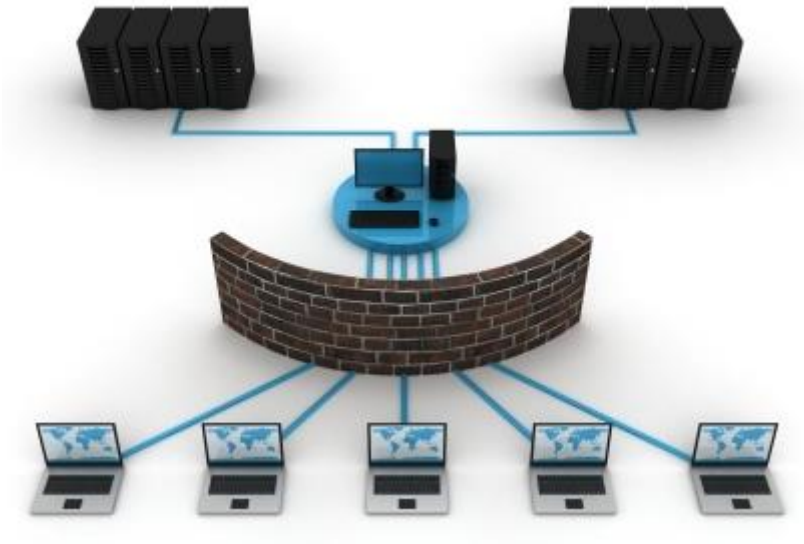
Arbeitsblätter

Grundlagen der Netzwerktechnik

Sicherheitsaspekte im LAN



Übersicht

00_Praxisbeispiele Recht

Urkundenfälschung

Phishing

Das Phishing lässt sich in zwei voneinander unabhängige Schritte wie folgt unterteilen:
Als ersten Schritt kontaktiert die Täterschaft das potentielle Opfer mittels einer e-mail, die es dazu verleiten soll, vertrauliche Informationen in Bezug auf seine E-Banking- Zugänge (Passwort, PIN-Code, weitere Sicherheitsmerkmale) preiszugeben. Häufig wird dabei das Opfer durch einen im e-mail aufgeführten Link auf eine Internetseite gelockt, welche das E-Banking-System seines Finanzinstitutes nachahmt.

Sobald das Opfer dort seine Zugangsinformationen eingibt, stehen diese der Täterschaft zur Verfügung. In einem zweiten Schritt loggt sich dann die Täterschaft mit diesen Zugangsinformationen in das E-Banking-System des betreffenden Finanzinstitutes ein und löst im Namen des Opfers entsprechende Geldtransaktionen aus. Bevor der Kontoinhaber oder das Finanzinstitut etwas bemerken sind die Gelder überwiesen und abgehoben.

Phishing-e-mails, die selber mit konkreten Handlungsanweisungen zur Eingabe der Zugangsdaten versehen und vom Original des konkreten Finanzinstitutes nicht zu unterscheiden sind, erfüllen überdies in der Schweiz den Straftatbestand der Urkundenfälschung (Gisin, 2007).

Unbefugte Datenbeschaffung

Unbefugte Datenbeschaffung im Vergleich zum Diebstahl

	Diebstahl	**Datenbeschaffung**
Tatobjekt	Fremde bewegliche Sache	Elektronische Daten, die nicht für den Täter bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind
Tathandlung	Wegnehmen	Beschaffen

(Albrecht)

Beispiel:
Kreditkartendaten hacken (über Internet abfangen) um schliesslich damit selbst einzukaufen.

