Sniffer:

Kleine nützliche Viecher

Geschichte des Sniffers:

Der Sniffer steht für ein Produkt der LAN-Analyse. Eines der ersten dieser Produkte stammte von einem Hersteller namens „Network General“, mit dem Namen „Sniffer“. Deshalb ist der Begriff „Sniffer“ auch ein eingetragenes Warenzeichen dieses besagten Herstellers. Populär wurde der Begriff, zu einem weil er so Eingängig war und zum anderen war der Sniffer das erste Produkt dieser Art auf dem Markt. Hinzu kommt wahrscheinlich, dass Network General Corporation zu dieser Zeit auf dem Markt vorherrschend war. Zur heutigen Zeit werde fast alle Produkte die zur LAN-Analyse dienen, unter den Begriff Sniffer gehandelt.

Auch wenn die Entwicklung des ersten Sniffers schon lange zurückliegt, ist die Firma Network General Corporation immer noch aktuell den je. So setzt sich ihre aktuelle Produktpalette aus folgenden Produkten zusammen:

- Sniffer Enterprise Platform
- Sniffer Enterprise Intelligence
- Sniffer Enterprise Management

Weiter bietet das Unternehmen Lehrgänge über Sniffer, und besitzt sogar eine eigene „Sniffer Universität“, in der man ein anerkanntes Zertifikat erwerben kann.

Historische Sniffer-Attacken:
Sniffer sind nichts ungewöhnliches, warum auch? Administratoren benutzen Sniffer schon lange, um Netzprobleme schnell und sicher lokalisieren zu können. Dennoch werden Sniffer auch gerne von Angreifern verwendet. In der Geschichte der Netzwerksicherheit, gab es ein paar interessante **Sniffer-Attacken**.
So zum Beispiel die Attacke im Jahre 1994, bei der das amerikanische Marineforschungsinstitut, Ziel einer massiven Sniffer-Attacke war. Dabei wurden über 100.000 Benutzernamen und Kennwörter ausspioniert. Dieser Angriff über das Netzwerk des Militärs war schwerwiegend.

Zu diesem Angriff äußerte sich ein Mitarbeiter der Abteilung für Computersicherheit. Die ganze Aussage können Sie unter: http://www.swiss.ai.mit.edu/6.805/articles/mcnulty-internet-security.txt lesen.

Ein weiterer bekannter Sniffer-Angriff, war der unter dem Namen: **Solar Sunrise** bekannte Angriff von zwei kalifornischen Jungendliche und ihrem Mentor aus Israel, auf das amerikanische Verteidigungsministerium. Dieser Solar Sunrise, fand im Februar 1998 statt.

Weitere Informationen finden Sie unter: http://www.sans.org/resources/idfaq/solar_sunrise.php

Bestandteile eines Sniffers:

Sniffer bestehen grundsätzlich aus folgenden „Komponenten“:

- Capture Driver
- Buffer
- Filter

Funktionsweise eines Sniffers:

Wie wir bereits gelernt haben besteht ein Sniffer aus folgenden drei Bestandteilen:

- Capture Driver
- Buffer
- Filter

Um nun an die Datenpaketen zu gelangen, klingt sich der Sniffer mit seinem **Capture Driver** in den Treiber der Netzwerkkarte ein. So gelangt er an die Daten, die die Netzwerkkarte erreichen. Von dort an geht es sofort in den **Buffer**. Buffer bedeutet auf Deutsch **Zwischenspeicher**. Im Buffer werden alle Daten so lange gespeichert, bis es zur Analyse kommt. Bei der Analyse, werden unwichtige Datenpakete per **Filter** ausgeblendet. Weiter kann man mit einem **Filter** auch nur ganz bestimmte Datenpakete in den **Buffer** „rein lassen“.

Sammelmodi eines Sniffers:

Sniffer sind sehr schwer in einem Netzwerk aufzuspüren. Das verdanken sie ihrer Eigenschaft, des passiven Mithörens. Sniffer gelangen in zwei verschiedenen Modi an die Daten. Das wäre zum einem der non-promiscuous mode und den Promiscuous Mode.

Non-Promiscuous-Modus:
Dieser Modus ist sehr einfach. Beim Non-Promiscuous-Modus werden einfach alle ankommende und abgehende Daten des eigenen Computers gesnifft. Für Angreifer ist dieser Modus, sofern sie nicht schon intern im Netz sind, denkbar ungeeignet. Anwendung findet der Modus, wenn ein bekannter PC Probleme aufweist.

