UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Praktikum 4

Netzwerksicherheit

Zu bearbeiten bis zum 16. Mai 2023

Cybersecurity im Sommersemester 2023

Jan Wichelmann, Anja Köhl

Einführung

Nachdem Sie in den vergangenen Praktika vor allem die lokale Systemsicherheit untersucht haben, soll es nun um die Sicherheit von Netzwerkkommunikation gehen. In diesem Praktikum werden Sie einige Tools ausprobieren, die das Mitschneiden und sogar Einbrechen in verschlüsselte WLAN-Verbindungen erlauben.

Im Gegensatz zu den anderen Praktika ist dieses Praktikum nicht ausschließlich online lösbar – einige Dinge wie lokale WLAN-Netze lassen sich leider nur schlecht anders darstellen. Falls Sie am Präsenztermin verhindert sein sollten, wenden Sie sich bitte an die Betreuer.

Bitte beachten Sie, dass das vom ITS bereitgestellte Netz nicht das einzige Netz ist, das um den Praktikumsraum herum aktiv ist; gleichzeitig lässt sich nicht der komplette Verkehr anderer Netze ohne weiteres herausfiltern, sodass Sie diesen zwangsläufig ebenfalls auffangen werden. Während das passive Mitscheiden durch die Verschlüsselung kein großes Problem darstellt, gilt es bei den *aktiven* Angriffskomponenten sehr sorgfältig zu arbeiten, damit diese ausschließlich auf unser getrenntes Netz zielen (wo der Einsatz entsprechender Tools explizit erlaubt ist). Bitte lesen Sie daher immer erst die gesamte Aufgabe inklusive Hinweisen[1], bevor Sie beginnen diese zu bearbeiten. Wenn Sie sich bei einer Maßnahme unsicher sind, fragen Sie die Betreuer!

Aufgabe 1 Vorbereitung

Für dieses Praktikum benötigen Sie einen WLAN-Adapter mit *Monitor Mode* Unterstützung, sowie die Softwarepakete *Thunderbird*[2], *Wireshark*[3] und *aircrack-ng*[4].

Idealerweise arbeiten Sie hierfür auf einem Linux-System. Falls Sie auf Ihrem Gerät kein entsprechendes System zur Verfügung haben oder dort keine spezielle Software installieren möchten, können Sie sich gern bei den Betreuern einen USB-Stick mit einem vorinstallierten Ubuntu-System ausleihen. Dieses System bringt alle nötigen Tools mit und kann mit Ihrem Gerät gebootet werden[5].

Ob Ihr WLAN-Adapter den Monitor Mode unterstützt, können Sie mit dem Befehl `iw list` herausfinden (mit Root-Rechten ausführen). Im Eintrag für Ihren WLAN-Adapter müsste dort unter `Supported interface modes` der Eintrag `monitor` auftauchen. Falls Ihr WLAN-Adapter dies nicht unterstützen sollte, können Sie sich von den Betreuern einen portablen Adapter bzw. ein Notebook ausleihen, der/das diese Funktion mitbringt (achten Sie dann im Folgenden darauf, mit dem richtigen Adapter zu arbeiten).

[1] ...und Fußnoten
[2] `https://www.thunderbird.net/`
[3] `https://www.wireshark.org/`
[4] `https://www.aircrack-ng.org/`
[5] Gegebenenfalls müssen Sie hierfür die Bootreihenfolge ändern, oder beim Start manuell das zu bootende Gerät auswählen. Falls bei Ihnen Secure Boot aktiviert ist, kann es zu Problemen kommen – in diesem Fall müssen Sie in Ihrer BIOS/UEFI Konfiguration die entsprechende Funktion abschalten.

Aufgabe 2 Eigenen Netzwerkverkehr mitschneiden: E-Mail-Sicherheit

Im ersten Schritt geht es darum, sich mit Wireshark vertraut zu machen und dabei etwas über die Sicherheit von E-Mail-Kommunikation herauszufinden. In diesem Teil schneiden Sie daher erstmal nur den Verkehr mit, der von ihnen stammt oder der an Sie adressiert ist.

Hierfür haben die Betreuer einen E-Mail-Server aufgesetzt, den Sie im unverschlüsselten Netz `ITS-Lab-Insecure` erreichen können. Der Server stellt die Protokolle IMAP (zum Abrufen von E-Mails) und SMTP (zum Versenden von E-Mails) zur Verfügung.