Unbefugtes Eindringen in Datenverarbeitungssysteme

Ein getrennt lebender Ehemann drang in das passwortgeschützte E-Mail-Konto der Ehefrau bei ihrem Provider ein, wobei er zwei Mails ausdruckte. Nachdem die Frau dies entdeckt hatte, stellte sie Strafantrag wegen unbefugtem Eindringen in ein Datenverarbeitungssystem. (Jusletter von HÄBERLIN & PARTNERS)

Unbefugtes Beschädigen von Daten

Wardriving[1]scheint für immer mehr Freaks auf der ganzen Welt ein interessanter Sport zu sein. Ausgerüstet mit einem Laptop, spezieller Software, einer Antenne und einem GPS ziehen sie aus und durchkämmen Städte und ganze Landstriche mit dem Ziel, über einen Accesspoint auf ein ungeschütztes Wireless-LAN zuzugreifen.

Gemäss eigenen Angaben der Wardriver besteht ihre Aktivität nur darin, mit Hilfe desspezifischen Equipments in nicht geschützte drahtlose Netzwerke zu gelangen. Falls ein einfacher Zugriff auf Computer oder Netzwerkkomponenten möglich ist, wird häufig ein Hinweis hinterlassen, damit dem zuständigen Netzwerkbetreiber bewusst wird, dass sein Netz ungeschützt ist (vgl. dazu beispielsweise unterwww.wardriving.ch).

Das Hinterlassen eines Hinweises auf dem System zuhanden der Administratoren ist eine Veränderung von Daten, was als Datenbeschädigung bestraft wird. (Sury, 2003)

Herstellung und Zurverfügungstellung bösartiger Programme

Die Beantwortung der Frage, was denn nun ein bösartiges Programm überhaupt sei, ist sehr schwierig. Unter bösartigen Programmen können in erster Linie Software-Routinen verstanden werden, die einer Sache oder eine Person direkt oder indirekt Schaden zuführen. Ein Computervirus oder –wurm mit offensichtlicher und durschlagender Schadensroutine wäre dem eindeutig zuzuteilen. Gehört aber nun ein Virus, der entwickelt wurde, um einen anderen Virus zu entfernen, ebenfalls zur Klasse der bösartigen Software?

Wie sieht es mit Tools aus, mit denen sich Schwachstellen auffinden und ausnutzen lassen (Securityscanner oder Exploits)? Diese können sowohl für den unerlaubten Einbruch in Systeme genutzt werden – Oder sie lassen sich von Administratoren einsetzen, um schnell und komfortabel etwaige Schwächen ausfindig zu machen und zu beheben. Sie sehen also, dass die „Bösartig-

[1] Mit dem Wort «war» ist nicht Krieg gemeint. Es stammt aus dem Film «War Games» aus den 80-er Jahren, bei dem «wardialing» vorkommt. Hier ruft man alle möglichen Nummern an um eine Schwachstelle zu finden.

keit“ eines Produkts in erster Linie von seiner Nutzung und dem Anwender abhängt. Der bekannte US-amerikanische Kryptologe und Buchautor Bruce Schneier hat dies ebenfalls in einem Briefwechsel mit Marc Ruef anhand der Beispiele von Telefonen und Autos geäussert [2006]. Es bleibt somit fragwürdig, eine schwer definierbare Gattung von Software pauschal zu verbieten, denn damit entstehen unter Umständen für eine Vielzahl gutartiger Benutzer entscheidende Nachteile.(Ruef, 2006)

Ein Praxisfall:

A.- X. (geb. 1970) schloss im Frühling 1996 mit der amerikanischen Gruppe "A." einen Lizenzvertrag, der ihn gegen Gebühr berechtigte, die amerikanische Version eines Datenträgers (CD-ROM) "B." in Europa zu vertreiben. Er liess 3’000 solche Datenträger pressen, ohne selber etwas am Datenbestand zu ändern, und bot diese im Internet im In- und Ausland zum Verkauf an. Er verschenkte Werbeexemplare und verkaufte rund 100 Stück zum Preis von je Fr. 70.-.
Die CD-ROM ist über ein Web-Browser-Programm (z.B. Microsoft, Internet-Explorer, Netscape) lesbar. Sie enthält im Inhaltsverzeichnis unter anderem einen Bereich, der mit "VIRUS" betitelt ist. Dieser Teil, der in fünf Unterbereiche gegliedert ist, enthält zwar kein lauffähiges Virusprogramm. Es finden sich dort jedoch Instruktionen und Hinweise zur Erzeugung von Programmen, die Daten infizieren, zerstören oder unbrauchbar machen. Das Bezirksgericht Zürich (Schweiz) erkannte X. am 20. Juli 2000 der gewerbsmässigen Datenbeschädigung schuldig und verurteilte ihn zu einer Busse von Fr. 300.-. Am 22. Februar 2001 bestätigte das Obergericht des Kantons Zürich (Schweiz) den Schuldspruch, sprach eine bedingte Gefängnisstrafe von zwei Monaten aus und büsste X. mit Fr. 5’000.- (publiziert in ZR 100/2001 Nr. 44).

