DREAMING ANDY/FOTOLIA

Wireshark-Netzwerkanalyse leicht gemacht

Kostenlose Software zur Analyse des Datenverkehrs in drahtgebundenen und Funknetzwerken

Inhalt

***Wer heutzutage sein Unternehmensnetzwerk analysieren möchte**, braucht keine großen Investitionen zu tätigen. Wireshark bietet Ihnen alles, was Sie von einem Netzwerk-Paket-Analyzer erwarten, und ist dazu auch noch kostenlos.*

Lesen Sie in diesem eGuide alles über die vier Schlüsselfunktionen von Wireshark und erfahren Sie anhand von Best Practices, wie Sie den Netzwerk-Paket-Analyzer für das Netzwerk-Sniffing nutzen können. Des Weiteren wird erklärt, wie Sie Wireshark als Werkzeug für Cloud-Monitoring einsetzen und mit der Software Ihren Netzwerkverkehr richtig mitschneiden, VoIP Datenpakete abfangen oder Ihren VoIP Traffic parsen.

Der Start mit Wireshark

Wireshark ist ein mächtiger Netzwerk-Paket-Analyzer. Die Software, früher bekannt als Ethereal, kann für Administratoren bei der Analyse des Datenverkehrs in drahtgebundenen und Funknetzwerken sehr hilfreich sein. Und das Beste: Wireshark ist Open Source und daher kostenlos.

Wireshark zu installieren ist ein Kinderspiel. Binäre Versionen lassen sich für Windows 32-Bit und Windows 64-Bit sowie Mac OS X herunterladen. Für die meisten Varianten von Unix/Linux ist es über die Standardsysteme zur Softwareverteilung ebenfalls verfügbar. Und für eine Installation auf anderen Betriebssystemen ist auch der Quellcode gratis zu haben.

„Die Windows-Version von Wireshark wurde auf der Grundlage der Bibliothek WinPcap zur Paketerfassung erstellt; diese muss zur Ausführung unter Windows also vorhanden sein. Dazu eine kleine Warnung: Wenn Sie eine veraltete Version von WinPcap haben, sollten Sie sie sicherheitshalber manuell über „Programme hinzufügen/entfernen“ in der Systemsteuerung löschen, bevor Sie das Wireshark-Installationsprogramm ausführen.

Die Installation erfolgt in der vertrauten, von einem Assistenten unterstützten Reihenfolge, bei der nur zwei wichtige Fragen auftreten: ob Sie auch WinPcap installieren wollen und ob Sie das Programm mit dem Dienst WinPcap Netgroup Packet Filter (NPF) starten möchten. Bei der zweiten Option können Nutzer ohne Administratorrechte selbst die Paketerfassungen starten. Wenn der Dienst nicht gestartet wird, können nur Administratoren Wireshark ausführen.

Der komplette Wireshark User's Guide steht auf der Homepage des Programms kostenlos als PDF und im HTML-Format bereit.

Inhalt

Inhalt

Vier Schlüsselfunktionen von Wireshark im Überblick

Brad Casey

Der Grundstock guter und effizienter Netzwerk-Security ist die Paketanalyse, also die Fähigkeit, zwischen guten und bösen Paketen zu unterscheiden. Natürlich gibt es noch viele weitere komplexe Schichten, die man bei der Analyse von Paketen beachten muss. Jeder Administrator, der sich für Netzwerk-Security interessiert, sollte aber die wichtigsten Netzwerkanalyse-Tools kennen und mit diesen auch umgehen können.

Wireshark ist für diesen Zweck eines der leistungsfähigsten Paket-Capturing-Tools für das Netzwerk. Zusätzlich werfen wir einen Blick auf die Security-Probleme in Unternehmen und erläutern, mit welchen vier Wireshark-Funktionen Sie diese adressieren können.

Validierung

Dann und wann möchte der Administrator wissen, ob die Firewall des Unternehmens wirklich blockiert, was sie blockieren soll. Möglicherweise möchten Sie nur sicherstellen, dass die Konfiguration der Firewall korrekt ist. Zum Beispiel gibt es keinen plausiblen Grund, Telnet-Traffic in ein Firmennetzwerk zu lassen. Die meisten Firewalls blockieren TCP-Port 23 per Standard. Ein guter Netzwerkadministrator geht aber auf Nummer sicher: Er überprüft hin und wieder, ob das auch tatsächlich der Fall ist.

Testen wir nun die Firewall des Unternehmens im Hinblick auf den Telnet-Traffic. Dazu kann der Administrator ein Capture (Erfassung) auf einem internen Node laufen lassen, der sich hinter der Gateway-Firewall befindet. Tippen Sie Nachfolgendes in das Filter-Feld, das Sie am oberen Ende der grafischen Schnittstelle von Wireshark finden:

telnet

Im Anschluss melden Sie sich auf einem Node an, der sich außerhalb des Firewall-Perimeters befindet. Hier versuchen Sie nun mittels Telnet, auf einen Knoten innerhalb der Firewall zuzugreifen.

Inhalt

Sollte sich jetzt irgendwelcher Telnet-Traffic in der Erfassung von Wireshark zeigen, ist eine Überprüfung der Firewall-Konfiguration dringend anzuraten. Es gibt hier ganz klare Anzeichen von falscher Konfiguration. Sollten Sie nichts Ungewöhnliches an der Konfiguration finden, weist das auf ein größeres Problem hin. In diesem Fall ist eine sofortige Kontaktaufnahme zum Hersteller ratsam.

