaining_time">
<numberValue crc="63679" receptionTime="1214203999" value="132" digits="0" unit="3"/>
</value>
<value crc="6008" name="current_infusion_remaining_volume">
<numberValue crc="33921" receptionTime="1214203999" value="1100" digits="2" unit="2"/>
</value>
```

Abbildung 15: Ausschnitt der Einstellungen der Infusionspumpen

Auffällig ist hierbei, dass die Parameter, welche während den Versuchen eingegeben wurden zwar übernommen und auch kommuniziert, jedoch in eine andere Einheit umgerechnet wurden. Während die Zeit, welche zuvor als zwei Stunden und zwölf Minuten angegeben wurde, lediglich in 132 Minuten umgerechnet wurde, ergaben sich sowohl bei der Durchflussrate, als auch dem verbleibenden Volumen eine Multiplikation mit 100. Der Grund hierfür ist unklar, jedoch könnte dies durch das einfachere Speichern von Zahlen mit Nachkommastellen bedingt sein. [57]

Als Nächstes werden ebenfalls Informationen über die verabreichten Medikamente versendet. Dazu gehört auch der Name des verabreichten Medikamentes, sowie die Priorität für den Alarm oder auch zu welcher Kategorie das Medikament gehört. Abbildung 16 zeigt hierbei einen Ausschnitt der übermittelten Informationen.

```
<value crc="27168" name="current_drug_concentration_short_name">
<stringValue crc="34171" receptionTime="39059" value=""/>
</value>
<value crc="60549" name="current_drug_long_name">
<stringValue crc="50664" receptionTime="1214030319" value=""/>
</value>
</valueGroup>
<valueGroup crc="36072" name="DRUG_INFO">
<value crc="58445" name="current_careunit_index">
<numberValue crc="8814" receptionTime="3697586" value="1" digits="0" unit="0"/>
</value>
<value crc="24873" name="current_careunit_name">
<stringValue crc="12214" receptionTime="3697586" value="Biosignallabor"/>
</value>
<value crc="63511" name="current_drug_category_name">
<stringValue crc="38926" receptionTime="1214030319" value="Alle Medikamente"/>
</value>
```

Abbildung 16: Ausschnitt der Medikmamenteninformationen

Im Anschluss daran werden die Patientendaten übermittelt. Begonnen wird hierbei mit dem Namen des Patientenprofils. In den praktischen Versuchen dieser Arbeit wurde ein generischer Name für ein Profil und damit kein Name einer spezifischen Person verwendet. Des Weiteren werden die anthropometrischen Daten des Patienten übermittelt. Dazu gehören vor allem das Alter, die Körpergröße, das Gewicht sowie das Geschlecht. Auch werden hier noch unter anderem eine Patienten-ID sowie eine Patienten-Armband-ID mit übersendet. Ein spezifischer Patientenname konnte jedoch nicht in dem Netzwerkverkehr gefunden werden. Abbildung 17 zeigt einen Ausschnitt der übermittelten Patientendaten.