Betrügerischer Missbrauch einer Datenverarbeitungsanlage

Im Juni und im August 2005 wurden schweizweit E-mails mit dem Vermerk „PostFinance Online Service“ mit einer vermeintlichen Absenderadresse von PostFinance an eine unbestimmte Anzahl Personen versendet. Die e-Mails enthielten die Botschaft, dass E-Banking-Kunden von PostFinance den im e-Mail enthaltenen Link lautend auf www.yellow-net.ch anwählen sollten.

Wählte man den erwähnten Link an, gelangte man auf eine Internetseite, welche dem e-Banking-System der Schweizerischen Post (www.yellownet.ch) zum Verwechseln ähnlichsah. Auf der Internetseite wurde man in englischer Sprache aufgefordert, seine yellownet-Benutzernummer, das Passwort und die nächsten 6 Sicherheitsnummern der verwendeten Streichliste (ein weiteres Si-

cherheitsmerkmal des E-Banking-Systems derSchweizerischen Post) anzugeben. Als Begründung wurde wenig aufschlussreich eine Überprüfung der Nutzungsrechte aufgeführt.

Aufgrund der Phishing-e-Mails vom Juni 2005 legte eine unbekannte Anzahl von PostFinance-Kunden die gewünschten Zugangsdaten offen. Als die Schweizerische PostKenntnis von der Phishing-Attacke erhielt, versuchten in einem ersten Schritt die internen Fachstellen gemeinsam mit der Melde- und Analysestelle Informationssicherung (MELANI) des Bundesamtes für Polizei die Internetseite der Phisher deaktivieren zulassen. Die fragliche Internetseite wurde von einem Server in Asien gehostet, welcher nach wenigen Stunden tatsächlich reagierte und die Seite vom Internet entfernte. Dennoch gelang es der Täterschaft ab 13 Konten Überweisungen via Western Union nach Russland und Estland auszulösen und in 10 Fällen dort das Geld auch in Empfang zu nehmen. In drei Fällen blieb es beim Versuch, weil PostFinance nachBekanntwerden der Vorgehensweise sämtliche Transaktionen im Western Union-Kanalder Post blockierte und jede weitere gewünschte Transaktion detailliert nachprüfte.

Die Phishing-Attacke vom Juni 2005 wurde vom zuständigen Untersuchungsrichter in10 Fällen als strafbare Handlung und in 3 Fällen als vollendeter Versuch dazu gewertet. (Gisin, 2007)

Erschleichen einer Leistung

Nutzung eines Swisscom hotspots, wobei der Passwortschutz umgangen wird und somit für die Dienstleistung nichts bezahlt wird.

Unbefugtes Benutzen von Computerprogrammen, Urheberrechtsgesetz

Microsoft geht nicht alleine gegen **illegale Software** vor. Um den Schaden, der durch illegalen Softwareeinsatz entsteht, zu reduzieren haben einige Softwarehersteller (Adobe, Autodesk, Bentley Systems, Microsoft, Symantec, Avid Technology, Macromedia, Nemetschek, O & O Software, Trend Micro, Veritas Software GmbH und WRQ Software) die **Business Software Alliance** (BSA) gegründet. Die BSA ist ein internationaler Interessenverband der Softwarehersteller, der sich weltweit für den urheberrechtlichen Schutz von Software einsetzt. Dabei verfolgt die BSA zwei Strategien:

1. Aufklärung und Information durch Veranstaltungen, Presseinformationen, Infobroschüren, Lobbyarbeit, Informationen und Hotline
2. Gezielte Verfolgung - sowohl zivil- als auch strafrechtlich.