Erkenntnis und Sensibilisierung

Die meisten Unternehmensnetzwerke haben irgendwo eine Art Log- und Warn-Mechanismus implementiert, um den Überblick über das Netzwerk zu haben und sich entsprechend sensibilisieren zu lassen. Diese Mechanismen können Sie in Verbindung mit einem IDS (Intrusion Detection System) oder einem allumfassenden SIEM (Security Information and Event Management System) verwenden. Die Produkttypen sind fast komplett von exaktem Paket-Capturing abhängig. Nun könnte sich der Administrator dafür interessieren, was in bestimmten Segmenten des Netzwerks genau vor sich geht. Dafür lässt sich zum Beispiel ein Monitor-Port auf einem der Layer-2-Switches innerhalb des Netzwerks einrichten. Nehmen wir an, dass das Netzwerk ein Subnetz mit 10.0.0.1/24 hat. Dann sollten Sie folgenden Wireshark-Filter anwenden:

```
ip.addr==10.0.0.1/24
```

Alle Pakete, die in das oben spezifizierte Subnet fallen, tauchen nun in diesem Wireshark-Capture auf. Der Systemadministrator kann an dieser Stelle entsprechend Anpassungen vornehmen. Soll die Geschichte spezifischer auf ein Protokoll abgestimmt sein, können Sie diesen Filter verwenden:

```
ip.addr==10.0.0.1/24 && ssl
```

Dieser Filter ist nützlich, wenn Sie verschlüsselten Traffic innerhalb eines speziellen IP-Bereichs entdecken möchten. Manche Formen von Malware benutzen SSL als Verschlüsselungs-Mechanismus. Administratoren können so unter Umständen besser eingrenzen, welche Hosts mit SSL-aktiver Malware verseucht sind.

Inhalt

Das GUI maximal ausnutzen

Während eines Einbruchs ins Netzwerk haben kleinere und mittelgroße Firmen oftmals keine oder schlechte Visualisierungs-Möglichkeiten. Gut, es gibt die kommandozeilenbasierten Ausgaben des Open-Source-IDS Snort. Diverse Entwickler haben beherzte Versuche unternommen, ein GUI für Snort zu schaffen. Ich persönlich bevorzuge aber die Visualisierungslösung für Arme, um Snort-Captures darzustellen: Wireshark.

Um das GUI für Snort einzusetzen, müssen Systemadministratoren einfach die Snort-Daten in eine .pcap-Datei speichern. Diese lässt sich dann wiederum mit Wireshark öffnen. An dieser Stelle könnten sich die Analysen der unterschiedlichen TCP-Streams mit Wireshark zu einer fesselnden Nachmittagsbeschäftigung auswachsen. Oftmals ist eine solche Analyse von Snort-Daten aber ziemlich aufschlussreich.

Malware sichten und bekämpfen

Ist ein Netzwerk lange genug mit dem Internet verbunden, rechnet man damit, sich früher oder später eine Infektion mit Malware einzufangen. Dabei spielt es keine Rolle, wie ausgeklügelt die Security-Strategie einer Firma ist. Deswegen sollte in einem Unternehmen immer ein Malware-Experte zur Stelle sein. Dieser kann den Grad der Infektion schnell bestimmen und erste Diagnosen durchführen. So einen Luxus kann sich allerdings nicht jede Organisation leisten. Auch an dieser Stelle hilft Wireshark weiter.

Sobald ein Stück Malware oder verdächtiger Code in Ihr Netzwerk eindringt, müssen Sie eine Kopie der ausführbaren Dateien in Quarantäne schicken und vom restlichen Netzwerk fernhalten. Am besten eignet sich eine virtuelle Umgebung für diese Zwecke. Läuft das Wireshark-Capture in dieser virtuellen Umgebung, sollte der Administrator die ausführbare Datei starten. Nun kann er den kompletten Traffic beobachten, der sich auf dem Bildschirm abspielt. Sobald sich DNS-Versuche zeigen, die auf seltsame URLs verweisen, sollte der Administrator die IP-Adressen und DNS-Informationen schnell notieren. Diese gehören umgehend in die Firewall, damit sie sich blockieren lassen. Somit haben Sie einen provisorischen Fix und können tiefer greifende Analysen durchführen.

Inhalt

Fazit

Diese vier Wireshark-Funktionen sind nur die Spitze des Eisberges, wenn wir über die Möglichkeiten der Open-Source-Security-Software sprechen. Ich bin der festen Überzeugung, dass Wireshark das Schweizer Taschenmesser unter den Security-Tools ist. Es gibt so viele Anwendungsfälle, bei denen Wireshark unerlässlich ist, von der Netzwerkanalyse bis hin zur Malware-Abwehr. Wireshark gehört in die digitale Werkzeugkiste eines jeden Security-Profis.

Über den Autor: *Brad Casey hat einen Master of Science in Informationssicherung von der University of Texas in San Antonio. Er bringt umfangreiche Erfahrung in den Bereichen Penetrations-Testing, Public-Key-Infrastruktur, VoIP- und Netzwerk-Paketanalyse mit sich. Weiterhin ist er auf die Themen Systemadministration, Active Directory und Windows Server 2008 spezialisiert. Casey hat fünf Jahre für die U.S. Air Force gearbeitet und dort Security-Prüfungen und -Tests durchgeführt. In seiner Freizeit wühlt er sich durch Wireshark-Captures und spielt mit diversen Linux-Distributionen in virtuellen Maschinen.*

Best Practices für das Network-Sniffing mit Wireshark

Von Angela Orebaugh, Gilbert Ramirez und Jay Beale

Inhalt

Wireshark verfügt auch über ein Werkzeug zum Mithören in drahtlosen Netzen. Damit können Administratoren Wireless-Datenverkehr mitschneiden und analysieren und so Probleme in ihren Netzen lösen.

Probleme bei WLAN-Sniffing

Drahtloses „Sniffing“ von Netzwerkverkehr kann einige Herausforderungen mit sich bringen. Eine davon ist die Wahl eines statischen Kanals, denn drahtlose Netze können am selben Ort mit vielen verschiedenen Kanälen auf unterschiedlichen Frequenzen arbeiten. Eine weitere Herausforderung besteht darin, den richtigen Kanal für das Mitschneiden bestimmter Traffic-Arten zu finden.