Promiscuous-Modus:
Der Promiscuous-Modus, im Englischen auch Promiscuous Mode genannt, ist ein Empfangsmodus, in dem Geräte in einem Netzwerk den gesamten Datenverkehr abfangen. Befindet sich ein Gerät nicht im Promiscuous-Modus, was normal bei Ethernetgeräte der Fall ist, so nimmt es nur die Pakete an, die auch an das Gerät gerichtet sind. Ähnliches findet man in einem Netz mit einem Hub, das die Datenpakete an alle Stationen weiterleitet.

Der Promiscuous-Modus ist aber nur dann wirklich nützlich, wenn auch tatsächlich die Pakete bis zur Schnittstelle gelangen. So können Geräte die im Promiscuous-Modus arbeiten, bei einem Netz mit Switches, ohne Aufwand, nur die Datenpakete von den Geräte in diesem Segment abfangen.

Sniffer entdecken:

Es ist ein Alptraum jeden Administrators: Ein Sniffer wurde nicht bemerkt, hunderte von Benutzernamen samt Passwörter wurden gestohlen. Doch wie entdeckt man Sniffer rechtzeitig? Sniffer machen es einem schwer sie zu entdecken, aus folgenden Gründen:

- Sie arbeiten passiv (sie hören „nur“ zu)
- Sie hinterlassen kaum Spuren
- Sie verbrauchen kaum Netzwerkressourcen

Promiscuous-Modus aktiv?
Dennoch haben Administratoren, ein paar Ansätze um einen Sniffer im Netzwerk aufzuspüren. So bringen beispielsweise, manche Betriebssysteme einen Mechanismus mit sich, der feststellt, ob eine Netzwerkkarte in den Promiscuous-Modus versetzt wurde. Ist dies der Fall, sollten bei einem

Administrator alle Alarmglocken läuten.

Doch auch wenn dieser Mechanismus fehlt, kann herausgefunden werden, ob der Promiscuous-Modus aktiv ist. Dies ermöglicht eine Messung der Latenzzeit, des betroffenen PCs. Da ein Computer im Promiscuous-Modus alle Pakete annimmt und verarbeitet, erhöht sich dadurch auch die Latenzzeit. Ist diese bei Messungen ungewöhnlich hoch, kann man auf einen aktiven Promiscuous-Modus schließen. Da diese Messungen aber im Mikrosekunden-Bereich liegen und es aufwändig ist, jeden PC mit dieser Methode nach einem Sniffer abzusuchen, ist es fraglich ob man so eine Bedrohung durch einen Sniffer ausschließen kann.

Sniffen nach dem Sniffer:
Befindet sich der Angreifer, bzw. der Lauscher außerhalb des Netzwerkes, gelangt er nicht ohne weiteres an die Daten, die der Sniffer gesammelt hat. Sie müssen ihm erst zugesandt werden. Und hier ist der Knackpunkt. Der Sniffer, der nur passiv war, muss aktiv werden. Diese Aktivität, die durch das vermitteln der Daten auftritt, kann wiederum mit einem Sniffer festgestellt werden. Hier zeigen sich beide Gesichter des Sniffers.

Weiter kann man einen Sniffer über einen Sniffer, durch einer Häufung von DNS-Traffic ausfindig machen.

Tools entdecken Sniffer:
Um das Leben eines Administrators ein wenig zu erleichtern, kamen einige Tools zum lokalisieren von Sniffern auf den Markt. Vorhanden müssen spezielle Betriebssysteme und Netzwerkarchitekturen sein, damit das Tool ordentlich funktioniert. Zu diesen Tools, gehören unter anderem:

- Sentinel – unter Linux und BSD-basierten Unix-Systemen
- PromiScan – unter Windows 200/XP
- Nitwit
- Snifftest – unter Solaris und SunOS
- PromiscDetect – unter Windows NT/2000/XP
- Sniffdet – unter Linux

Und viele mehr…

Schutzmaßnahmen vor Sniffer:

Da Sniffer schwer wegen ihrer Passivität zu finden sind, darf man sich nie in Sicherheit wiegen. Sie verbrauchen meistens wenig Systemressourcen und hinterlassen so gut wie keine Spuren. Man sollte sich schon vor dem Aufbau eines Netzwerkes überlegen, wie man gegen Sniffer vorgehen kann. Um einigermaßen vor Sniffer geschützt zu sein, sollte folgendes unbedingt umgesetzt werden:

- Verwenden Sie eine Sichere Netzwerk-Topologie
- Wichtiger Datenverkehr muss verschlüsselt werden
- Seien Sie wachsam

Folgend werden die ersten zwei Sicherheitsmaßnahmen gegen einen Sniffer vorgestellt.

