ITS – Praktikumsaufgaben WS 2014/15

Grundlegende Netzwerkanalysen mit Hilfe des Internet-Analyse-Systems

Stand: 2014/11/06 -14-

Dominique Petersen <petersen@internet-sicherheit.de>
Thomas Schyra <schyra@internet-sicherheit.de>
Peter Honerbom <honerbom@internet-sicherheit.de>
Institut für Internet-Sicherheit, https://www.internet-sicherheit.de
Westfälische Hochschule

Inhaltsverzeichnis

Rahmenbedingungen

Im Rahmen des Praktikums sollen Sie mit Hilfe des Rich Clients oder der Webversion des Eagle-X Clients den Netzwerkverkehr an mehreren Standorten analysieren.
Eventuell auftretende Limitierungen des zur Verfügung stehenden Funktionsumfanges der unterschiedlichen Client Versionen entnehmen sie bitte den weiteren Dokumenten.

Erlaubt sind der Zugriff auf die IAS-Sonde im **Fachbereich Informatik** (Sondennummern: 80000001 [Inbound FB5] , 8000002 [Outbound FB5]) sowie die Sonde bei der **Messe AG** (Sondennummer: 90000001). Alle Zugriffe Ihrer Gruppen werden protokolliert und ggfs. ausgewertet. Ein Zugriff auf andere Sonden ist nicht erlaubt und kann zu unangenehmen Konsequenzen führen (siehe gesondertem Geheimhaltungsvertrag).

Die Beobachtungen und Analysen müssen – soweit nicht anders mit der Praktikumsbetreuung abgesprochen – im Zeitraum vom **01.01.2014** bis **01.11.2014** für die beiden Sonden im Fachbereich und der Messe AG durchgeführt werden.

Fristen

Die Anmeldung zum Praktikum im Moodle muss bis zum *06.11.2014 09:50* erfolgt sein.
Nicht eingetragene Teilnehmer können aufgrund der zu erwartenden Gruppenstärke nicht berücksichtigt werden.

Die Aufgaben sind **schriftlich ausgearbeitet** bis zum *11.01.2014* im **PDF-Format per E-Mail** an Dominique Petersen (petersen@internet-sicherheit.de) abzugeben.
Der Betreff ist folgendermaßen zu wählen (**Abweichungen führen zu nicht bestehen!**):

*ITS Praktikum 2014 Ausarbeitung #<**hier Gruppennummer einfügen**>*

Eine spätere Einsendung wird nicht mehr berücksichtigt.

Formvorschriften

Ein **Deckblatt** mit den üblichen Informationen ist **Pflicht**, ansonsten gilt das Dokument als nicht eingegangen und das Praktikum als **nicht bestanden**.

Dazu gehören **mindestens**:

- Gruppennummer
- Namen

Die Screenshots und weitere Grafiken müssen in lesbarer Weise eingebunden werden. Die Beschriftungen der Grafiken sind notfalls zu ergänzen oder anzupassen. Eine strukturierte Gliederung der Aufgaben sollte selbstverständlich sein.

Kontakt

Im Normalfall wird mindestens ein Praktikumsbetreuer bei den Praktikumsterminen anwesend sein. Diesen können Sie selbstverständlich bei auftretenden Problemen ansprechen.

Nachfragen zu der technischen Vorgehensweise sind erwünscht, werden jedoch nicht beantwortet, falls dieses die Lösung einer Aufgabe vorweg nehmen würde.
Der Zweck dieses Praktikums besteht letztendlich im Erlernen der Anwendung verschiedener Analysetechniken mit Hilfe des EagleX-Client. Dies bedeutet Sie müssen in der Lage sein, selbst nach Lösungswegen zu suchen.

Nachfragen per E-Mail sind an folgende Adresse zu richten:
honerbom@internet-sicherheit.de (inhaltlich)
schyra@internet-sicherheit.de (technisch)
petersen@internet-sicherheit.de

Umfang

Zu jeder Aufgabe wird eine vollständige Antwort erwartet, keine Stichpunkte! Es sind zu jeder Behauptung aussagekräftige Screenshots beizufügen. Dies kann sinnvoll sein, auch wenn es nicht explizit in der Aufgabenstellung gefordert ist. Eigene Grafiken zur Veranschaulichung sind nicht nur erlaubt, sondern auch erwünscht! Ebenso ist es sinnvoll Zeiträume, Deskriptoren und Sonden in der Ausarbeitung anzugeben, falls diese Angaben nicht direkt ersichtlich sind.