```
<value crc="41090" name="current_patient_age">
<numberValue crc="31688" receptionTime="46031" value="0" digits="0" unit="5"/>
</value>
<value crc="13762" name="current_patient_bodysurface">
<numberValue crc="19445" receptionTime="46031" value="21" digits="0" unit="0"/>
</value>
<value crc="16949" name="current_patient_height">
<numberValue crc="28195" receptionTime="46031" value="0" digits="3" unit="19"/>
</value>
<value crc="62264" name="current_patient_id">
<stringValue crc="18420" receptionTime="1214030317" value=""/>
</value>
<value crc="50877" name="current_patient_sex">
<enumValue crc="31269" receptionTime="46030" value="UNDEF"/>
</value>
<value crc="37721" name="current_patient_weight">
<numberValue crc="14123" receptionTime="46030" value="0" digits="3" unit="22"/>
```

Abbildung 17: Ausschnitt der Patientendaten

Außerdem speichern und senden die Infusionspumpen noch weitere Informationen zum System selber. Zum einen gehören dazu Informationen zum Eigentümer der Pumpen, die Zeit, in welcher die Pumpen bereits in Betrieb sind oder auch welche Medikamentendatenbank benutzt wird. Zum anderen werden hier ebenfalls die Grenzfälle der verschiedenen Einstellungen kommuniziert. Dazu gehören unter anderem die minimale, aber auch maximale Durchflußrate.

4.3.3 Ergbnisse der Mitschnitte (nach dem Sicherheitsupdate)

Wie auch in *4.2.2 Ergebnisse des zweiten Schwachstellenscans* bereits kaum Veränderungen festgestellt werden konnten, sind auch hier wieder keine Änderungen zu finden. Wie im Schwachstellenscan zuvor festgestellt wurde, benutzen die Pumpen eine veraltete Version von TLS. Dennoch fehlt beim Verbindungsaufbau weiterhin der TLS-Handschlag und damit die Einbindung des Protokolls. Als Resultat dessen wird erneut der gesamte Netzwerkverkehr im Klartext übermittelt.

Die Struktur bzw. der Aufbau der Kommunikation hat sich hierbei nicht verändert. Die Kommunikation läuft immer noch über TCP und nutzt dabei XML sowie SOAP. Auch werden alle sensitiven Daten, welche bereits in *4.3.2 Ergebnisse der Mitschnitte (vor dem Sicherheitsupdate)* vertieft wurden, weiterhin zwischen den Pumpen und der Online-Suite kommuniziert.

5. Bewertung und Diskussion der Ergebnisse

Die zuvor besprochenen Ergebnisse werden im nächsten Schritt ausgewertet und anhand ihres Schweregrades bewertet.

5.1 Bewertung der Portscans

In den Portscans finden sich die wenigsten direkten Sicherheitsschwachstellen. Hierbei waren, soweit dies extern beurteilbar ist, lediglich essenzielle Ports wie Port 80 oder Port 443 offen. Der größte Teil der Ports war geschlossen, das ist besonders wichtig, wenn miteinbezogen wird, dass weniger geöffnete Ports eine größere Sicherheit bieten. [58] Eine genaue Beurteilung, welche Ports für die interne Softwarearchitektur wichtig sind, ist aus externer Sicht nicht realisierbar. Dennoch scheint die Freigabe der Ports auf ein Minimum reduziert zu sein. Die eigentlichen Sicherheitsrisiken ergeben sich erst bei den Diensten bzw. der Software, welche auf den Ports läuft. Diese werden jedoch erst in *5.2 Bewertung der Schwachstellenanalyse* bewertet. Insgesamt scheinen die Ports nur ein geringes bis kein Sicherheitsrisiko zu bergen.

5.2 Bewertung der Schwachstellenanalyse