Datenverkehr verschlüsseln:

Wenn man es nicht verhindern kann, dass Sniffer sich ins Netz einmisten, dann muss man sich überlegen wie man trotzdem seine wichtigen Daten vor Missbrauch schützt. Hier kommt eine Verschlüsselung des Datenverkehrs ins Spiel. Der Sniffer sitzt im Netz, er erhält die Daten, aber dann ist auch Schluss. Denn obwohl der Sniffer, die Datenpakete abfängt, kann er mit ihnen nichts

anfangen. Dieses Sicherheitskonzept, als Maßnahme gegen Sniffer, bringt aber leider auch einige Nachteile mit sich:

- Technische Vorraussetzungen
- Benutzerfreundlichkeit

Technische Vorraussetzungen
Über die Technische Vorraussetzungen muss man sich Klaren sein. Die Welt der Technik steht nicht, auch Angreifer entwickeln sich weiter. Primär geht es darum, erst einmal ein ausreichend starke Verschlüsselung zu finden. Man denke z.B. an die Verschlüsselungsmethode von WLAN – WEP. Lange Zeit dachte man, WEP würde man nie knacken können (manche denken das im Übrigen heute immer noch), inzwischen reichen dafür 5 Minuten. D.H. man muss mit der Zeit gehen. Hinzu kommt, dass nicht alle Programme eine Verschlüsselungslösung bieten. Hier erwartet dem Administrator viele Überlegungen und einiges an Arbeit.

Benutzerfreundlichkeit
Auch wenn die meisten Administratoren die Sicherheit ihres Netzwerkes sehr am Herzen liegt, ist es doch schwer, die Anwender auch davon zu überzeugen. Da wird lieber ein einfaches Passwort genommen, das man sicher besser merken kann, als ein Sicherhheit-Konformes. Bei den meisten Benutzern, rennen Administratoren an eine Wand, wenn es sich um Sicherheitsfragen handelt. Und selbst wenn ein Anwender sich die ersten Tage vorbildlich verhält, wird es auf die Dauer, dennoch nachlassen.

Als Lösung beider Probleme, präsentiert sich **SSH**. SSH bedeutet **Secure Shell** und ermöglicht eine sichere Kommunikation auf der Anwendungsebene. SSH wird schon in den meisten Unternehmen eingesetzt. Es verbindet Benutzerfreundlichkeit mit Sicherheit.

Weitere Informationen zu SSH finden Sie unter: www.ssh.com

Sichere Topologien

Topologien sind in einem Netzwerk ein elementarer Baustein. Bei einer Fehlplanung, kann hier schnell ganz viel Geld aus dem Fenster geschmissen werden. Gerade wegen der erheblichen Kosten die auf einem zukommen, sobald man sein altes Netz sanieren möchte, findet man oft noch veraltet Topologien. So werden z.B. zu heutigen Zeit überhaupt keine Hubs mehr eingesetzt, dennoch sieht man immer wieder gerade ein solches Gerät im Netzwerk hängen, oft mit fatalen Folgen.

Man muss sich vor Augen halten, das Sniffer alle Daten in einem Netzwerksegment abfangen können. Daraus ergibt sich, umso kleiner die Abschnitte sind, an umso weniger Daten gelangt der Sniffer. Früher war eine solche Trennung, mit erheblichen Kosten verbunden. Switche waren zu dieser Zeit noch um einiges teurer, wie Hubs. So griffen viele Firmen zu Hubs statt zu Switchen. Ein Fehler, der sich eventuell sogar gerächt hat.

Da aber zur heutigen Zeit, Switche kaum mehr kosten, wie Hubs (wenn man denn noch welche findet), fällt es einem leichter, ein sicheres Netzwerk aufzubauen. Folgende Geräte, kann ein Sniffer ohne weiteres nicht passieren:

- Router
- Switch
- Bridge

Benutzen Sie diese Geräte um das Netzwerk zu „zerteilen“. Doch dass dies auch nicht die sicherste Lösung ist, zeigt der nächste Abschnitt. Wir haben uns gefragt, ob man mit Switchen wirklich die Gefahr eines Sniffers eliminieren kann.

Switche, die ultimative Superlösung gegen Sniffer?

