Prüfungsleistung für MA-TINF21CS2 Vorlesung Network Security

Beschreibung der Prüfungsleistung

Die Prüfungsleistung besteht aus dem Programmentwurf zweier Programme, der dazugehörigen Dokumentation sowie der Demonstration von beiden Programmen im Rahmen einer Kurzpräsentation.

Die Prüfungsleistung darf als Gruppe mit maximal vier Teilnehmer:innen erbracht werden. Die Bewertung der Prüfungsleistung erfolgt gemeinsam für alle Teilnehmer:innen der Gruppe. Eine individuelle Bewertung der einzelnen Teilnehmer:innen ist nicht vorgesehen.

Szenario Beschreibung

Mit Hilfe von zwei selbst entwickelten Programmen soll die Extraktion von Daten über das Netzwerk nachgestellt und demonstriert werden. Das erste Programm („Programm A“) extrahiert die zu übertragenden Daten aus einer Textdatei und sendet diese an das zweite Programm („Programm B“) über das Netzwerk. Das zweite Programm stellt die empfangenen Daten als Ausgabe auf dem Bildschirm dar. Als Methode für die Extraktion über das Netzwerk kann eine der folgenden drei Methoden gewählt werden: ARP, ICMP, DNS. Die Programmiersprache ist frei wählbar.

Um eventuell vorhandene Sicherheitssysteme zu umgehen und die Erkennung zu erschweren, dürfen die extrahierten Daten nicht im Klartext, sondern nur codiert über das Netzwerk übertragen werden.

Im Rahmen des Szenarios wird davon ausgegangen, dass Programm A bereits im Netzwerk erfolgreich durch einen vorherigen Angriff installiert wurde (z.B. durch einen Drive-by Download oder über einen entsprechend gestalteten Anhang in einer E-Mail).

Ebenfalls kann davon ausgegangen werden, dass Programm B an einer entsprechenden Stelle im Netz bereits vorhanden ist und unter vollständiger Kontrolle der angreifenden Partei steht:

- Bei Methode ARP befindet sich Programm B in der gleichen Broadcast Domain wie Programm A.
- Bei den Methoden ICMP und DNS befindet sich Programm B aus Vereinfachungsgründen innerhalb des gleichen IPv4 Subnetzes wie Programm A.

Zu übertragender Text

Der folgende Text stellt die zu extrahierenden Daten dar und soll als auslesbare Textdatei auf dem Computersystem von Programm A vorhanden sein. Es handelt sich hierbei um das „Nullte Gesetz“ (siehe https://de.wikipedia.org/wiki/Robotergesetze). Der Text ist vollständig inklusive Leer- und Sonderzeichen zu übertragen:

```
0. Ein Roboter darf die Menschheit nicht verletzen oder
   durch Passivität zulassen, dass die Menschheit zu Schaden
   kommt.
1. Ein Roboter darf keinen Menschen verletzen oder durch
   Untätigkeit zu Schaden kommen lassen, außer er verstieße
   damit gegen das nullte Gesetz.
2. Ein Roboter muss den Befehlen der Menschen gehorchen – es
   sei denn, solche Befehle stehen im Widerspruch zum
   nullten oder ersten Gesetz.
3. Ein Roboter muss seine eigene Existenz schützen, solange
   sein Handeln nicht dem nullten, ersten oder zweiten
   Gesetz widerspricht.
```

Prüfungsleistung Programmentwurf

Beschreibung Programm A

Programm A stellt im Szenario die Malware dar, welche vom User des Systems heruntergeladen und gestartet wurde. Folgende Funktionen müssen im Programm A gegeben sein:

1. Auslesen der Textdatei mit den zu extrahierenden Daten (siehe vorherigen Absatz).
2. Codierung des Textinhaltes mit einem geeigneten Codierungsverfahren (zum Beispiel Base64). Eine symmetrische oder asymmetrische Verschlüsselung der Daten ist nicht erforderlich und wird im Rahmen der Prüfungsleistung gleichrangig wie ein anderes geeignetes Codierungsverfahren gewertet.
3. Senden der codierten Daten über den Netzwerkstack mit Hilfe einer der folgenden Methoden: ARP, ICMP, DNS.