Auch die Reichweite kann Probleme bereiten, denn die Entfernung zwischen der Erfassungsstation und dem anvisierten Transmitter kann erheblich sein – das ist wichtig für eine zuverlässige Erfassung. Und schließlich kann es auch zu Interferenzen und Kollisionen kommen.

Linux und Windows für WLAN-Sniffing konfigurieren

Um mit dem Sniffing mittels Wireshark beginnen zu können, müssen Sie zunächst Ihre WLAN-Hardware manuell auf den Monitormodus umstellen. Die meisten WLAN-Treiber für Linux verwenden die Schnittstelle Linux Wireless Extension, die eine konsistente Konfigurationsmöglichkeit für die Wireless-Erweiterung bietet. Anschließend können Sie die Paketerfassung starten. Auf diese Weise sammeln Sie Informationen, die Sie später mit den Wireshark-Analysemechanismen auswerten können.

Windows-Treiber für Wireless-Karten enthalten oft keinen Support für den Monitormodus. Falls vorhanden, lässt sich diese Beschränkung jedoch per Software umgehen, sodass Sie auch auf diesen Windows-Hosts WLAN-Datenverkehr mit Wireshark erfassen können.

Als kommerzielles Produkt dafür kommt AirPcap infrage. Wenn Sie darin Ihre Präferenzen für die Erfassung angegeben haben, können Sie Wireshark

starten, und eine neue Paketerfassung beginnen. Haben Sie genügend Verkehr mitgeschnitten, dann können Sie anfangen, Informationen daraus zu extrahieren.

Inhalt

Daten aus WLAN-Sniffing analysieren

Die Analysefunktionen von Wireshark sind fast immer dieselben – unabhängig davon, ob Sie eine gespeicherte Paketerfassung untersuchen oder mit einem Live-Interface auf einem Windows- oder Linux-Host arbeiten. Zu den Funktionen zählen Protocol Dissectors, starke Display-Filter, individuell einstellbare Display-Eigenschaften und die Möglichkeit, WLAN-Datenverkehr zu entschlüsseln.

Bei der Untersuchung einer großen Anzahl von Paketen können Sie auf beliebige Pakete klicken, um sich deren Inhalt anzeigen zu lassen. Ebenso können Sie vorgegebene Filter darauf anwenden und hoffen, dass sie etwas Nützliches zutage fördern. Um die Bewertung von erfassten Paketen zu erleichtern, bietet Wireshark im Fenster „Packet List“ außerdem die Möglichkeit, bestimmte Paketarten farblich zu kennzeichnen. Dies erleichtert zum Beispiel die Fehlersuche bei einem Drahtlosnetzwerk.

Ebenfalls hilfreich ist es zu wissen, ob Datenverkehr von einem drahtgebundenen oder einem drahtlosen Netzwerk stammt. Dazu können Sie in den Kennzeichnungen im Header Frame Control nach den Einträgen From DS bit und To DS bit suchen. Die Analyse von erfassten Paketen geht leichter von der Hand, wenn Sie störenden Datenverkehr und wiederholte Übertragungsversuche markieren und weitere Informationsspalten hinzufügen.

Diese Schritte sind nur die Grundlagen für die Analyse drahtloser Netze mit Wireshark. Mehr über die Erfassung von Wireless-Verkehr unter Realbedingungen, den Ausfall von Drahtlosverbindungen, Probing von Drahtlosnetzen, Konten-Sharing bei EAP-Authentifizierung, DoS-Attacken, Spoofing-Angriffe und fehlerhafte Verkehrsanalysen erfahren Sie, wenn Sie das gesamte Kapitel (in englischer Sprache) über Drahtlos-Sniffing mit Wireshark lesen.

Das Kapitel „Wireless Sniffing with Wireshark“ *aus dem von Angela Orebaugh, Gilbert Ramirez und Jay Beale geschriebenen Buch* Wireshark & Ethereal Network Protocol Analyzer Toolkit *erklärt, wie sich drahtloser Datenverkehr mithilfe der Wireshark-Software analysieren lässt. Es nennt die Herausforderungen beim Namen und beschreibt, wie sich Linux und Windows für drahtloses Mitschneiden und Analysen konfigurieren lassen.*

Inhalt

Inhalt

Netzwerkverkehr richtig mitschneiden

Von Mike Chapple

In diesem Kapitel erklärt Mike Chapple, wie Sie Netzwerk-Traffic richtig mitschneiden und so herausfinden können, ob das Netzwerk in Ihrem Unternehmen Sicherheitslücken aufweist.

Wireshark kann in Netzwerke hineinblicken und Details des Datenverkehrs auf unterschiedlichen Ebenen erfassen – von Informationen über die Verbindungsebene bis zu den Bits eines einzelnen Pakets. Diese Flexibilität und Detailliertheit machen es möglich, mit Wireshark Sicherheitsereignisse zu analysieren und Probleme mit der Netzwerksicherheit von Geräten anzugehen. Und auch der Preis ist attraktiv: Wireshark ist kostenlos!

Wie und warum man Netzwerkverkehr mitschneiden soll

Der Ausdruck „Netzwerkverkehr mitschneiden“ klingt zunächst nach Orwell'schen Visionen und einem Netzwerkadministrator als Big Brother, der die privaten E-Mails von Beschäftigten liest. Vor jedem Einsatz von Wireshark sollten Organisationen deshalb dafür sorgen, dass es eine klar definierte Datenschutzrichtlinie gibt. Diese sollte die individuellen Rechte bei der Netzwerknutzung enthalten, eine Erlaubnis für das Mitschneiden von Datenverkehr für Zwecke von Sicherheit und Problembehandlung vorsehen und die Anforderungen im Zusammenhang mit der Erfassung, Analyse und Aufbewahrung von Verkehrsdaten nennen. Wer Werkzeuge wie Wireshark ohne die nötigen Genehmigungen einsetzt, kann rechtlich schnell in gefährliches Terrain geraten.