Da Sniffen in geswitchten Netzen theoretisch unmöglich ist, wäre die offensichtlichste Lösung, einfach Switche in das Netz zu installieren. Die auftretende Kosten der Umrüstung bzw. Neuinstallation könnte dann auch noch damit begründet werden, das Switche gerade gemessen mit Hubs, auf jeden Fall ins Netz gehören. Doch ist man dann mit den neuen Switche wirklich Sicher? Müssen sich Administratoren mit Switchen im Netz keine Sorge mehr wegen Sniffern machen?

Die Antwortet lautet ganz klar NEIN. Auch wenn man mit Switchen mehr Arbeit für den Angreifer bereitet, ist es zur heutigen Zeit keine große Kunst mehr, Switche auszutricksen. Mit folgenden Methoden können Angreifer Switche austricksen:

Fälschen der MAC-Adresse:
Das fälschen der MAC-Adresse ist keine große Kunst. Sendet nun der Angreifer ein Paket mit der gefälschten MAC-Adresse an den Switch, „lernt" der Switch zu welchem Port die gefälschte MAC-Adresse gehört. So liefert der Swich jedes mal die Daten falsch aus. Mit dieser einfachen Manipulation kann man einfach an Daten herankommen. Als Gegenmaßnahmen, bietet sich eine feste manuelle Konfiguration der MAC-Adressen an. So kann die Adresse im Switch nicht mehr geändert werden.

Den Switch überfluten (flooden):
Diese Methode (flooden) kennt man von DOS-Attacken, bei denen ein Ziel so lange mit „Müll" bombardiert wird, bis es in die Knie geht. Dies funktioniert auch mit einigen Switches die so vom Switching- in den Repeatmodus schalten. Im Repeatmodus werden alle Daten an alle Stationen weitergeleitet. Diese schon recht „banale" Attacke wird aber kaum noch verwendet, da sie zum einen zu schnell entdeckt wird und zum anderen es genügen Schutzmaßnamen, auch innerhalb des Switches gibt.

Datenpakete per ICMP:
ICMP steht für Internet Control Message Protocol. Router verwendeten ICMP um Host mitzuteilen, wer ein Router ist bzw. welcher der nahste Router ist. Mit diesen Informationen baut sich der Host eine Liste zusammen. Fälscht man nun diese ICMP Pakete, hat man die Möglichkeit den eigenen Rechner als Router auszugeben.

Nun hat man zwei Möglichkeiten: ICMP Redirect oder ICMP Advertisement.

Durch ICMP-Redirect leitet ein Router normalerweise einen Host auf einen anderen Router um. Dies ist sehr praktischen, wenn über diesen Router, die Route verkürzt ist. Um sich diese Mitteilung dauerhaft zu merken, wird Routing-Tabelle des Host umgeschrieben. Dies kann sich ein Angreifer zu nutzen machen, und sich nun selber als Router ausgeben.

Auch per ICMP-Advertisement gibt sich der Angreifer als Router aus. Durch ICMP Advertisement kündigt sich ein Router an. Um sich vor solchen Angriffen zu schützen, werden oft ICMP Advertisement nicht akzeptiert.

Mirror Port einstellen:
Besitz man die Möglichkeit an die Konfiguration eines Switches zu kommen, z.B. wenn das Passwort nicht geändert wurde und so ein Standartpasswort des Herstellers noch eingespeichert ist, hat man die Möglichkeit den Switch zu konfigurieren. So kann man bei vielen Geräten einen Port als Mirror Port definieren. Über diesen Mirror Port läuft dann der gesamte „gespiegelte" Datenverkehr. Hängt man nun ein Gerät z.B. ein Laptop an diesen Mirror Port, ist es ganz einfach, den ganzen Datenverkehr zu sniffen. Deshalb sollte die ganze Hardware, wie Switch, Router usw.

in einem separaten gesicherten Raum stehen, in den nur qualifizierte Mitarbeiter Zutritt bekommen. Sollte so ein Raum nicht zu Verfügung stehen, gerade in kleinen Firmen kann das der Fall sein, könnte man die Hardware in einen Schrank stellen, der ebenfalls verschließbar ist. Denn wer Zutritt zur Netzwerkhardware besitz, der hat Zutritt zum ganzen Netz.