1. Verbinden Sie sich mit dem Netz `ITS-Lab-Insecure`.
2. Starten Sie Thunderbird und richten Sie ein neues E-Mail-Konto ein:
   - Benutzername: (wird Ihnen von den Betreuern mitgeteilt)
   - Passwort: (wird Ihnen von den Betreuern mitgeteilt)
   - IMAP Hostname: `its-cybersec`[6]
   - IMAP Connection Security: None
   - IMAP Port/Authentication/Username: Vorgegebene Standardwerte lassen
   - SMTP Hostname: `its-cybersec`
   - SMTP Connection Security: None
   - SMTP Port/Authentication/Username: Vorgegebene Standardwerte lassen

   Ein Klick auf `Re-test` sollte die leer gelassenen/Autodetect Felder automatisch ausfüllen. Anschließend können Sie das neue Konto speichern. Sie sollten nun in dessen Posteingang eine E-Mail von `admin@mail.its` vorfinden.
3. Starten Sie nun Wireshark und lassen Sie es auf dem mit `ITS-Lab-Insecure` verbundenen WLAN-Adapter lauschen. Richten Sie einen geeigneten Displayfilter ein, damit Ihnen nur SMTP-Pakete angezeigt werden.
4. Versenden Sie eine E-Mail mit einem netten Gruß an Ihre Nachbargruppe (oder sich selbst), und untersuchen Sie den aufgefangenen Netzwerkverkehr. Welche Daten konnten Sie dort mitschneiden? ◀ 40 / 8
5. Erzeugen Sie sich unter *Tools* > *OpenPGP Key Manager* ein neues Schlüsselpaar. Versenden Sie den öffentlichen Schlüssel anschließend an Ihre Nachbargruppe, und bitten Sie diese, Ihnen ebenfalls einen Schlüssel zukommen zu lassen. Alternativ können Sie mit `admin@mail.its` kommunizieren, in dessen E-Mail an Sie bereits ein Schlüssel angehängt ist.
6. Versenden Sie an Ihre Nachbarn (bzw. admin) eine PGP-verschlüsselte E-Mail. Schneiden Sie wieder den Netzwerkverkehr mit und analysieren Sie, welche Daten dort preisgegeben werden. ◀ 40 / 8
7. Gehen Sie in die Kontoeinstellungen und ändern Sie bei den SMTP-Einstellungen die Connection Security auf `STARTTLS`. Versenden Sie anschließend erneut eine unverschlüsselte E-Mail an Ihre Nachbarn und untersuchen Sie den Netzwerkverkehr. ◀ 40 / 8

Hinweise:

- (auch für die nachfolgenden Aufgaben) Lassen Sie die Wireshark-Aufzeichnung nicht durchgehend laufen, da diese alle empfangenen Pakete im Arbeitsspeicher ablegt. Ist der Speicher voll, kann die Aufzeichnung abstürzen oder das System langsam/instabil werden. Es ist besser, immer nur kurze Zeitfenster (z.B. eine Minute lang) aufzuzeichnen, da Sie so erstens nur den Verkehr bekommen, der Sie wirklich interessiert, und zweitens das Filtern und Untersuchen dessen erheblich schneller wird. Etwaige im Netzwerkverkehr versteckte Geheimnisse und Flags werden häufig genug gesendet, dass Sie diese auch bei einer Minute Aufzeichnungsdauer auf jeden Fall mindestens einmal auffangen können.
- SMTP codiert Passwörter unter Umständen mit Base64. Sie können diese mittels `echo "<code>" | base64 -d` decodieren.

[6] Falls Sie nicht auf einem von den Betreuern vorkonfigurierten System arbeiten, tragen Sie bitte `192.168.1.10 its-cybersec` in Ihre `/etc/hosts`-Datei ein.

Aufgabe 3 Beliebigen unverschlüsselten Netzwerkverkehr mitschneiden

Nachdem Sie in der letzten Aufgabe den eigenen Netzwerkverkehr mitgeschnitten haben, geht es nun darum den *gesamten* Verkehr des Netzes aufzufangen und zu analysieren. Hierzu müssen Sie Ihren Netzwerkadapter in den *Monitor Mode* versetzen: Normalerweise leitet der Adapter nur die Pakete weiter, die auch für Sie bestimmt sind (also die entsprechende MAC-Adresse tragen). Im Monitor Mode werden stattdessen *alle* Pakete weitergeleitet die von diesem aufgefangen werden, also auch solche die zwischen anderen Geräten ausgetauscht werden. Zunächst beschränken wir uns wieder auf das unverschlüsselte Netzwerk `ITS-Lab-Insecure`.

1. Das Netzwerk `ITS-Lab-Insecure` wird ausschließlich auf Kanal 6 gesendet. Nutzen Sie das `airmon-ng` Programm, um ein Monitor-Mode-Netzwerkinterface für Ihren WLAN-Adapter zu erstellen, das sämtliche Pakete auf Kanal 6 mitschneidet. Der Name des erstellten Interface wird Ihnen ausgegeben.

