simeon weigel MICHAEL FREVERT Daniel nagel Devin alexander meier nikolai kloß Eduard Ljaschenko Dominik schulz Daniel Haering Martin Ziel Felix Schilk Gerrit haake

Fachhochschule Bielefeld

Lehrgebiet Sicherheit und zuverlässigkeit

Prof. Dr. Christoph Thiel

Sicherheit und Zuverlässigkeit

Wintersemester 2017/2018

Dokumentation

Sicherheit und Zuverlässigkeit

6. Dezember 2017

Inhaltsverzeichnis

Inhaltsverzeichnis1

1 Einleitung2

1.1 Projektbeschreibung2

1.2 Zweck des Dokuments2

1.3 Aufteilung der Teams | Aufgabenverteilung3

1.4 Verwendete Tools3

1.5 Beschreibung Security Onion4

1.6 Beschreibung KaliLinux4

1.7 Charakterisierung der vorgestellten Angriffe5

2 Detaillierte Angriffsbeschreibungen und Gegenmaßnahmen6

2.1 Datendiebstahl physisch6-10

2.2 Exploitangriff10f

2.3 Penetrationsangriff11f

2.4 WLAN-Angriff12f

2.5 Spoofingangriff13f

**8 Glossar14**

**9 Quellen15**

# Einleitung

# Projektbeschreibung

In diesem Projekt stellen wir die Konzeption und Durchführung verschiedener Hackingangriffe vor. In einem Beispielszenario werden mögliche Fallbeispiele und Angriffe vorgestellt, sowie mögliche Schutzmaßnahmen aufgezeigt. Die technischen Hintergründe werden näher erklärt und ggf. eine zugrunde liegende Systemarchitektur näher erläutert. Zudem werden die Linux-Distributionen *KaliLinux* und *SecurityOnion* vorgestellt.

# Zweck des Dokuments

Diese Dokumentationist ein Dokument, welches einen Überblick über verschiedene Hackingangriffe vermitteln soll und wie man sich vor diesen schützen kann. Zudem werden die Linux-Distributionen *KaliLinux* und *SecurityOnion* vorgestellt, mit denen man sich weiteres Wissen zum Aufspüren von Sicherheitslücken sowie Abwehrmaßnahmen gegen Hackingangriffe aneignen kann. Der Leser soll nach Lesen dieses Dokuments die Vorgehensweise und den Ablauf verschiedener Angriffe besser verstehen.

# Aufteilung der Teams | Aufgabenverteilung

Zunächst wurde das Team auf zwei einzelne Gruppen aufgeteilt. Zum einen, die Angreifer, die sich über die Linux-Distribution KaliLinux informiert haben und sich Informationen zum Ablauf verschiedener Angriffe überlegt haben.

Team Offense

Nikolai Kloß, Daniel Haering, Daniel Nagel, Devin Alexander Meier, Eduard Ljaschenko

Zudem die Verteidiger, sich über die Linux-Distribution SecurityOnion informiert haben und sich Informationen zur Abwehr und zu den Schutzmaßnahmen gegen verschiedene Hackingangriffe überlegt haben.

Team Defense

Martin Ziel, Felix Schilk, Gerrit Haake, Michael Frevert, Dominik Schulz, Simeon Weigel

Nach Abschluss dieser Maßnahmen wurden kleinere Teams gebildet, die verschiedene Angriffe gemeinsam ausgearbeitet und dokumentiert haben. Diese bestanden meist aus einem Mitglied des Team Offense und einem Mitglied des Team Defense. Dadurch fanden bessere und zielführende Absprachen und Ausarbeitungen statt.

*Datendiebstahl physisch:* Simeon Weigel

*Exploitangriff*: Daniel Haering, Dominik Schulz, Felix Schilk

*Penetrationsangriff:* Devin Alexander Meier, Martin Ziel

*WLAN-Angriff:* Eduard Ljaschenko*, Nikolai Kloß*

*Spoofingangriff:* Daniel Nagel*,* Michael Frevert*,* Gerrit Haake

# Verwendete Tools

Folgende Tools wurden verwendet:

|  |  |  |
| --- | --- | --- |
| **Tool** | **Version** | **Bemerkung** |
| Git | aktuell | Versionierung |
| KaliLinux | 2017.3 | Offense |
| Security Onion | 14.04.5.5 | Defense |

# Beschreibung Security Onion

Security Onion ist eine Linux-Distribution für Intrusion Detection1 und Network Security Monitoring2. Es bietet viele nützliche Instrumente zum Erfassen, Erkennen und Analysieren in einer NSM-Suite.

* Welche Tools haben wir benutzt!? Darauf eingehen!?Iwie komplex?

# Beschreibung KaliLinux

Kali Linux ist eine Linux-Distribution, die verschiedene Tools zum Aufspüren von Sicherheitslücken und Konfigurationsfehlern bereitstellt. Mit diesen Tools können verschiedenste Angriffe ausgeführt werden.

* Welche Tools haben wir benutzt!? Darauf eingehen!? Wie komplex?

***Hinweis !!!***

Viele der mitgelieferten Tool sind ausschließlich für den privaten oder autorisierten Gebrauch zugelassen. Die Nutzung der Tools dazu, in fremde Systeme einzudringen, stellt nach der derzeitigen Rechtslage eine Straftat dar.

1: System zur Erkennung von Angriffen

2: Zeichnet und zeigt Netzwerkverkehr auf

# Charakterisierung der vorgestellten Angriffe

Im Folgenden Abschnitt wird auf die Charakterisierung der einzelnen Angriffe eingegangen. Es wird ein kurzer Überblick vermittelt, was die Idee hinter diesen Angriffen ist und wie diese grob funktionieren.