Diverse Tools:
Diverse Tools erlauben selbst Laien, einen Switch zu umgehen. Sie bewirken, das alle, aber auch alle Daten an den PC auf dem das Programm ausgeführt wird gelangen. Diese mehr als nur erschreckende Entwicklung sollte jedem Administrator zu denken geben. Benötigte man vor einiger Zeit noch ein fundiertes Wissen über das „hacken“ in Netzen, kann heute schon jeder Laie, den Administrator Arbeit bereiten. Einziger Lichtblick, ist hierbei das diese oft sogenannten „Script Kiddies“ recht einfach aufzuhalten sind. Dennoch kann gerade ein Mitarbeiter z.B. mit solchen Tools intern im eigenen Netz enormen Schaden anrichten. Das verhindern von Installationen von solchen Tools, ist leider nicht so einfach. Ein Weg wäre die Kompletten Rechte der User zu nehmen. So das sie nicht mehr als Administrator unterwegs sind. Diese Maßnahme bringt dazu noch einige weitere sicherheitstechnische Vorteile mit sich. Dennoch können die Tools z.B. auch über USB-Sticks, Karte, Disketten oder allgemein Datenträger ins Netz gehängt werden. Als Administrator darf man keinen Weg außer acht lassen. Bei solchen Themen sind Mitarbeiter besonders einfallsreich.

Bekannte Freeware Sniffer:

Ethereal bzw. Wireshark
Ethereal war einer der beliebtesten Freeware-Sniffer für das Betriebssystem: Windows. Doch wird es Ethereal bald nicht mehr geben. Der Sniffer bekam nämlich einen Namenswechsel verpasst. Da der Entwickler nun bei einer anderen Firma arbeitet, die Namensrechte von Ethereal aber noch bei der alten Firma liegen, musste ein neuer Name her. Ethereal wird zukünftig nun Wireshark heißen. Strukturell unterscheidet sich Wireshark bis jetzt noch nicht von Ethereal, man darf aber gespannt sein, wie sich Wireshark noch entwickeln wird.

Weitere Informationen und den Download finden Sie unter: http://www.wireshark.org/

TCPDUMP:
Neben Ethereal bzw. Wireshark, ist TCPDUMP mit einer der bekannteste Freeware-Sniffer. Programmiert wurde TCPDUMP von Van Jacobson, Craig Leres und Steven McCanne. Im Gegensatz zu Wireshark (bzw. Ethereal), stellt TCPDUMP keine Benutzoberfläche bereit. Gearbeitet wird über Kommandozeile im Textmodus. TCPDUMP ist bei den meisten Unix-Sytemen, bereits in Grundsystem enthalten, sodass eine zusätzliche Installation entfällt. Momentan ist die Version 3.9 aktuell.

Weitere Informationen und den Download von TCPDUMP finden Sie unter:
http://www.tcpdump.org/

Snoop:
Snoop ist ein Sniffer für das Betriebssystem Solaris. Snoop wird schon mit Solaris ausgeliefert, sodass man ihn nicht extra nachinstallieren muss. Um mehr über diesen Sniffer zu erfahren, geben Sie auf einem Solaris-System, den Befehl:

man snoop

ein. Dadurch erhalten Sie das Manual, sprich die Anleitung zu Snoop.

Bekannte Kommerzielle Sniffer:

LANdecoder32:
LANdecoder32 stammt von der Firma: *Triticom*. Der LANdecoder32 ist sehr populär und wird auf dem Betriebsystem Windows benutzt. Der Sniffer eignet sich für Ethernet und Token Ring LANs. Leistungsmerkmale vom LANdecoder32 sind unter anderem:

- Analyse von Frames
- ASCII-Filterung
- Remoteüberwachung
- Einfache Bedienoberfläche

Der LANdecoder 32 unterstützt folgende Topologien:

- 10 Mbps Ethernet
- 100 Mbps Ethernet
- 4 Mbps Token-Ring
- 16 Mbps Token-Ring
- 802.11b Wireless
- PPP/WAN

Weitere Informationen sowie eine kostenlose Probeversion, finden Sie auf der Seite von Triticom: http://www.triticom.com/triticom/LANdecoder32/

EtherPeek,OmniPeek,GigaPeek und AiroPeek:
EtherPeek,OmniPeek,GigaPeek und AiroPeek sind Sniffer von WildPackets Inc. Die Namen sagen, welcher Sniffer für was geeignet, bzw. gedacht ist. So wird EtherPeek in Ethernet-Netzwerken eingesetzt, während AiroPeek für einen Einsatz in Funknetzen gedacht ist. Erhältlich sind EtherPeek,OmniPeek,GigaPeek und AiroPeek für Windows.