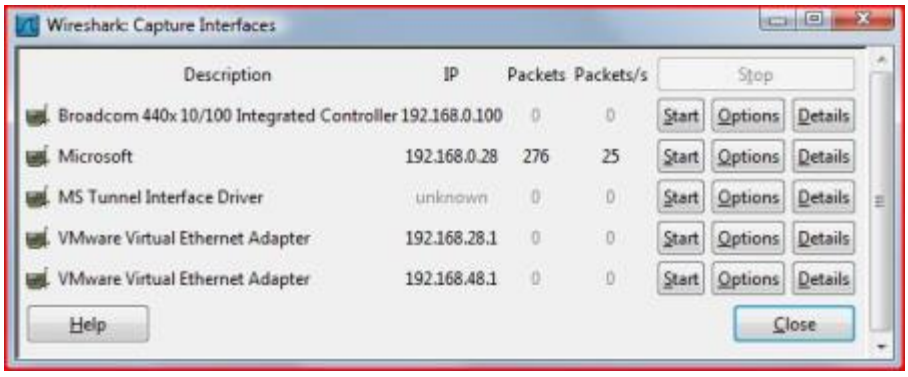
Dennoch: Für Sicherheitsprofis gibt es zwei wichtige Gründe, Netzwerkverkehr mitzuschneiden. Erstens kann es von unschätzbarem Wert sein, sich die Details von Paketen anzusehen, wenn es um die Analyse eines Angriffs auf das Netzwerk geht. So lässt sich mit Wireshark bei einem Denial-of-Service-Angriff die genaue Art des Angriffs identifizieren; zudem kann man Upstream-Regeln für die Firewall festlegen, die unerwünschten Traffic blockieren. Der zweite Hauptzweck von Wireshark liegt in der Problembehandlung bei Sicherheitsausrüstung. Ich selbst nutze es zum Beispiel für die Pflege von Firewall-Regeln. Wenn auf beiden Seiten der

Firewall Systeme mit Wireshark laufen, lässt sich leicht erkennen, welche Pakete die Firewall überwinden und ob dies die Ursache für Verbindungsprobleme ist.

Man sollte also stets daran denken, dass Wireshark für gute wie für böse Zwecke eingesetzt werden kann – so wie viele andere Werkzeuge für Sicherheitsanalysen auch. In den Händen eines Netzwerk- oder Sicherheitsadministrators ist es ein wertvolles Hilfsmittel. In den Händen von Personen mit zweifelhafter Moral aber ist Wireshark ein mächtiges Abhörwerkzeug, mit dem sich jedes Paket ansehen lässt, das ein Netzwerk durchquert.

Durchführung einer einfachen Paketerfassung

Wenn Wireshark installiert ist und Sie es starten, sehen Sie einen fast leeren Bildschirm. Um das Scannen zu beginnen, wählen Sie aus dem Capture-Menü den Punkt Interfaces. Es erscheint ein Pop-up-Fenster ähnlich wie dieses:

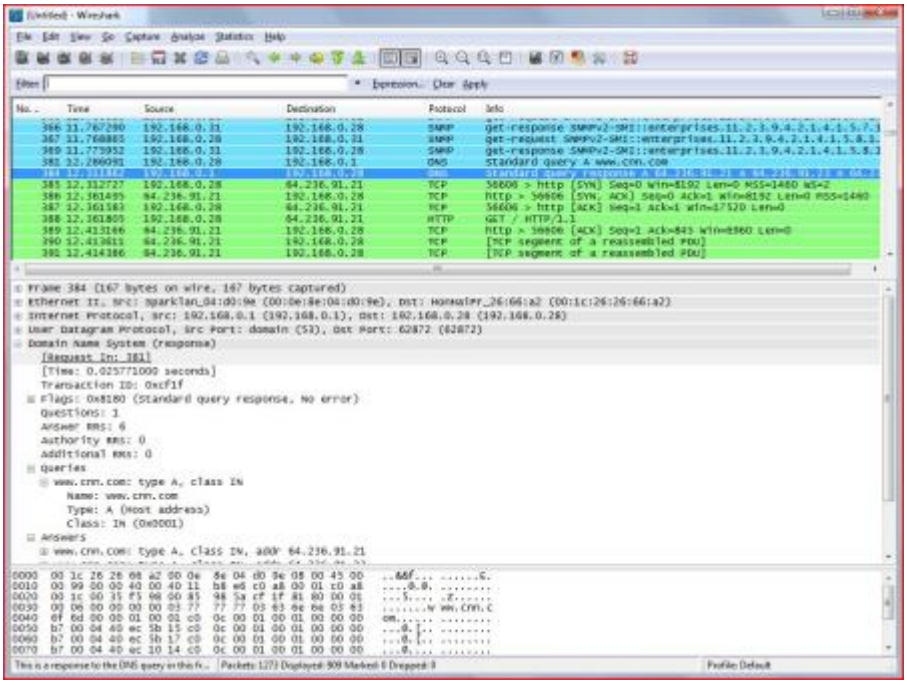


Wenn Sie erweiterte Optionen etwa zum Erfassen einer Datei, für die Auflösung von MAC-Adressen oder zu Grenzen für Zeitdauer oder Umfang einer Erfassung konfigurieren wollen, klicken Sie auf den Optionsknopf beim jeweiligen Interface. Viele der Optionen können dabei helfen, die Performance von Wireshark zu verbessern. So lassen sich damit Probleme bei der Auflösung von Namen verhindern, die ansonsten das Erfassungssystem verlangsamen und viele Namenabfragen generieren. Mit Limits für Zeit und Umfang der Erfassung lassen sich außerdem Grenzen für