   Anschließend kann es nötig sein, das Interface mittels `ip link set <interface name> up` zu aktivieren. Den Status des Interface können Sie mittels `ip addr` einsehen.

2. Starten Sie Wireshark und zeichnen Sie den Netzwerkverkehr auf dem Monitor-Mode-Netzwerkinterface auf. Nutzen Sie die verschiedenen Filterfunktionen, um die aufgefangenen Pakete zu analysieren. Finden Sie das Geheimnis, das in einem TCP-Chat von Alice an Bob gesendet wird.

◀ 130 / 0

Hinweise:

- Im Monitor Mode verlieren Sie wahrscheinlich die WLAN-Verbindung, und können diese erst wieder aufbauen nachdem Sie mit `airmon-ng` wieder den Monitor Mode verlassen haben. Dies liegt am geänderten Betriebsmodus des WLAN-Adapters, da dieser in eine Art passiven Modus versetzt wird.

Aufgabe 4 In WPA2-Netzwerk einbrechen (freiwillig)

Zuletzt untersuchen wir, wie man mit einem Offline-Wörterbuchangriff in ein verschlüsseltes WPA2-Netzwerk einbrechen und die darin verschickten Daten extrahieren kann. Das einzige, was hierfür nötig ist, ist das Mitschneiden des 4-Wege-Handshakes zwischen dem Access Point und einem Gerät das sich in dem Netz befindet.

Das Zielnetz trägt den Namen `ITS-Lab-WPA2` und wird vom Access Point mit der MAC-Adresse `50:C7:BF:91:6C:A0` ausgestrahlt. Die MAC-Adresse des mit dem WLAN verbundenen Geräts wird im Praktikum bekanntgegeben.

1. Beenden Sie den Monitor-Mode ihres WLAN-Adapters, falls dieser von der vorherigen Aufgabe noch aktiv sein sollte. Die in dieser Aufgabe genutzten Programme starten und beenden den Modus selbstständig.

2. Nutzen Sie `airodump-ng`, um das Netzwerk mit der (E)SSID `ITS-Lab-WPA2` zu finden. Auf welchem Kanal wird das Netzwerk ausgestrahlt?

3. Im nächsten Schritt müssen Sie einen 4-Wege-Handshake aufzeichnen. Hierfür müssen zwei Dinge geschehen: Erstens sollten sämtliche entsprechenden Pakete mitgeschnitten und für die spätere Analyse abgespeichert werden. Zweitens muss ein entsprechender Handshake erst ausgelöst werden, denn in einer einmal etablierten Verbindung kommt ein solcher nicht mehr vor.

   Erstellen Sie einen Ordner, in dem Sie mitgeschnittene Pakete speichern können. Nutzen Sie das `airodump-ng` Programm, um das Zielnetzwerk zu belauschen (die `--bssid` Option ist hier nützlich) und Handshake-Pakete abzuspeichern. Stellen Sie sicher, dass Sie auf dem richtigen Kanal lauschen, um Paketverluste durch das Scannen anderer Kanäle zu vermeiden.

   Während der Mitschnitt läuft, nutzen Sie in einem separaten Terminal das Programm `aireplay-ng`, um das Zielgerät mit einem *Deauthentication*-Paket vom Netzwerk zu trennen. Fälschen Sie dieses Paket hierfür so, dass es aussieht als wäre es vom Access Point gekommen, und nicht von Ihnen. Beachten Sie, dass sie eventuell mehrere Versuche benötigen.

4. Sobald Ihnen im Terminal mit dem `airodump-ng` Prozess angezeigt wird, dass ein WPA2-Handshake aufgezeichnet werden konnte (EAPOL-Frames), können Sie das Mitschneiden beenden. Nutzen Sie nun die aufgezeichneten Pakete, um daraus mithilfe von `aircrack-ng` und dem im Moodle bzw. unter `http://cybersec/` bereitgestellten Wörterbuch das Passwort zu bestimmen.

◁ 170 / 0

5. Falls Sie Flags suchen und glauben, dass in den mit WPA2 verschlüsselten Paketen der Netzwerkteilnehmer etwas versteckt sein könnte, können Sie dies mit Wireshark bewerkstelligen: Nachdem Sie Ihren Adapter wieder in den Monitor Mode versetzt haben, lässt sich in Wireshark unter *Edit* > *Preferences* > *Protocols* > *IEEE 802.11* > *Decryption Keys* das WLAN-Passwort hinterlegen. Anschließend können Sie sämtliche Kommunikation entschlüsseln, für die Sie einen 4-Wege-Handshake abgefangen haben (hier lässt sich mit `aireplay-ng` wieder nachhelfen).