Ein konkretes Beispiel

Im **April 2007** wurde eine gerichtlich Hausdurchsuchung bei einem Unternehmen der Finanzbranche in Linz angeordnet. Bei dem darauf folgenden Strafverfahren gegen den Geschäftsführer aufgrund von Verwendung unlizenzierter Software verpflichtete sich das Unternehmen zu einer **Schadenersatzzahlung** von **EUR 30.000**. Darüber hinaus hat das Unternehmen die Pauschalgebühren des gerichtlichen Vergleichs zu tragen und die Pauschalkosten des Strafverfahrens zu ersetzen. Weiter ist für jede weitere einzelne Verletzung eine Vertragsstrafe von 300,- Euro zu bezahlen. Die gesamte Unternehmensgruppe muss nun im großen Umfang Lizenzen nachkaufen.

Weitere Beispiele auf
http://www.microsoft.com/austria/originalsoftware/aktuellefaelle.mspx(Microsoft)

Verletzung von Persönlichkeitsrechten, Datenschutzgesetz

21.09.2009
Großbritannien

Erneut Selbstmord wegen Cyber-Mobbing

Zum dritten Mal innerhalb von zwei Jahren hat sich in Großbritannien ein junges Mädchen das Leben genommen, weil es online gemobbt wurde. Der Online-Psychoterror wird zum Massenphänomen. Das Problem dabei: Die meisten Jugendlichen nehmen ihn nicht ernst genug - manche aber zerbrechen daran.

London - Sie fühlte sich in Online-Netzwerken wie Facebook mehrfach gemobbt - jetzt hat sich ein Mädchen in England vermutlich unter anderem wegen solcher Hänseleien umgebracht. Holly Grogan war 15 Jahre alt, als sie vergangene Woche nahe der Stadt Gloucester von einer Brücke sprang, wie die britische Zeitung "The Times" am Montag berichtete. Die Eltern beklagten, ihre Tochter sei nicht mit dem Druck und dem Mobbing auf Netzwerken und in "Freundschafts-Gruppen" im Internet wie Facebook, Bebo und MySpace zurechtgekommen.

Freunde erklärten, mehrere Mädchen hätten Holly auf ihrer Facebook-Seite reihenweise beschimpft. Sie sei auch in der Schule gemobbt worden und habe kein Selbstvertrauen gehabt. Teenager kennen das, manche von ihnen werden zu "Opfern" - so heißt das im Jugendjargon manchmal allzu treffend. Mobbing ist ein Phänomen, das oft von einzelnen ausgeht, bald aber von einer wachsenden Gruppe billigend oder teilnehmend mitgetragen wird. Auch Online ist es dann mitunter schwer, Verursacher auszumachen - und genauso nehmen das auch die Opfer wahr: Alle Welt ist gegen sie.

Erst Ende August war in Großbritannien erstmals ein Teenager wegen Mobbings im Internet zu einer drei Monate langen Haftstrafe verurteilt worden. Die 18-Jährige musste in eine Jugendstrafanstalt, unter anderem weil sie auf Facebook eine ehemalige Schulkameradin mit dem Tod bedroht hatte.

Aktuellen Schätzungen zufolge haben zwischen 30 und 40 Prozent aller Jugendlichen im Web Erfahrungen mit Formen des Cyber-Mobbing. Psychologen sehen darin ein wachsendes Problem, auch wenn herkömmliche Mobbing-Methoden meist als bedrohlicher empfunden werden: Auch sie werden immer wieder ursächlich für Selbstmorde gesehen.