Im Gegensatz zu den Portscans ergeben sich bei der Schwachstellenanalyse deutlich mehr Probleme und Sicherheitsrisiken. Hierbei ergeben sich diverse Sicherheitsschwachstellen, welche durch reines Aktualisieren der Software umgangen und verbessert werden könnten.

Beginnend mit den Schwachstellen in der Webserver-Applikation „Lighttpd“, fand GVM hierbei, dass eine Aktualisierung auf Version 1.4.35 bereits ausreichen würde, um einen verbesserten Schutz zu garantieren. Diese Version vom Webserver ist dabei vor fast neun Jahren veröffentlicht worden und wurde seit dem um eine Vielzahl von neuen Versionen ergänzt. [59] Eine ähnliche Problematik ergibt sich auch bei TLS. Wie bereits in *4.2.1 Ergebnisse des ersten Schwachstellenscans* erörtert, haben die Infusionspumpen eine veraltete Version des Protokolls implementiert. Auch hier findet sich bereits seit 2008 eine verbesserte

Version. [60] Ähnliche Sicherheitsrisiken, welche auf nicht aktualisierter Software basieren, häufen sich in der Softwarearchitektur der Pumpen und machen damit einen Großteil der Sicherheitsschwachstellen aus.

Außerdem findet sich in der Schwachstellenanalyse die einzig behobene Schwachstelle. Durch das Ausbessern der TCP-Zeitstempel, ist es nun nicht mehr möglich als Nebeneffekt die Gesamtlaufzeit des Systems zu ermitteln. Dies ist jedoch im Vergleich nur ein sehr kleines Problem gewesen und ist damit nicht Teil der eigentlichen Probleme.

Hierbei stellen vor allem die zuvor angesprochenen Beispiele ein großes Sicherheits- und Datenschutzrisiko dar. Das Ausnutzen der Schwachstellen dieser veralteten Software kann zum einen die Integrität, als auch die Vertraulichkeit des Systems kompromittieren. Die benutzte Software stellt damit auch nach dem Sicherheitsupdate noch ein sehr großes Sicherheitsrisiko dar und wurde nicht maßgeblich verbessert.

5.3 Bewertung des Netzwerkverkehrmitschnitts

Der Netzwerkverkehrmitschnitt schließt direkt an die Schwachstellenanalyse an und hat dabei ähnliche Probleme.

Besonders gravierend ist hierbei das Senden aller Daten in Klartext. Hierbei ist auffällig, dass laut dem Schwachstellenscan von GVM, eine Version von TLS implementiert wurde, diese jedoch nicht funktioniert. Obwohl es sich bei der Version um eine bereits sehr alte Version von TLS handelt, sollte diese dennoch die Daten verschlüsseln. Ein Senden von Klartext deutet darauf hin, dass die Implementierung fehlerhaft ist. Hierbei unterteilen sich die gesendeten Daten in zwei grobe Kategorien.

Zum einen werden Informationen zu den Infusionspumpen in Klartext gesendet. Eine dritte Person, die diese Daten mitliest, erhält damit Auskunft über verschiedene Status der Pumpen. In Zusammenarbeit mit der „Lighttpd“-Schwachstelle, vor welcher GVM bereits zuvor gewarnt hatte, dass es möglich sei, fremden SQL-Code auszuführen, könnte es zu unbefugtem Zugriff auf die Pumpen kommen. Als Folge dessen kann es zu Schäden für den Patienten kommen.

Zum anderen werden außerdem auch patientenspezifische Daten kommuniziert. Hierzu gehören fast alle patientenbeschreibenen Daten, mit Ausnahme des Namens, welcher nicht in den Versuchen gefunden werden konnte. Jedoch sendeten die Pumpen und die Online-Suite