Weitere Informationen Informationen über EtherPeek,OmniPeek,GigaPeek und AiroPeek gibt es beim Hersteller: http://www.wildpackets.com

Vericept:
Vericept ist ein ganz außergewöhnlicher Sniffer. Er wurde nie mit der Absicht entwickelt, unzählige Datenströme ausführlich zu analysieren zu können. Viel mehr ist er dazu gedacht, zu kontrollieren ob die Mitarbeiter gegen Unternehmensrichtlinien verstoßen.

Weitere Informationen unter: http://www.vericept.com/

WLAN Sniffer:

Prinzipiell ist bei einem W-LAN überhaupt kein spezielles Sniffer-Programm von Nöten. Schließlich werden die Daten im W-LAN per Funk übertragen und so jeder wie bei einem Hub „mithören“ kann. Damit dies Funktioniert, muss einfach nur die Netzwerkkarte in den Promiscuous Mode geschalten werden.

Grundsätzlich unterscheidet man bei den W-LAN Sniffer, zwischen zwei Arten. Man unterscheidet zwischen **Aktiven W-LAN Sniffern** und **Passiven W-LAN Sniffern**

Aktive WLAN-Sniffer:

Ein Aktiver WLAN-Sniffer zeichnet sich, wie sein Name schon sagt, durch seine Aktivität aus. Um es genauer zu beschreiben: Ein aktiver WLAN-Sniffer sendet Probe-Request-Pakete an den Accesspoint. Dieser beantwortet das ganze mit einem Probe-Response-Paket. Dieses Probe-Response-Paket beinhaltet interessante Informationen für den Angreifer. So sind die wichtigsten enthaltenen Teilchen in diesem Probe-Response-Paket:

- Destination Adress(Adresse des Clients z.B. Laptop des Angreifers)
- Source Adress (Adresse des Access-Points)
- Fixed Parameters (Informationen über die Fähigkeit des Netzwerkes)
- Tagged Parameters (SSID, Länge der SSID, Channel und unterstützende Übertragungsgeschwindigkeit

Dadurch ergeben sich folgenden Informationen für den Angreifer:

- Logischer Netzwerkname (SSID)
- MAC Adresse des Access-Points
- Konfiguration des Access-Points

Um es zusammenfassend zu erklären: Der Sniffer ruft einfach mal in den Raum ob jemand da sei und jeder Access-Point antwortet: Ja bin hier im Netz so und so.
Einer der bekanntesten Aktive Sniffer ist NetStumpler.

Passive WLAN-Sniffer:

Passive WLAN-Sniffer arbeiten im **Monitormodus** englisch **Monitor Mode**. Im Gegensatz zum Promiscuous Modus, werden beim Monitormodus alle Daten, roh weitergeleitet. Denn beim Promiscuous Modus werden nur die Pakete des „Netzwerkes“ (Accesspoint) weitergeleitet, beim Monitor Modus sind es wirklich alle.
Sind nun genügend Pakete gesammelt, kann z.B. damit begonnen werden den WEP-Schlüssel zu „erraten“.

Vorteile von Passive WLAN-Sniffer gegenüber Aktiven:

- Passive Sniffer können nicht aufgespürt oder bemerkt werden
- Passive WLAN.Sniffer erkennen Aktive WLAN-Sniffer anderstherum nicht
- Passive WLAN-Sniffer erkennen auch exotische Netzwerke

Zu den Passiven WLAN-Sniffern zählen unter anderem: Kismet, NetDetect oder Airopeek.

Fazit:

Sniffer sind zum einem sehr nützlich. Unstimmigkeiten und Probleme im Netzwerk können mit Sniffer aufgeklärt und lokalisiert werden. Aber so sehr sie auch nützlich sind, so sehr können sie Schaden anrichten. Durch Sniffer können Passwörter, Benutzernamen und streng vertrauliche Informationen gestohlen werden. Da Sniffer passiv agieren sind sie nur schwer zu entdecken. So können Schäden in einem erheblichen Ausmaß entstehen. Deshalb ist es wichtig, dass sich Administratoren der Gefahr, die ein Sniffer darstellt, bewusst sind. Sie müssen verstehen, wie ein Sniffer arbeitet und wie man ihn einsetzt.

Letztendlich schützt man sich vor Sniffer, durch einen wachen Administrator, einer sicheren Topologie und durch eine starke Verschlüsselung.

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung des Webmasters von www.easy-network.de.

Für die Vollständigkeit und Korrektheit des Angebotes übernimmt der Autor keine Haftung. Für Inhalte externer Seiten, auf die von dem Dokument aus gelinkt wird, übernimmt der Autor keine Verantwortung.

© www.easy-network.de