Weil Jugendliche online aber quasi rund um die Uhr erreichbar sind und sich das Mobbing zudem auf einer für jedermann zugänglichen Plattform abspielt, wird es von einem Teil der Betroffenen als noch demütigender empfunden als andere Formen des Mobbings. Oft begleitet wie im aktuellen Fall das Cyber-Mobbing zudem den täglichen Terror auf dem Schulweg oder -hof. In einzelnen Fällen endet schon der pubertäre Online-Terror tödlich: Bekannt sind Fälle in den USA, Kanada, in Australien und eben Großbritannien.

Verbreitetes Problem

Erst im Juli 2009 nahm sich dort die erst fünfzehnjährige Megan Gillan mit einer Medikamentenüberdosis das Leben. Im Sommer 2008 erhängte sich der dreizehnjährige Sam Leeson, nachdem er mehrere Monate lang als angeblich depressiver Emo-Fan gemobbt worden war.

Im Januar 2008 überlebte ein 16-jähriger einen Selbstmordversuch. Der Junge versuchte sich umzubringen, nachdem er erkannte, dass ein homosexuelles Cyber-Verhältnis, auf das er sich auch emotional eingelassen hatte, von einer dritten Person mit Hilfe einer erdachten Identität inszeniert und Details daraus weitergegeben worden waren.

Der Fall endete mit einer ersten Verurteilung wegen Cybermobbings in Großbritannien: Der 17-jährige Täter wurde für zwölf Monate unter Beobachtung eines Jugendhilfe-Projektes gestellt und dazu verurteilt, seinem Opfer 250 Pfund Schmerzensgeld zu zahlen. Im Laufe des Prozesses wurde klar, wie weit die Wahrnehmungen von Opfer und Täter auseinander klafften: Auch für den Mobber war der Selbstmordversuch ein Schock, weil er mit so einer Konsequenz nicht gerechnet hatte. Für ihn war das Mobbing mit virtuellen Mitteln ein "Streich", den er später bedauerte.

In den USA führte der spektakuläre Fall der Megan Meier, die im Oktober 2006 von einer erwachsenen Frau in den Selbstmord gemobbt worden war, zu einer Verschärfung der Gesetze in mehreren Bundesstaaten: Noch anhängig ist der Gesetzantrag "Megan Meier CyberbullyingPreventionAct", der dem US-Kongress seit April 2009 vorliegt. In Deutschland werden Mobbing

und Diffamierungen online analog zu solchen Sachverhalten in gedruckter oder vor Zeugen geäußerter Form behandelt. Beleidigungen, üble Nachrede und Ähnliches werden auf Basis der entsprechenden Gesetze geahndet.*pat/dpa*

(pda, 2009)

Quellverzeichnis

Albrecht, P. (kein Datum). *http://ius.unibas.ch.* Abgerufen am 12. Mai 2010 von http://ius.unibas.ch: http://ius.unibas.ch/typo3conf/ext/x4eunical/scripts/handleFile.php?file=6932

Gisin, M. (16. April 2007). *Phishing und Skimming - Die Strafbarkeit aktueller Deliktsformen im elektronischen Zahlungsverkehr.* Abgerufen am 10. Mai 2010 von Competence Center Forensik und Wirtschaftskriminalistik: http://www.ccfw.ch/gisin_markus.pdf

Jusletter von HÄBERLIN & PARTNERS. (kein Datum). Abgerufen am 10. Mai 2010 von HÄBERLIN & PARTNERS : http://www.hps-law.ch/hps_net/hps_net_d/doku/LO2_1_009.pdf

Microsoft. (kein Datum). *Rechtslage - Aktuelle Fälle.* Abgerufen am 12. Mai 2010 von http://www.microsoft.com: http://www.microsoft.com/austria/originalsoftware/aktuellefaelle.mspx

pda. (21. September 2009). *http://www.spiegel.de/netzwelt/web/0,1518,650340,00.html*. Abgerufen am 12. Mai 2010 von Spiegel.de: http://www.spiegel.de/netzwelt/web/0,1518,650340,00.html