den Namen des Patientenprofils, welcher in den Versuchen dieser Arbeit lediglich ein generischer Name für ein Patientenprofil (z.B. „Profil 1“), und damit kein richtiger Name eines Patienten war. Dennoch ist es denkbar, dass es hierbei zu Verwechslungen kommen kann, weswegen es wichtig ist, die Nutzer solcher Geräte ordentlich und angemessen zu schulen.

6. Abschluss und Fazit

Wie der Stand der Literatur bereits erahnen lassen konnte, sind Medizingeräte, im speziellen Fall dieser Arbeit die B. Braun Infusionspumpen, noch nicht sicher genug und beinhalten noch immer Sicherheitsrisiken. Die Ergebnisse dieser Arbeit konnten hierbei teilweise auch aufzeigen, was die Gründe für solche Sicherheitslücken sind.

Besonders häufig ist veraltete Software hierbei das Problem. Dies wurde größtenteils in *4.2.1 Ergebnisse des ersten Schwachstellenscans* deutlich. Im Zuge dessen zeigte sich dann der eigentliche Schweregrad. Im Falle von TLS ist seit über 14 Jahren eine erneuerte und sichere Version veröffentlicht, dennoch wurde TLS noch nicht aktualisiert und stellt damit ein großes Sicherheitsproblem dar, welches sehr einfach ausgebessert werden könnte. Eine einfache Aktualisierung für die Pumpen würde hierbei bereits ausreichen.

Ein komplexeres Problem ergibt sich bei der Implementierung von TLS. Hierbei ist diese offensichtlich fehlerhaft und ermöglicht dadurch das Lesen aller gesendeten Daten. Die gesamte Kommunikation zwischen den Infusionspumpen und der Online-Suite war ohne Entschlüsselung direkt im Klartext lesbar. Warum diese Implementierung fehlerhaft war, ist jedoch unklar, dennoch sollte es von hoher Priorität sein, dass hierfür eine Fehlerbehebung veröffentlicht wird.

Abschließend ergeben sich diverse Probleme mit den, in dieser Arbeit, untersuchten Medizingeräten. Mit nur wenigen Ausnahmen sind vor allem die Sicherheitsrisiken mit den größten Schweregraden durch veraltete oder mittlerweile als unsicher angesehene Software bedingt. Die Kommunikation zwischen den Infusionspumpen und der Online-Suite ist im hohen Maße unsicher und kann vor allem für den Patienten sogar gefährlich werden. Das Senden aller Daten im Klartext, trotz TLS, stellt einen riesigen Fehler dar und sollte so schnell wie möglich behoben werden.

Anhangsverzeichnis

Anhang 1: Ergebnisse der Nmap Portscans

Anhang 1.1: TCP-Scan

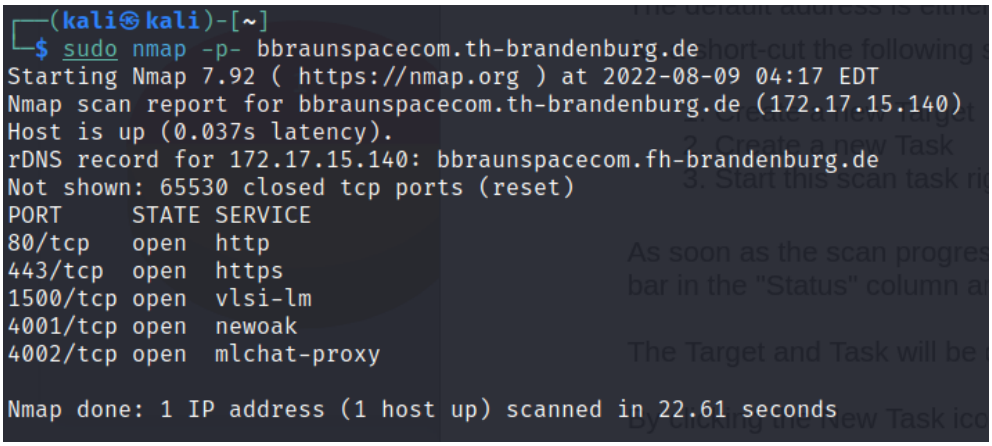


Abbildung 18: vollständige Ergebnisse des TCP-Scans der Pumpen

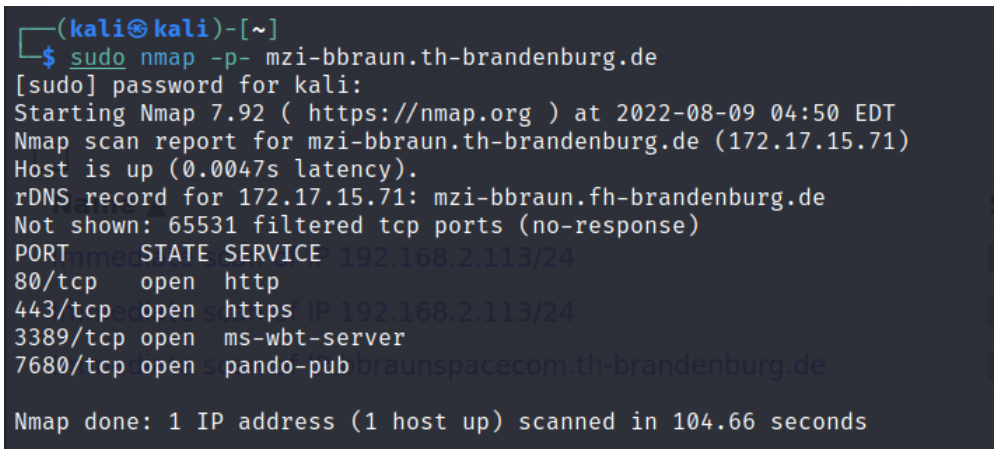


Abbildung 19: vollständige Ergebnisse des TCP-Scans der Online-Suite

Anhang 1.2: UDP-Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU bbraunspacecom.th-brandenburg.de
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 03:56 E
DT
Stats: 0:07:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 46.34% done; ETC: 04:13 (0:09:11 remaining)
Stats: 0:07:57 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 46.44% done; ETC: 04:13 (0:09:10 remaining)
Nmap scan report for bbraunspacecom.th-brandenburg.de (172.17.15.140)
Host is up (0.0058s latency).
rDNS record for 172.17.15.140: bbraunspacecom.fh-brandenburg.de
Not shown: 999 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp open|filtered dhcpc

Nmap done: 1 IP address (1 host up) scanned in 1083.87 seconds
```