Inhalt

Inhalt

unbeaufsichtigte Erfassungen vorgeben. Ansonsten können Sie einfach auf den Startknopf neben dem Namen eines Interface klicken, um mit der Erfassung seines Datenverkehrs zu beginnen. Sofort wird sich der Wireshark-Bildschirm zu füllen beginnen und in etwa so aussehen:



Ergebnisse mit den Farb-Codes von Wireshark interpretieren

Jede Zeile im oberen Bereich von Wireshark entspricht einem einzelnen Paket, das im Netzwerk erfasst wurde. Standardmäßig werden die Zeit (relativ zum Start der Erfassung), die IP-Adresse für Quelle und Ziel, das verwendete Protokoll und einige Informationen über das Paket angezeigt. Wenn Sie auf eine Zeile klicken, bekommen Sie in den unteren beiden Bildschirmbereichen detaillierte Informationen dazu angezeigt.

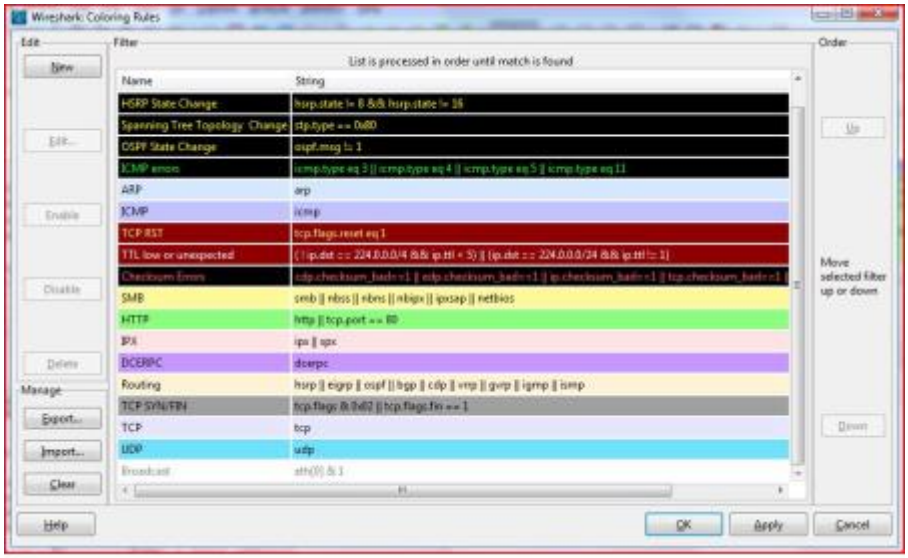
Der mittlere Bildschirmbereich enthält die Details zu oben ausgewählten Paketen. Die „+“-Symbole zeigen an, wenn weitere Details zu einem Paket zur Verfügung stehen. Im Beispiel habe ich ein DNS-Response-Paket ausgewählt und den Bereich DNS Response (Anwendungsebene) des

Inhalt

Pakets erweitert. So lässt sich sehen, dass es eine DNS-Auflösung für cnn.com angefordert hatte; die Antwort verrät uns, dass zu den dafür verfügbaren IP-Adressen 64.236.91.21 gehört. Im unteren Fenster werden die Inhalte des Pakets in hexadezimaler wie ASCII-Form angezeigt.

Die Farbkodierungen von Wireshark

Bei der Analyse von Paketen mit Wireshark erhalten Sie Unterstützung durch die Farben der einzelnen Zeilen. Die dunkelblauen Zeilen im Beispiel oben entsprechen dem DNS-Datenverkehr, die hellblauen dem UDP-SNMP-Traffic und die grünen dem HTTP-Verkehr. Wireshark ermöglicht komplexe Farbkodierungen, die Sie selbst einstellen können. Vorgegeben sind sie in dieser Form:



Dies zeigt zusammenfassend sehr gut, wie Wireshark Netzwerkverkehr mitschneidet und analysiert. Am schnellsten werden Sie hier zum Experten, wenn Sie sich die Hände schmutzig machen und einfach mit der Netzwerkerfassung beginnen. Ohne Zweifel werden Sie Wireshark dann als nützliches Werkzeug kennenlernen – ob es nun darum geht, Firewalls zu konfigurieren, oder darum, Eindringlinge zu entdecken. Denken Sie aber immer daran: Vor jeder Erfassung von Paketen brauchen Sie eine Genehmigung des Netzwerkeigentümers.

Über den Autor: *Mike Chapple, CISA, CISSP ist Experte für IT-Sicherheit an der University of Notre Dame und hat früher als IT-Sicherheitsforscher für die National Security Agency und die U.S. Air Force gearbeitet. Er ist regelmäßiger Autor für SearchSecurity, technischer Redakteur beim Magazin Information Security und Autor mehrerer Publikationen über Informationssicherheit, darunter der CISSP Prep Guide und Information Security Illuminated.*

Inhalt

Inhalt

Wireshark als Werkzeug für Cloud-Monitoring

Herkömmliche Werkzeuge für die Netzwerküberwachung bekommen neue Betätigungsfelder: Durch die zusätzliche Nutzung von privaten, hybriden und öffentlichen Clouds werden die Netze von Unternehmen komplexer – und Werkzeuge für Netzwerküberwachung und -problemlösung berücksichtigen zunehmend auch diese Umgebungen.

Denn nur weil eine Cloud-Umgebung für IT-Administratoren und Netzwerktechniker nicht direkt zu sehen ist, heißt das nicht, dass sie sich darum nicht kümmern müssten. Für Netzwerküberwachung und -problemlösung setzen sie deshalb Werkzeuge ein, die sich bei ihnen bewährt haben, zum Beispiel auch Wireshark.