Ruef, M. (18. April 2006). *Lehrgang Computersicherheit von Marc Ruef*. Abgerufen am 10. Mai 2010 von http://www.computec.ch/mruef/publikationen/lehrgang_computersicherheit/

Sury, U. (25. Oktober 2003). *http://www.dieadvokatur.ch.* Abgerufen am 10. Mai 2010 von Zeitschrift Informatik-Spektrum der deutschen Gesellschaft für Informatik: http://www.dieadvokatur.ch/html/publikationen/pfd/infspektrum603.pdf

01_Arbeitsblatt IP-Grundlagen

Beantworte die folgenden Fragen mit eigenen Worten mit Unterstützung des Internets und mache korrekte Quellenangaben.

1. Welche Funktion hat die IP-Adresse?

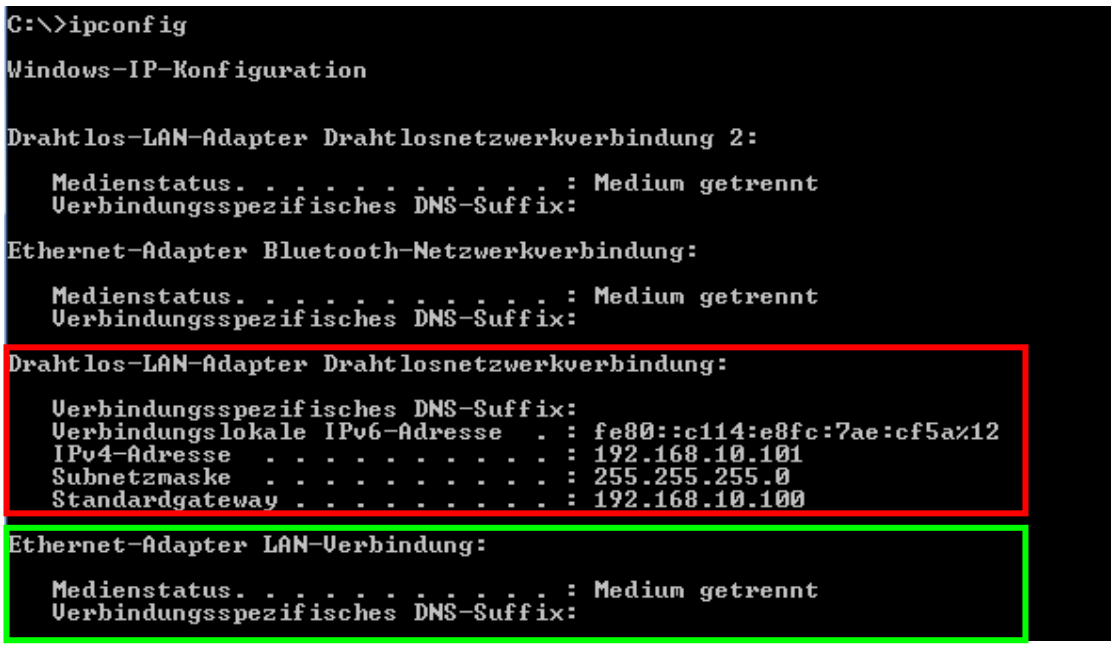
2. Zähle mindestens zwei alltägliche Analogien zur IP-Adresse auf.

3. Wie ist die IPv4 Adresse aufgebaut?

4. Worin liegt der grundsätzliche Unterschied zwischen IPv4 und IPv6?

5. Starte die Konsole mit «**cmd**».

6. Welche IP-Adresse hat dein Computer? Verwende den Befehl «**ipconfig**».
   Die Antwort auf den Befehl ist insbesondere unter Windows 7 sehr umfangreich. Unten ein Ausschnitt. Von Bedeutung sind nur Adapter, deren Status nicht getrennt ist. Wenn du über das Kabel am Netzwerk angeschlossen bist, dann findest du die Angaben unter Ethernet Adapter. In diesem Beispiel ist der Computer drahtlos verbunden.