Abbildung 20: vollständige Ergebnisse des UDP-Scans der Pumpen

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU mzi-bbraun.th-brandenburg.de
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 04:22 EDT
Nmap scan report for mzi-bbraun.th-brandenburg.de (172.17.15.71)
Host is up (0.0041s latency).
rDNS record for 172.17.15.71: mzi-bbraun.fh-brandenburg.de
All 1000 scanned ports on mzi-bbraun.th-brandenburg.de (172.17.15.71) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 1589.40 seconds
```

Abbildung 21: vollständige Ergebnisse des UDP-Scans der Online-Suite

Anhang 1.3: OS-Detection-Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O bbraunspacecom.th-brandenburg.de
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 04:58 EDT
Nmap scan report for bbraunspacecom.th-brandenburg.de (172.17.15.140)
Host is up (0.014s latency).
rDNS record for 172.17.15.140: bbraunspacecom.fh-brandenburg.de
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
1500/tcp open  vlsi-lm
4001/tcp open  newoak
4002/tcp open  mlchat-proxy
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32 - 2.6.35
Network Distance: 3 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
```

Abbildung 22: vollständige Ergebnisse der OS-Detection der Pumpen

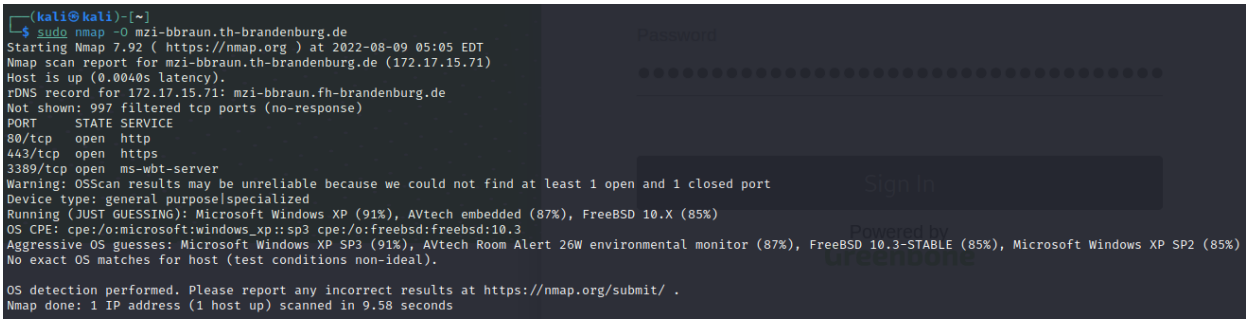


Abbildung 23: vollständige Ergebnisse der OS-Detection der Online-Suite

Anhang 1.4: SV-Detection-Scan

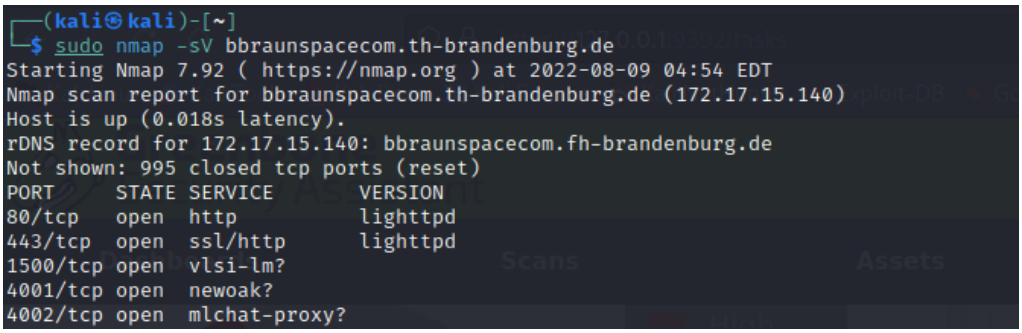


Abbildung 24: vollständige Ergebnisse der SV-Detection-Scans der Pumpen

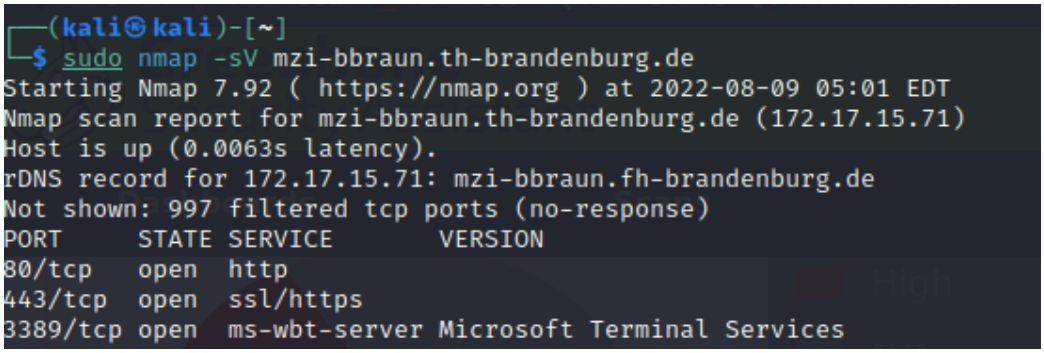


Abbildung 25: vollständige Ergebnisse der SV-Detection-Scans der Online-Suite

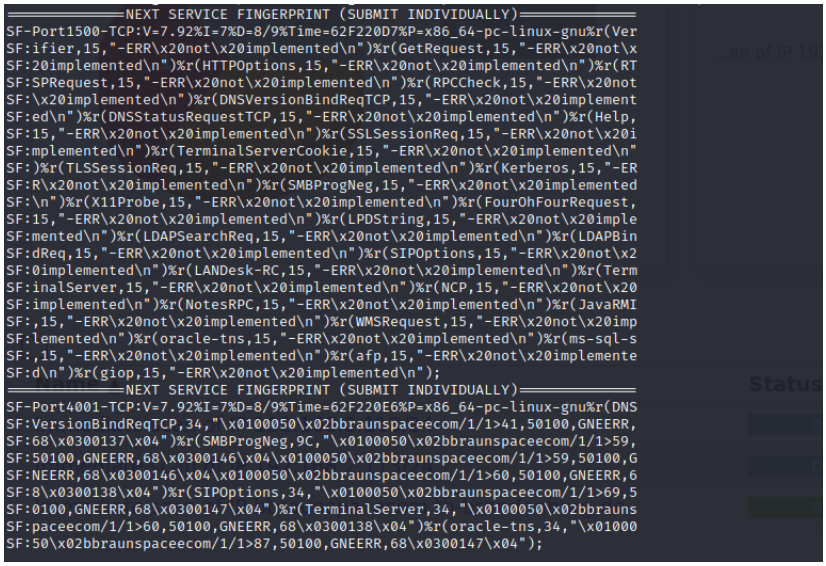


Abbildung 26: nicht erkannter Dienst (SV-Detection-Scan Pumpen)

Abbildung 27: erster nicht erkannter Dienst (SV-Detection-Scan Online-Suite)

Abbildung 28: zweiter nicht erkannter Dienst (SV-Detection-Scan Online-Suite)

Literaturverzeichnis

[1] E. McCann, „Healthcare data breaches on the rise, with potential $7B price tag," 06. 12. 2012. [Online]. Available: https://www.healthcareitnews.com/news/healthcare-data-breaches-trend-upward-come-potential-7b-price-tag. [Zugriff am 27. 11. 2022].