„Das Analyse-Tool für Netzwerkprotokolle ist ein Open-Source-Produkt und wurde traditionell meistens für Paketanalysen hinter der Firewall verwendet. Jetzt wird es auch zu einer Option für Cloud-Problembehandlung in Unternehmen“, sagt Jonah Kowall, Research-Leiter für IT Operations Management bei Gartner.

Ähnlich sieht das John Pironti, Präsident der Beratungsfirma IP Architects: Wireshark habe zwar nicht den gesamten Funktionsumfang anderer Analysewerkzeuge, könne Sicherheits- und Netzwerkadministratoren aber durchaus dabei helfen, Datenverkehr über jegliche Netze zu optimieren, sagt er.

Brauchen Unternehmen Werkzeuge für Cloud-Monitoring?
Ob sich Wireshark wirklich für Cloud-Umgebungen eignet, hängt zu großen Teilen davon ab, wie gut es sich mit anderen Werkzeugen für Cloud-Monitoring integrieren lässt.

Cloud-Umgebungen sind üblicherweise deutlich größer als die üblichen Unternehmensnetze. Wireshark lasse sich deshalb als Teil der Due Diligence für Netzwerküberwachung nutzen, nicht aber als einziges Werkzeug zur Traffic-Erfassung, sagt Pironti: „Wireshark ist ein tolles Techniker-Tool für die

Analyse von Umgebungen und sehr speziellen Netzwerkthemen, aber für eine große Umgebung wie die Cloud reicht es nicht aus."

Inhalt

Zusammen mit Wireshark können Unternehmen für abstraktere Paketerfassung und Verhaltensanalysen Monitoring-Tools wie NetScout oder NetWitness einsetzen. Diese werden laut Pironti bereits vielfach für Sondierungen in Cloud-Umgebungen eingesetzt, wo sie fortschrittliche Monitoring-Möglichkeiten bieten, die Wireshark allein nicht bieten kann. „Das Werkzeug lässt sich ohne Frage in jedem Unternehmen mit Netzwerkinfrastruktur verwenden, aber es bleibt noch die Frage der Skalierbarkeit", so Pironti.

Einblicke ins Netzwerk sind bei hybriden oder öffentlichen Clouds nur begrenzt möglich – IT-Administratoren auf Kundenseite können nicht das gesamte Netzwerk ihres Anbieters analysieren. Trotzdem muss sich das interne Team für Monitoring und Problembehandlung nicht vollkommen auf seine Cloud-Provider verlassen: „Die IT-Abteilung sollte zumindest in der Lage sein, Netzwerkprobleme für ihre Nutzer zu analysieren und zu lösen", sagt Joe McEachern, Gründer und CEO von QA Café, einem Anbieter von IP-Testlösungen.

QA Café ist selbst ein langjähriger Nutzer von Wireshark und hat das Produkt CloudShark entwickelt. Dabei handelt es sich um eine Monitoring-Anwendung für die Erstellung, Weitergabe und Analyse von Netzwerkinformationen. „Manche Unternehmen glauben vielleicht, dass sie Tools wie Wireshark in einer Cloud-Umgebung nicht mehr brauchen, aber das stimmt nicht. Die IT-Abteilung wird sich immer noch Pakete anschauen wollen, und sei es nur die zwischen dem Unternehmen und dem Provider", so McEachern.

Weil Wireshark ein traditionelles Desktop-Tool ist, hat QA Café CloudShark so ausgelegt, dass Capture-Dateien über eine Web-Oberfläche von jedem Gerät aus zugänglich sind. „Es ist eine Brücke zwischen Desktop- und Web-basierten Anwendungen", sagt McEachern. Nach seinen Worten müsste jeder Netzwerkadministrator, der mit Wireshark zurechtkommt, auch CloudShark in einer Web-Umgebung gut bedienen können.

Entwickelt sich Wireshark zum Monitoring-Tool für die Cloud?
„Für Problembehandlungen aller Art in Zusammenhang mit einem Netzwerk kann die IT definitiv traditionelle Werkzeuge nutzen, um Netzwerk-Traffic vom Server zu erfassen“, sagt Gartner-Analyst Kowall. Mit Wireshark sei dies auf Paketebene gut möglich. Zudem habe die Software besondere Stärken beim Hineinwühlen in die Innereien von Netzwerken. „Es wird vielleicht nicht zu einem echten Cloud-Diagnosewerkzeug, aber es lässt sich in der Cloud genauso nutzen wie im Rechenzentrum oder in einem Heimnetz.“

Ähnlich äußert sich Pironti: Die Cloud sei letztlich ein Netzwerk wie jedes andere. Wireshark sei hier zwar nicht unbedingt dafür geeignet, Probleme zu verhindern oder schnell zu beheben – „aber es ist eine gute letzte Möglichkeit für das Netzwerkteam.“