Der erwartete Umfang der Ausarbeitung, **exklusive** der Screenshots, beträgt :

Aufgaben	Erwartete Seiten (pro Aufgabe)
1., 2., 3., 4., 5. ,6. , 7., 8., 9.	1
10.	1++
11., 12. ,13.	1
14.	1++
15.	1
16.	1++

Diese Angaben sind als Mindestanforderungen zu betrachten. Ausnahmen durch besonders scharfe und treffende Formulierungen werden im Einzelfall geprüft.

Nach Abgabe werden Sie eine schriftliche Bewertung ihrer Ausarbeitung bekommen sowie eine Rückmeldung, ob die Ausarbeitung so gut ist, um das Praktikum erfolgreich abzuschließen. Bitte stellen Sie deshalb auch sicher, das Sie eine **korrekte** E-Mail Adresse angeben, unter welcher Sie erreichbar sind.

Beachten Sie, dass die Ausarbeitung anteilig in die Bewertung und damit in die Endnote im Fach ITS einfließen kann.

Theorieaufgaben

Diese Aufgaben sollen nicht am Rechner durchgeführt werden, sondern vorab (!) theoretisch überlegt werden.

Aufgabe 1

Welches Verhältnis der Pakete mit ausschließlich gesetztem SYN Flag, ausschließlich gesetztem FIN Flag, gesetztem SYN und gesetztem ACK Flag sowie gesetztem FIN und gesetztem ACK Flag ist theoretisch immer zu erwarten? Warum?

___ % SYN ___ % SYN/ACK ___% FIN ___ % FIN/ACK

Aufgabe 2

Welches Verhältnis erwarten Sie ungefähr in der Praxis? Warum?

___ % SYN ___ % SYN/ACK ___% FIN ___ % FIN/ACK

Aufgabe 3

Wieso können Pakete mit ausschließlich gesetztem ACK Flag nicht für die Analyse des TCP-Handshake verwendet werden, obwohl der Handshake mit so einem Paket abgeschlossen wird (schlüssige Begründung)?

Praxisaufgaben

Diese Aufgaben sollen am PC mit Hilfe des EagleX oder WebEagleX durchgeführt werden. Es dürfen weitere Hilfsmittel zur Berechnung benutzt werden (z.B. Taschenrechner oder ein Tabellenkalkulationsprogramm wie OpenOffice Calc).

Aufgabe 4

Welches Verhältnis liegt **im Fachbereich** vor? Analysieren Sie die beiden Sonden des FB5 im Verbund über einen Zeitraum von mindestens ca. 4 Wochen. Belegen Sie Ihr Ergebnis mit Screenshots.

Weicht das Ergebnis von der Erwartung ab? Wenn ja, wieso?

___ % SYN ___ % SYN/ACK ___% FIN ___ % FIN/ACK

Aufgabe 5

Suchen Wie in den Daten **des Fachbereichs** nach einem SYN-Scan-Angriff. Dokumentieren Sie Ihren Fund mit Screenshots in unterschiedlichen Ansichten. Beschreiben Sie den Angriff. Nehmen Sie den Deskriptor für Pakete mit gesetztem RST-Flag in die Analyse auf und beschreiben Sie die Zusammenhänge.
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 6

Betrachten Sie das Verhältnis von HTTP zu HTTPS Verkehr.
A) Wie ist die momentane und historische Lage **im Fachbereich** und **bei der Messe AG?**
Betrachten Sie für die historische Entwicklung das letzte halbe Jahr.
B) Wie bewerten Sie die Situation?
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 7

Betrachten Sie das Verhältnis von DNS-Requests zu DNS-Responses.
A) **Im Fachbereich**
B) **Bei der Messe AG**

C) Worauf könnte eine Anomalie hierbei hinweisen?
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 8

A) Suchen Sie in den Daten **des Fachbereichs** nach einem Beispiel für einen typischen Wochenverlauf. Erkennt man das Wochenende?
B) Beschreiben Sie anhand eines Beispiels die Änderungen (im Bezug auf Protokolle).
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 9