[2] I. Lella, M. Theocharidou, E. Tsekmezoglou, A. Malatras, C. Ardagna, S. Corbiaux, A. Sfakianakis und C. Douligeris, „ENISA Threat Landscape 2021," 27. 10. 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. [Zugriff am 02. 09. 2022].

[3] D. Truxius, E. Müller, N. Krupp, J. Suleder, O. Matula und D. Kniel, „ManiMed Abschlussbericht," 11. 12. 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/ManiMed_Abschlussbericht.html. [Zugriff am 05. 09. 2022].

[4] J. Suleder, A. Dewald und F. Grunow, „ERNW White Paper 66," 25. 04. 2018. [Online]. Available: https://ernw.de/en/whitepapers/issue-66.html. [Zugriff am 05. 09. 2022].

[5] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3. [Zugriff am 08. 09. 2022].

[6] Bundesamt für Sicherheit in der Informationstechnik, „IT-Sicherheit im Home-Office im Jahr 2020," 2020. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html. [Zugriff am 08. 09. 2022].

[7] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2022," 2022. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html. [Zugriff am 06. 12. 2022].

[8] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2022," 2022. [Online]. Available:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6. [Zugriff am 06. 12. 2022].

[9] S. Isabel, „Recommendations for safety and IT security," 2017. [Online]. Available: https://faculty-research.esmt.berlin/sites/faculty/files/2019-03/dsi-ipr_2017-6_en-de.pdf. [Zugriff am 27. 11. 2022].

[10] B. Filkins, „Health Care Cyberthreat Report," 02. 2014. [Online]. Available: https://www.qualityplusconsulting.com/res/infosec/2014-2_HealthCareCyberthreatReport.pdf. [Zugriff am 27. 11. 2022].

[11] E. Amberg und D. Schmid, „Hacking: Der umfassende Praxis-Guide," mitp, 2021, pp. 58-60.

[12] Gordon Lyon, „Nmap: Discover your network," n.d.. [Online]. Available: https://nmap.org. [Zugriff am 07. 09. 2022].

[13] S. Thelberg, „Nmap - what is it and how does it work," 29. 01. 2021. [Online]. Available: https://www.holmsecurity.com/resources/what-is-nmap. [Zugriff am 07. 09. 2022].

[14] Greenbone OpenVAS, „Greenbone OpenVAS," n.d.. [Online]. Available: https://www.openvas.org. [Zugriff am 07. 09. 2022].

[15] Wikipedia-Autoren, „OpenVAS," 21. 02. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=OpenVAS&oldid=1073203419. [Zugriff am 07. 09. 2022].