1. ***Datendiebstahl physisch***

Bei klassischem physischen Datendiebstahl werden sicherheitsrelevante oder persönliche Daten durch physischen Datenklau vollzogen. Daten werden von einem Datenträger in einem Verbundsystem oder von einen mobilen System entwendet. Die Durchführung dazu kann ganz unterschiedlich ausfallen. Der kritische und relevante Sicherheitsfaktor stellt dabei immer der Mensch dar (human factor).

1. ***Exploitangriff***

Beim Exploitangriff wird eine Schadsoftware geschickt und unbemerkt auf das Zielsystem geschleust. Der Prozess findet im Hintergrund ohne Erkenntnis des Benutzers statt und sammelt gewünschte Informationen für den Angreifer.

1. ***Penetrationsangriff***

Bei einem Penetrationstest werden wiederholt Befehle, Anforderungen, Nachrichten o.ä. an das Zielsystem versendet, mit der Absicht, das Zielsystem teilweise oder komplett außer Funktion zu setzen.

1. ***WLAN-Angriff***

Bei einem WLAN-Angriff verschaffen sich Angreifer unbefugten Zugriff in das Netzwerk oder sogar auf im Netzwerk angemeldete Rechner.

1. ***Spoofingangriff***

Beim ARP-Spoofing werden gefälschte ARP-Pakte versendet, mit dem Ziel, das eine Kommunikation zwischen Rechnersystemen in einem Netzwerk stattfindet, die fälschlicherweise als eine sichere Verbindung angesehen wurde.

Im nächsten Kapitel wird der Ablauf und die Vorgehensweise, sowie Schutzmaßnahmen für jeden Angriff ausführlich beschrieben. Technische Details sowie die zugrunde liegende Systemarchitektur werden erläutert.

# Detaillierte Angriffsbeschreibungen und Gegenmaßnahmen

# Datendiebstahl physisch

|  |  |
| --- | --- |
| 1. **Angriffsbeschreibung Angriffsbeschreibung** | |
| **Name:** Datendiebstahl von Festplatte(physisch) | **Hauptverantwortlicher**: Simeon Weigel |
| **Ziel des Angriffs**: Datendiebstahl | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Frau Müller , Herr Zimmermann **Fallbeschreibung**:  Frau Müller möchte ihren alten USB-Stick auf eBay verkaufen. Aus Angst, das jemand ihre persönlichen Daten lesen kann, löscht Sie ihre Daten.  (Exemplarisch eine *Textdatei*: LoginnamePasswort). | |
| 1 . Ausgangssituation: | |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *2. Nach Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Frau Müller verkauft ihren USB-Stick an Herrn Zimmermann auf ebay. Herr Zimmermann hat böse Absichten und möchte sich den Daten von Frau Müller annehmen. Dazu verwendet er das Freewareprogramm *Recuva*, mit dem sich gelöschte Daten widerherstellen lassen. |
| *3. Wiederherstellen der Datei mit Recuva* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *4. Inhalt der Datei nach Wiederherstellung* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Der Angreifer kann nun alle vertrauliche Daten von Frau Müller einsehen. |
| **Kommentare**: Ein mögliches Szenario wäre zudem, das man seinen USB-Stick entsorgt und ein Angreifer sich diesen annimmt. |
| **Schutzmaßnahmen** |
| Um sich gegen so einen physischen Angriff zu schützen, kann man seinen USB-Stick sicher überschreiben. Zum Beispiel mit dem Programm: Abylon Shredder. Mit diesem wird der Speicherplatz überschrieben und der Angreifer kann somit Dateien nicht widerherstellen. |
| *5. Sicheres Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Das Programm recuva erkennt die Datei noch……* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *6. Die Datei kann jedoch nicht mehr so wiederhergestellt werden, wie sie ursprünglich war* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Ein Encodieren der Zeichen ist auf keinen Fall möglich!!! |
| **Kommentare**:  Das Programm Abylon Shredder besitzt 5 verschiedene Sicherheitslevel:  0: normales Löschen – Verknüpfungen entfernen  1: 2x überschreiben mit binären Nullen  2: 3x überschreiben mit Nullen und Zufallszahlen  3: 7x überschreiben nach DoDII-Methode  4: 13x überschreiben DoDII und Zufallszahlen  5: 35x überschreiben (Peter Gutman Methode)  Diese Möglichkeit schützt nicht davor, wenn man vertrauliche Daten in Dateinamen schreibt.  Technische Details:   * In jedem USB-Stick befinden sich sogenannte Flash-Speicherzellen, die wie Transistoren funktionieren. Zum größten Teil bestehen sie aus einem Halbleiter-Material, zum Beispiel aus Silizium. Darin befinden sich zwei kleinere Bereiche aus viel leitfähigerem Material, Source (Quelle) und Drain (Abfluss). * Durch einen Isolator getrennt vom Rest, befindet sich zwischen Source und Drain das Floating-Gate (etwa: Schwebe-Tor). Dieses Bauteil ist der eigentliche Speicherort der Flash-Zelle. Über das Steuer-Gate, das mit dem Floating-Gate verbunden ist, kann eine postive oder negative Spannung angelegt werden. * Wird nun an das Steuer-Gate eine positive Spannung angelegt (etwa 3,3 Volt), entsteht ein Kanal zwischen Source und Drain, es fließt Strom. Dieser Zustand wird als 0-Zustand bezeichnet. * Jede der Zellen kann entweder im 0- oder im 1- Zustand sein. Aus sehr vielen dieser Zellen kann ein Computer dann gespeicherte Daten auslesen. * Bei einem Löschvorgang wird zwar die Verknüpfung zu einem bestimmten Speicherbereich gelöscht, jedoch kann man diese durch verschiedene Programme wiederherstellen. |