Betrachten Sie die Verteilung der HTTP-Request-Typen **im Fachbereich.**
A) Was fällt auf?
B) Wieso ist das so?
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 10

A) Welche Anomalien können sowohl Hinweise auf Angriffe, als auch Hinweise auf Fehlkonfigurationen sein?
B) Welche davon können vom IAS erkannt werden? Auf welche kann das IAS nur Hinweise geben?
Es werden hier mindestens zwei Beispiele erwartet.
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 11

A) Wie verändert sich der Traffic **im Fachbereich** an einem Beispieltag jeweils in der Vorlesungszeit und zur vorlesungsfreien Zeit?
B) Welche Ursachen könnte es für Unterschiede geben?
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 12

Geben Sie näherungsweise das Volumen des gesamten IPv4-Verkehrs **im Fachbereich** an (in GB).
Beschreiben Sie hierbei Ihre Erhebungstechnik und begründen Sie, wieso diese sinnvoll ist.
A) Für den gesamten erlaubten Messzeitraum
B) Für den Monat [Gruppennummer]

Dokumentieren Sie Ihre Ergebnisse mit Screenshots und selbst erstellten Grafiken.

Aufgabe 13

Wie hoch ist der Anteil von DNS-Traffic am gesamten IPv4-Verkehr **im Fachbereich**?
Betrachten sie das:
A) Für den gesamten erlaubten Messzeitraum
B) Für den Monat [Gruppennummer]

Aufgabe 14

A) Suchen Sie nach den Top Anwendungen (TCP und UDP getrennt) **im Fachbereich** (bezogen auf die Anzahl der Pakete).
B) Betrachten Sie den eingehenden und ausgehenden Traffic getrennt. Gibt es Unterschiede?
Bitte nehmen Sie unbedingt **nur den Zeitraum von einem frei wählbaren Tag** im erlaubten Messbereich!
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 15

Wie hoch ist jeweils der Anteil an Unix-Systemen (Linux, MacOs, Android) im Vergleich zu Windows-basierten Systemen oder Cisco-Routern auf dem gesamten erlaubten Messzeitraum.
A) **Im Fachbereich**
B) **Bei der Messe AG**
Dokumentieren Sie Ihre Ergebnisse mit Screenshots.

Aufgabe 16

Wie weit sind externe Server im Durchschnitt **vom Fachbereich** entfernt (Hopcount)? Ermitteln Sie den Mittelwert für den Monat [Gruppennummer]
Achtung: Dies können Sie nur näherungsweise herausfinden!

TCP - Exkurs

Drei-Wege-Handshake[1]

TCP Netzwerkverbindungen werden durch den „TCP Handshake“ initiiert und durch den „TCP Teardown“ abgebaut. Diese Vorgänge werden durch die TCP Flags im TCP Header gesteuert.

Der Drei-Wege-Handshake ist die Bezeichnung für ein Verfahren, um eine verlustfreie Datenübertragung zwischen zwei Instanzen zu ermöglichen. Obwohl überwiegend in der Netzwerktechnik verwendet, ist der Drei-Wege-Handshake nicht auf diese beschränkt.

Verbindungsaufbau

Beim Aufbau einer TCP-Verbindung kommt der Drei-Wege-Handshake zum Einsatz. Der Rechner, der die Verbindung aufbauen will, sendet dem anderen ein *SYN*-Paket (von engl. *synchronize*) mit einer Sequenznummer *x*. Die Sequenznummern sind dabei für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate wichtig. Es handelt sich also um ein Paket, dessen *SYN-Bit* im Paketkopf gesetzt ist (siehe TCP-Header). Die Start-Sequenznummer ist eine beliebige Zahl, deren Generierung von der jeweiligen TCP-Implementierung abhängig ist. Sie sollte jedoch möglichst zufällig sein, um Sicherheitsrisiken zu vermeiden.