[16] Wireshark, „About Wireshark," n.d.. [Online]. Available: https://www.wireshark.org. [Zugriff am 21. 09. 2022].

[17] B. Jessey und J. T. Parker, „Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework," Wiley, 2017, pp. 2-9.

[18] F. Neugebauer, „Pentestit.de," 28. 10. 2017. [Online]. Available: https://pentestit.de/hak5-stellt-packet-squirrel-vor/. [Zugriff am 22. 09. 2022].

[19] tcpdump.org, „tcpdump," n.d.. [Online]. Available: https://www.tcpdump.org. [Zugriff am 22. 09. 2022].

[20] National Institute of Standards and Technology, „CVSS Vulnerability Metrics," n.d.. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Zugriff am 05. 09. 2022].

[21] B. Braun, „B. Braun Space OnlineSuite," 2016. [Online]. Available: https://docplayer.org/34586116-B-braun-space-onlinesuite.html. [Zugriff am 08. 12. 2022].

[22] G. Lyon, „Port Scanning Basics," n.d.. [Online]. Available: https://nmap.org/book/man-port-scanning-basics.html. [Zugriff am 28. 09. 2022].

[23] G. Lyon, „Port Specification and Scan Order," n.d.. [Online]. Available: https://nmap.org/book/man-port-specification.html. [Zugriff am 28. 09. 2022].

[24] G. Lyon, „UDP Scan," n.d.. [Online]. Available: https://nmap.org/book/scan-methods-udp-scan.html. [Zugriff am 30. 09. 2022].

[25] G. Lyon, „OS Detection," n.d.. [Online]. Available: https://nmap.org/book/man-os-detection.html. [Zugriff am 30. 09. 2022].

[26] G. Lyon, „Service and Version Detection," n.d.. [Online]. Available: https://nmap.org/book/man-version-detection.html. [Zugriff am 30. 09. 2022].

[27] Greenbone Networks, „7. Reports and Vulnerability Management," 07. 10. 2022. [Online]. Available: https://docs.greenbone.net/GSM-Manual/gos-21.04/en/reports.html. [Zugriff am 31. 10. 2022].

[28] Hacker Target, n.d.. [Online]. Available: https://hackertarget.com/openvas-tutorial-tips/. [Zugriff am 31. 10. 2022].

[29] Greenbone Networks, „11. Reports and Vulnerability Management," 30. 08. 2022. [Online]. Available: https://docs.greenbone.net/GCS-Manual/gcs/en/reports.html. [Zugriff am 31. 10. 2022].

[30] Hak5, „PacketSquirrel,“ n.d.. [Online]. Available: https://docs.hak5.org/packet-squirrel/getting-started/led-status-indications. [Zugriff am 04. 10. 2022].

[31] Internet Assigned Numbers Authority, „Service Name and Transport Protocol Port Number Registry,“ 12 10 2022. [Online]. Available: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml. [Zugriff am 13. 10. 2022].

[32] Wikipedia-Autoren, „List of TCP and UDP port numbers,“ 09. 10. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=List_of_TCP_and_UDP_port_numbers&oldid=1114998768. [Zugriff am 12. 10. 2022].

[33] Microsoft, „Welcome to Remote Desktop Services,“ 23. 12. 2021. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds. [Zugriff am 12. 10. 2022].

[34] Wikipedia-Autoren, „Pando (application),“ 27. 08. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Pando_(application)&oldid=1106918268. [Zugriff am 12. 10. 2022].

[35] net(t)work(s), n.d.. [Online]. Available: https://www.eisfair.org/fileadmin/eisfair/doc/node38.html. [Zugriff am 14. 10. 2022].

[36] G. Lyon, „Device and OS classification (Class lines),“ n.d.. [Online]. Available: https://nmap.org/book/osdetect-fingerprint-format.html#osdetect-class. [Zugriff am 18. 10. 2022].

[37] Wikipedia-Autoren, „Common Platform Enumeration,“ 21. 08. 2022. [Online]. Available: https://de.wikipedia.org/w/index.php?title=Common_Platform_Enumeration&oldid=225525155. [Zugriff am 18. 10. 2022].

[38] G. Lyon, „Usage and Examples,“ n.d. [Online]. Available: https://nmap.org/book/osdetect-usage.html. [Zugriff am 18. 10. 2022].

[39] G. Lyon, „Device Types,“ n.d.. [Online]. Available: https://nmap.org/book/osdetect-device-types.html. [Zugriff am 18. 10. 2022].

[40] Wikipedia-Autoren, „Lighttpd,“ 22. 06. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Lighttpd&oldid=1094348845. [Zugriff am 20. 10. 2022].