Inhalt

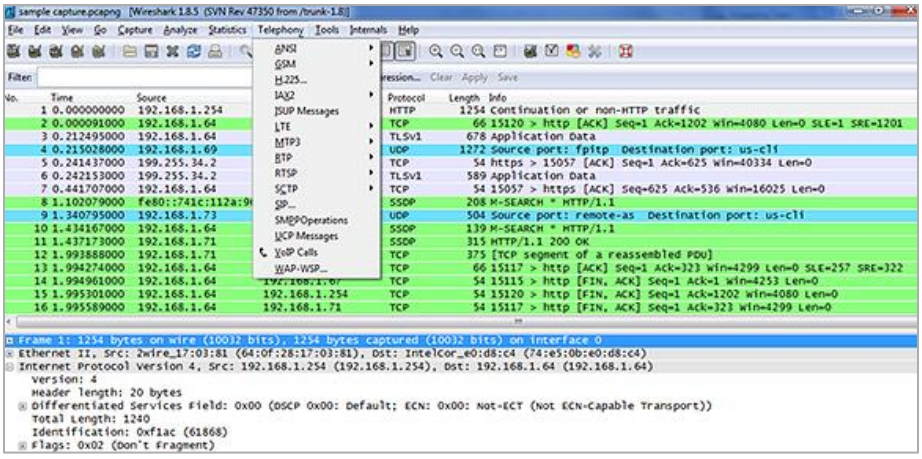
Inhalt

Wie Sie mit Wireshark VoIP-Datenpakete abfangen

Unified Communication (UC) verwischt die Grenze zwischen Sprach- und Datenkommunikation. Es ist noch nicht lange her, da waren SS7- (Signaling System 7) und IP-Kommunikation komplett eigene Bereiche. Beide wurden gleich behandelt und gleichermaßen genutzt. Derzeit gibt es einen Trend, Sprach- und Datenkommunikation über dieselbe Netzwerkinfrastruktur laufen zu lassen. Durch diese Entwicklung wird es immer wichtiger, dass man genau versteht, was durch das Netzwerk fließt. Ein effizientes Tool für das Abfangen und Analysieren von Datenpaketen ist auch hier Wireshark.

VoIP-Sniffing mit Wireshark

Ein großer Vorteil von Voice over IP (VoIP) ist, dass Netzwerkadministratoren diesen Traffic relativ einfach mit Wireshark sniffen können. In neueren Versionen von Wireshark gibt es einen kompletten Softwarebereich, der ausschließlich für die Analyse von VoIP-Traffic entwickelt wurden. Sie können VoIP-Pakete abfangen (Packet Capture), indem Sie das „Telephony“-Menü auf der Wireshark-Capture-Page nutzen.



Eine effektive Möglichkeit für das Traffic-Capturing in einem Netzwerk ist, Wireshark auf dem VoIP-Server zu installieren. Verwenden Sie einen Server mit Asterisk Session Initiation Protocol (SIP), dann möchten Sie vielleicht auch einen GNOME- oder KDE-Desktop installieren, um die Nutzung zu

Inhalt

vereinfachen. Alternativ gibt es schlankere Desktop-Umgebungen, wie LXDE oder IceWM. Linux-Puristen sehen eine grafische Oberfläche (GUI) auf einem Server womöglich nicht gerne und bevorzugen die Kommandozeileneingabe von Wireshark: TShark. Allerdings bietet TShark nicht die reichhaltige Auswahl von Grafiken und anderen Analyse-Tools, die Sie vielleicht erwarten würden. Das Capturing lässt sich auch mit TShark ausführen, wobei man das Ergebnis auf einen anderen Rechner überträgt. Dort können die Daten anschließend mit Wireshark analysiert werden.

Nachdem Sie Wireshark auf dem VoIP-Server installiert haben, öffnen Sie die Software und wählen die Schnittstelle, auf der das Capture erscheint. Klicken Sie auf den Start-Button. Nun sollten die abgefangenen Pakete über den Bildschirm laufen.

Stellen Sie sicher, dass mindestens zwei Endgeräte am SIP-Server registriert sind, und rufen Sie von einem Gerät das andere an. SIP-fähige Endgeräte können VoIP-Telefone, Videokonferenzgeräte und Softphones sein, die auf einer Workstation installiert sind.

Nachdem Sie genügend Pakete abgefangen haben, um damit eine ausreichend große Beispieldatei zu erzeugen, beenden Sie den Anruf. Stoppen Sie gleichzeitig das Capturing. „Ausreichend groß“ ist in diesem Fall natürlich subjektiv, und das Volumen wird sicher von Netzwerk zu Netzwerk variieren. Sind allerdings nur zwei Telefone und ein Server involviert, können Sie das Capturing nach geschätzten zehn bis 15 Sekunden beenden. Damit sollten Sie mindestens 4000 bis 5000 Pakete zur Verfügung haben.

Sobald das Capturing mit Wireshark erfolgreich abgeschlossen ist, wollen Sie natürlich überprüfen, ob Sie die Daten korrekt analysieren können. Im nächsten Kapitel zeigen wir, wie Sie Wireshark Packet Captures richtig filtern und ein genaues Bild Ihres VoIP-Traffics erhalten.

Inhalt

Wireshark Packet Capture filtern: So parsen Sie Ihren VoIP-Traffic

Sie wissen nun, warum wir Wireshark für das Capturing von VoIP-Paketen verwenden. Im Folgenden erkläre ich Ihnen, wie Sie dieses Wireshark Packet Capture so filtern, dass Sie nur noch den von VoIP (Voice over Internet Protocol) verursachten Traffic sehen.

Das Wireshark Packet Capture nach VoIP-Filtern

Nachdem Sie das Sammeln der Daten mit Wireshark abgeschlossen haben, müssen Sie den Traffic nach den Paketen aus dem getätigten VoIP-Anruf filtern. Nur so sehen Sie, was genau abgelaufen ist. Ein gutes Verständnis in Sachen Boolescher Logik ist an dieser Stelle sehr hilfreich.