Die Gegenstelle (siehe Skizze) empfängt das Paket. Ist der Port geschlossen, antwortet sie mit einem TCP-RST um zu signalisieren, dass keine Verbindung aufgebaut werden kann. Ist der Port geöffnet, sendet sie in einem eigenen SYN/ACK-Paket im Gegenzug ihre Start-Sequenznummer *y* (die ebenfalls beliebig und unabhängig von der Start-Sequenznummer der Gegenstelle ist). Zugleich bestätigt sie den Erhalt des ersten SYN-Pakets, indem sie die Sequenznummer *x* um eins erhöht und im ACK-Teil (von engl. *acknowledgment* = *Bestätigung*) des Headers zurückschickt.

Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Pakets durch das Senden eines eigenen ACK-Pakets mit der Sequenznummer *y+1*. Dieser Vorgang wird auch als „Forward Acknowledgement“ bezeichnet. Außerdem sendet der Client den Wert *x+1* aus Sicherheitsgründen ebenso zurück. Dieses ACK-Segment erhält der Server.

1 http://de.wikipedia.org/wiki/Transmission_Control_Protocol#Der_Drei-Wege-Handschlag

Das ACK-Segment ist durch das gesetzte ACK-Flag gekennzeichnet. Die Verbindung ist damit aufgebaut.

1.	SYN-SENT	→	<SEQ=100><CTL=SYN>	→	SYN-RECEIVED
2.	SYN/ACK-RECEIVED	←	<SEQ=300><ACK=101><CTL=SYN,ACK>	←	SYN/ACK-SENT
3.	ACK-SENT	→	<SEQ=101><ACK=301><CTL=ACK>	→	ESTABLISHED

Verbindungsabbau

Der geregelte Verbindungsabbau erfolgt ähnlich. Statt des SYN-Bits kommt das FIN-Bit (von engl. *finish = Ende, Abschluss*) zum Einsatz, welches anzeigt, dass keine Daten mehr vom Sender kommen. Der Erhalt des Pakets wird wiederum mittels ACK bestätigt. Der Empfänger des FIN-Pakets sendet zuletzt seinerseits ein FIN-Paket, das ihm ebenfalls bestätigt wird.

Obwohl eigentlich vier Wege genutzt werden, handelt es sich beim Verbindungsabbau auch um einen Drei-Wege-Handshake, da die ACK- und FIN-Operationen vom Server zum Client als ein Weg gewertet werden. Zudem ist ein verkürztes Verfahren möglich, bei dem FIN und ACK genau wie beim Verbindungsaufbau im selben Paket untergebracht werden. Die *maximum segment lifetime* (MSL) ist die maximale Zeit, die ein Segment im Netzwerk verbringen kann, bevor es verworfen wird. Nach dem Senden des letzten ACKs wechselt der Client in einen zwei MSL andauernden Wartezustand (Waitstate), in dem alle verspäteten Segmente verworfen werden. Dadurch wird sichergestellt, dass keine verspäteten Segmente als Teil einer neuen Verbindung fehlinterpretiert werden. Außerdem wird eine korrekte Verbindungsterminierung sichergestellt. Geht ACK *y+1* verloren, läuft beim Server der Timer ab, und das LAST_ACK Segment wird erneut übertragen.

Control-Flags

Control-Flags sind zweiwertige Variablen mit den möglichen Zuständen *gesetzt* und *nicht gesetzt*, welche zur Kennzeichnung bestimmter für die Kommunikation und Weiterverarbeitung der Daten wichtiger Zustände benötigt werden. Im folgenden werden die Flags des TCP-Headers und die von ihrem Zustand abhängigen, auszuführenden Aktionen beschrieben.

URG

Ist das Urgent-Flag *(urgent = dringend)* gesetzt, so werden die Daten, auf die das *Urgent-*

Pointer-Feld zeigt, sofort von der Anwendung bearbeitet. Dabei unterbricht die Anwendung die Verarbeitung der Daten des aktuellen TCP-Segments und liest das Byte aus, auf das der Urgent-Pointer zeigt. Dieses Verfahren ist fern verwandt mit einem Softwareinterrupt. Dieses Flag kann zum Beispiel verwendet werden, um eine Anwendung auf dem Empfänger abzubrechen. Das Verfahren wird nur äußerst selten benutzt, Beispiele sind rlogin und telnet.