[41] IBM, „TLS protocol overview,“ 11. 08. 2022. [Online]. Available: https://www.ibm.com/docs/en/sdk-java-technology/7.1?topic=provider-tls-protocol-overview. [Zugriff am 03. 11. 2022].

[42] Bundesamt für Sicherheit in der Informationstechnik, „Man-In-The-Middle-Angriff,“ n.d.. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html. [Zugriff am 03. 11. 2022].

[43] Internet Engineering Task Force, „RFCs,“ n.d.. [Online]. Available: https://www.ietf.org/standards/rfcs/. [Zugriff am 05. 11. 2022].

[44] V. Jacobson, R. Braden und D. Borman, „TCP Extensions for High Performance,“ 05. 1992. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1323. [Zugriff am 05. 11. 2022].

[45] D. Borman, B. Braden, V. Jacobson und R. Scheffenegger, „TCP Extensions for High Performance,“ 09. 2014. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7323. [Zugriff am 05. 11. 2022].

[46] Wikipedia-Autoren, „Diffie–Hellman key exchange,“ 06. 11. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Diffie%E2%80%93Hellman_key_exchange&oldid=1120272073. [Zugriff am 08. 11. 2022].

[47] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelin und P. Zimmermann, 12. 10. 2015. [Online]. Available: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf. [Zugriff am 08. 11. 2022].

[48] Wikipedia-Autoren, „Elliptic-curve Diffie–Hellman,“ 11. 06. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Elliptic-curve_Diffie%E2%80%93Hellman&oldid=1092692098. [Zugriff am 08. 11. 2022].

[49] Wikipedia-Autoren, „Elliptic-curve cryptography," 31. 10. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Elliptic-curve_cryptography&oldid=1119186096. [Zugriff am 08. 11. 2022].

[50] Wikipedia-Autoren, „Transmission Control Protocol," 11. 11. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Transmission_Control_Protocol&oldid=1121332899. [Zugriff am 12. 11. 2022].

[51] F.-H. Hsu, Y.-L. Hwang, C.-Y. Tsai, W.-T. Cai, C.-H. Lee und K. Chang, „TRAP: A Three-way handshake server for TCP connection establishment," 2016. [Online]. Available: https://www.researchgate.net/publication/310473420_TRAP_A_Three-way_handshake_server_for_TCP_connection_establishment/link/5bafcdc992851ca9ed30d089/download. [Zugriff am 12. 11. 2022].

[52] D. E. Comer, in *Internetworking with TCP/IP*, New Jersey, Alan Apt, 2000, p. 211.

[53] Wikipedia-Autoren, „SOAP," 31. 08. 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=SOAP&oldid=1107766999. [Zugriff am 15. 11. 2022].

[54] IBM, „The structure of a SOAP message," 24. 08. 2022. [Online]. Available: https://www.ibm.com/docs/en/integration-bus/10.0?topic=soap-structure-message. [Zugriff am 15. 11. 2022].

[55] Internet Society, „TLS Basics," n.d.. [Online]. Available: https://www.internetsociety.org/deploy360/tls/basics/. [Zugriff am 17. 11. 2022].

[56] National Cancer Institute, „bolus dose," National Cancer Institute at the National Institutes of Health, n.d.. [Online]. Available: https://www.cancer.gov/publications/dictionaries/cancer-terms/def/bolus-dose. [Zugriff am 19. 11. 2022].

[57] Microsoft-Autoren, „Why Floating-Point Numbers May Lose Precision," Microsoft, 03. 08. 2021. [Online]. Available: https://learn.microsoft.com/en-us/cpp/build/why-floating-point-numbers-may-lose-precision?view=msvc-170. [Zugriff am 19. 11. 2022].

[58] T. T. Abi und S. Kaushik, „UpGuard What is an Open Port? | Definition & Free Checking Tools for 2022,“ 11. 05. 2022. [Online]. Available: https://www.upguard.com/blog/open-port. [Zugriff am 23. 11. 2022].

[59] Lighttpd, „Lighttpd Important changes,“ 12. 03. 2014. [Online]. Available: https://www.lighttpd.net/2014/3/12/1.4.35/. [Zugriff am 24. 11. 2022].

[60] End of Life, „TLS Lifecycle (EOL),“ nd. [Online]. Available: https://endoflife.software/protocols/encryption/tls. [Zugriff am 24. 11. 2022].

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Ich willige ein, dass meine Arbeit mittels einer Plagiatssoftware überprüft werden kann.