Für unser Beispiel definieren wir, dass der IP-Adressbereich unseres Netzwerks 192.168.1.0/24 ist. Weiterhin nehmen wir an, dass die beiden Endgeräte, die den VoIP-Traffic generiert haben, die IP-Adressen 192.168.1.10 und 192.168.1.11 haben. Der anfängliche Filter für das Packet Capture könnte dann so aussehen:

```
ip.addr==192.168.1.10 || ip.addr==192.168.1.11
```

Die doppelte Pipe (||) zwischen den beiden IP-Adressen steht für ein logisches OR (oder). Der gesamte Ausdruck erzeugt einen Filter, der alle Pakete des einen oder des anderen Endgeräts mit den oben beschriebenen IP-Adressen ausgibt.
Bei der Analyse dieses Traffics fällt Ihnen sicherlich schnell auf, dass Wireshark auch Datenpakete anzeigt, die VoIP nicht verursacht hat. Dieser Umstand ist einfach zu erklären: Nicht-VoIP-Traffic wie Datenpakete von ARP (Address Resolution Protocol) und Domain Name System (DNS) wird durch das User Datagram Protocol (UDP) dauernd zwischen den beiden Endgeräten kommuniziert. Um das Ergebnis ein wenig klarer zu machen, müssen wir den Filter weiter anpassen. Der Ausdruck sieht dann wie folgt aus:

```
(ip.addr==192.168.1.10 || ip.addr==192.168.1.11) && !arp
```
&& !dns

Inhalt

Nun haben wir den Ausgabebereich der Paketerfassung im Vergleich zum Anfang drastisch eingeschränkt. Die meisten nun angezeigten Pakete sollten den Typen Session Initiation Protocol (SIP) und Real-Time Transport Protocol (RTP) entsprechen. Eventuell möchte der Netzwerkadministrator noch weitere Filter verwenden. Diese variieren aber mit Sicherheit von Netzwerk zu Netzwerk.

Weiteres zu Packet-Capture-Filtern bei Wireshark

An dieser Stelle lassen sich die Pakete des VoIP-Traffics mit Wireshark analysieren. Von jedem einzelnen Paket können Sie sich die Header-Werte und andere Informationen ansehen. Sie fragen sich aber möglicherweise, warum wir nicht von Beginn an nur nach RTP und SIP gefiltert haben. Das könnten Sie natürlich machen, wir empfehlen es aber nicht. Denn damit entgehen Ihnen womöglich TCP- und UDP-Pakete, die ebenfalls für eine Analyse des Traffics hilfreich sind und für das Gesamtbild dienliche Informationen liefern. Zum Beispiel erhält der Asterisk-Server in diversen Netzwerkkonfigurationen aus Gründen des Managements Anfragen von anderen Nodes. Wird ein Audit durchgeführt, führt ein strenger Filter mit nur RTP und SIP möglicherweise zu falschen Ergebnissen. Sollten Sie einen Einbruch ins Netzwerk vermuten, finden Sie den schädlichen Code mit einem Filter nur nach RTP und SIP sehr wahrscheinlich nicht. Weiterhin haben wir in unserem Beispiel lediglich zwei Endgeräte verwendet. In einer Enterprise-Umgebung können aber Hunderte von VoIP-Anrufen simultan ablaufen. Unter Umständen ist in einem solchen Fall ein einfacher SIP- oder RTP-Filter nutzlos.

Während der Traffic-Analyse von VoIP finden Netzwerkadministratoren möglicherweise diverse Nuancen, die zunächst verwirrend sein können. Wenn Sie diese Irritationen schnell hinter sich lassen möchten, müssen Sie solides Wissen über die Netzwerkarchitektur und fundierte Kenntnisse über Wireshark-Filter mitbringen. Außerdem sind Ausdauer und Geduld gefragt, um VoIP-Traffic richtig und sorgfältig zu analysieren.

Inhalt

Kostenlose Onlineressourcen für IT-Experten

TechTarget publiziert qualifizierte Medieninhalte im IT-Bereich, die Ihren Informationsbedarf bei der Suche nach neuen IT-Produkten und Technologien decken und Ihr Unternehmen somit gezielt in der Strategieentwicklung unterstützen. Es ist unser Ziel, Ihnen durch die Bereitstellung von Onlineressourcen zu den aktuellsten Themen der IT-Branche die Kaufentscheidungen für IT-Produkte zu erleichtern und kostengünstiger zu gestalten.

Unser Netzwerk an technologiespezifischen Webseiten erlaubt es Ihnen, auf eine der weltweit größten Onlinebibliotheken zum Thema IT zuzugreifen und anhand von unabhängigen Expertenmeinungen und Analysen, zahlreichen Whitepapern, Webcasts, Podcasts, Videos, virtuellen Messen und Forschungsberichten zu ausgewogeneren Kaufentscheidungen zu gelangen.

Unsere Onlineressourcen berufen sich auf die umfangreichen Forschungs- und Entwicklungskompetenzen führender Technologieanbieter und ermöglichen es Ihnen somit, Ihr Unternehmen für künftige Marktentwicklungen und –herausforderungen zu rüsten. Unsere Live-Informationsveranstaltungen und virtuellen Seminare geben Ihnen die Möglichkeit, Ihre täglichen individuellen Herausforderungen im Bereich IT mit herstellerunabhängigen Experten zu diskutieren.

Des Weiteren können Sie in unserem Social Network, dem IT Knowledge Exchange, praxisnahe Erfahrungsberichte mit Fachkollegen und Experten in Echtzeit austauschen.

Inhalt

Was macht TechTarget so einzigartig?

Bei TechTarget steht die Unternehmens-IT im Mittelpunkt. Unser Redaktions- und Autorenteam und unser breites Netzwerk an Industrieexperten bietet Ihnen Zugriff auf die neuesten Entwicklungen und relevantesten Themen der Branche.
TechTarget liefert klare und überzeugende Inhalte und umsetzbare Informationen für die Profis und Entscheidungsträger der IT-Branche. Wir nutzen die Schnelligkeit und Unmittelbarkeit des Internets um Ihnen in realen und virtuellen Kommunikationsräumen hervorragende Networking-Möglichkeiten mit Fachkollegen zur Verfügung zu stellen.

Weitere deutsche TechTarget Webseiten:

- SearchDataCenter.de
- SearchEnterpriseSoftware.de
- SearchNetworking.de
- SearchSecurity.de
- SearchStorage.de