Beschreibung Programm B

Programm B stellt im Szenario die Software des Angreifers dar, welche die von der Malware gesendeten Daten empfängt, decodiert und als Bildschirmausgabe darstellt. Folgende Funktionen müssen im Programm B gegeben sein:

1. Empfang der von Programm A gesendeten Daten vom Netzwerkstack.
2. Decodierung der Daten (Umwandlung in Text).
3. Ausgabe der decodierten Daten auf dem Bildschirm.

Beschreibung des Netzwerksetups für das Szenario

Programm A und Programm B müssen in zwei unterschiedlichen Betriebsumgebungen gestartet werden und über ein Netzwerk miteinander verbunden sein. Dies kann durch eine der beiden genannten Methoden umgesetzt werden:

- Zwei physikalisch getrennte Computersysteme, welche über einen Switch miteinander verbunden sind (Computersystem A für Programm A, Computersystem B für Programm B). Sowohl auf Computersystem A als auch auf Computersystem B muss zur Überprüfung des Netzwerkverkehrs das Programm Wireshark (www.wireshark.org) vorhanden sein. Programm A und Programm B können hier jeweils pro Computersystem auch in einer virtualisierten Umgebung laufen.
- Ein Computersystem mit einer Virtualisierungslösung, welche zwei virtuelle Gastsysteme beinhaltet (Gastsystem A für Programm A, Gastsystem B für Programm B). Die beiden virtuellen Gastsysteme sind durch die Virtualisierungslösung netzwerktechnisch miteinander verbunden. Sowohl im Gastsystem A als auch im Gastsystem B muss zur Überprüfung des Netzwerkverkehrs das Programm Wireshark vorhanden sein.

Prüfungsleistung Dokumentation

Die im Rahmen der Prüfungsleistung zu erstellende Dokumentation muss folgende Punkte umfassen:

- Die Vor- und Nachnamen aller Teilnehmer:innen der Gruppe
- Gewählte Angriffsmethode (ARP, ICMP oder DNS)
- Eine technische Beschreibung der gewählten Angriffsmethode - wie erfolgt der Transport der extrahierten Daten über den Netzwerkstack?
- Name und Beschreibung des gewählten Codierungsverfahrens (bei Methodik ICMP und DNS) bzw. Darstellung der Codierungstabelle (bei Methodik ARP)
- Empfehlungen, wie die gewählte Angriffsmethode im Netz erkannt und gegebenenfalls verhindert werden könnte

Prüfungsleistung Kurzpräsentation

Die Funktionsfähigkeit der beiden Programme A und B soll im Rahmen einer Kurzpräsentation durch die Gruppe demonstriert werden.

Bewertungsmatrix

Im Rahmen dieser Prüfungsleistung können maximal 5 (fünf) ECTS-Leistungspunkte erzielt werden. Die Bewertung erfolgt dabei anhand der folgenden Prüfpunkte für die gesamte Gruppe:

Prüfpunkte	**Anzahl erreichbarer ECTS-Leistungspunkte**
Programm A: • Erfolgreiches Auslesen der Textdatei mit dem vorgegebenen Text • Codierung mit dem in der Dokumentation beschriebenen Codierungsverfahren • Erfolgreiches Senden der codierten Daten über den Netzwerkstack mit dem dafür vorgesehenen Netzwerkprotokoll • Die Daten werden nicht im Klartext übertragen * Programm B: • Empfang der von Programm A gesendeten und codierten Daten vom Netzwerkstack • Decodierung mit dem in der Dokumentation beschriebenen Codierungsverfahren und Überführung in Klartext • Ausgabe des vorgegebenen Textes auf dem Bildschirm inklusive aller Satz-, Sonder- und Leerzeichen	2 2
Dokumentation	1
Kurzpräsentation **	0

* Bei ARP ist es technisch nicht möglich, eine Übertragung der Daten in Klartext vorzunehmen. Dieser Prüfpunkt gilt daher automatisch als erfüllt, wenn Programm A erfolgreich die Daten über das Netzwerk sendet und die vom Programm A erzeugten ARP Requests im Netzwerkstack mittels Wireshark sichtbar sind.

** Die Kurzpräsentation selbst wird nicht bewertet. Im Rahmen der Kurzpräsentation wird aber die erfolgreiche Durchführung der Datenextraktion von der Gruppe demonstriert und dient somit als Basis für die Bewertung der anderen Prüfpunkte.

Ein Code Review von Programm A und Programm B im Rahmen der Prüfungsleistung und deren Bewertung wird sich vorbehalten.