ACK

Das *Acknowledgment*-Flag hat in Verbindung mit der *Acknowledgment*-Nummer zwei unterschiedliche Aufgaben. Zum einen dient es bei gleichzeitig gesetztem SYN-Flag zur Bestätigung beim Drei-Wege-Handshake, zum anderen wird es ohne SYN-Flag zur Bestätigung von TCP-Segmenten beim Datentransfer genutzt. Die *Acknowledgment*-Nummer ist nicht gültig, wenn das Flag nicht gesetzt ist.

PSH

Das *Push*-Flag hat die Aufgabe, die Daten unter Umgehung des Puffers, eines Speichers für die Zwischenlagerung von Daten, sofort an die Anwendung weiterzuleiten. Hilfreich ist dies, wenn man zum Beispiel bei einer Telnet-Sitzung einen Befehl an den Empfänger senden will. Würde dieser Befehl erst im Puffer zwischengespeichert werden, so würde dieser (stark) verzögert abgearbeitet werden.

RST

Das *Reset*-Flag wird verwendet, wenn eine Verbindung abgebrochen werden soll. Dies geschieht zum Beispiel bei technischen Problemen oder zur Abweisung unerwünschter Verbindungen.

SYN

Pakete mit gesetztem SYN-Flag initiieren eine Verbindung, d.h. beginnen den Drei-Wege-Handshake. Der Server antwortet normalerweise entweder mit SYN+ACK, wenn er bereit ist, die Verbindung anzunehmen, andernfalls mit RST. Es dient der Synchronisation von *Sequenznummern* beim Verbindungsaufbau (daher die Bezeichnung SYN).

FIN

Dieses Finish-Flag dient zur Freigabe der Verbindung und zeigt an, dass keine Daten mehr vom Sender kommen. Die FIN- und SYN-Flags haben Sequenznummern, damit diese in der richtigen Reihenfolge abgearbeitet werden.

Verhältnis der Flag-Kombinationen

Über das Verhältnis der Anzahl der Flag-Kombinationen können Informationen über das analysierte Netzwerk erlangt werden. Relevante Flag-Kombinationen sind SYN, SYN/ACK, FIN und FIN/ACK.

Beispiel (fiktiv): In einem Zeitraum von 5 Minuten konnte beobachtet werden, dass über eine Kommunikationsleitung folgende Pakete mit oben angegebenen Flag-Kombinationen übertragen wurden:

SYN: 112 Pakete
SYN/ACK: 6 Pakete
FIN: 60 Pakete
FIN/ACK: 22 Pakete

Daher ergibt sich das folgende Verhältnis der Pakete untereinander:

SYN: 56 %
SYN/ACK: 3 %
FIN: 30 %
FIN/ACK: 11%

SYN-Scan[1]

Hacker verwenden für einen sog. SYN-Scan eine Technik, die sich der TCP-Flags bedient.

Beim TCP SYN Scan wird ein TCP-Paket mit SYN-Flag an den Ziel-Host gesendet, um einen Verbindungsversuch vorzutäuschen. Die Antwort des Hosts gibt Aufschluss über den Port: Sendet er ein SYN/ACK-Paket, den zweiten Teil des Drei-Wege-Handshakes von TCP, akzeptiert der Port Verbindungen und ist daher offen. Der Quell-Host antwortet dann in der Regel mit einem RST-Paket, um die Verbindung wieder abzubauen (dies geschieht meist allerdings nicht durch den Portscanner, sondern durch das Betriebssystem, da offiziell kein Verbindungsversuch

1 http://de.wikipedia.org/wiki/Portscanner#TCP_SYN_Scan

unternommen wurde). Sendet der Host ein RST-Paket, ist der Port geschlossen. Sendet der Ziel-Host überhaupt kein Paket, ist ein Paketfilter vorgeschaltet.

Der Vorteil dieser Methode ist, dass die gescannte Anwendung keinen Verbindungsversuch erkennt. Deshalb erscheint die Verbindung nicht in den Logdateien und kann daher auch nicht analysiert werden. Jede bessere Firewall erkennt diesen Scan allerdings. Auf den meisten Quell-Systemen sind außerdem Systemverwalterrechte notwendig, weil TCP-Pakete vom Portscanner handgefertigt werden müssen.

TCP SYN Scans lassen sich für Denial-of-Service-Attacken in Form von SYN-Flood nutzen.