7. Mit «**PING** IP-Adresse» kannst du testen, ob dein Gegenüber erreichbar ich. Teste, ob du selber erreichbar bist?
8. Solltest du deine eigene IP-Adresse (da zum Beispiel deine Rechte stark eingeschränkt sind) nicht kennen, dann kannst du dich mit der IP 127.0.0.1[1] selbst anpingen. Diese Adresse ist standardmässig auf jeder Netzwerkkarte eingebaut. Teste bei dir, ob es funktioniert.
9. Tausche deine IP-Adresse mit deinen Nachbarn aus. Testet, ob ihr gegenseitig erreichbar seid. Funktioniert es? Wieso nicht? Notierte dir mögliche Ursachen.

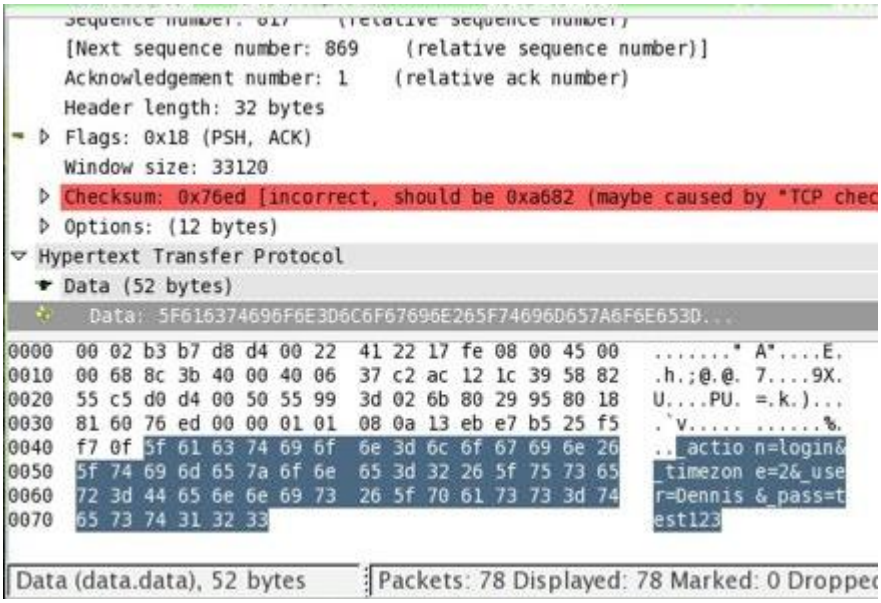
Versucht möglichst viele Clients im Netzwerk zu «finden». Protokolliere die gefundenen IP's.

[1] Von aussen ist die IP 127.0.0.1 nicht erreichbar.

02_"Hackerparagraf":

Auch die Aufpasser müssen aufpassen

Der "Hackerparagraf" zur Bekämpfung der Computerkriminalität zeigt Wirkung - aber anders als erwartet. Gerade wird das Bundesamt für Sicherheit in der Informationstechnik verklagt:
Die Behörde verstoße angeblich selbst gegen das Gesetz. Von Rainer Mersmann



Das Linux-Sicherheitstool "Wireshark" zeigt Übertragungsdaten im Klartext - und ist theoretisch illegal

Das Gesetz, das im Volksmund auch als "Hackerparagraf" bezeichnet wird, wurde am Donnerstag vor Pfingsten gegen die Stimmen von PDS sowie des SPD-Abgeordneten Jörg Tauss abgenickt. Nachts um 2.00 Uhr hatten die Abgeordneten wohl keine Lust mehr, sich ausführlich mit dem Hackerparagrafen zu beschäftigen - sie wollten in den Pfingsturlaub - und die Redner gaben ihre Wortbeiträge lediglich zu Protokoll.

Sicherheitsexperten und die Verbände der IT-Branche hatten starke Bedenken geäußert und konkrete Änderungen vorgeschlagen. Die blieben jedoch unberücksichtigt und fanden keinen Eingang in das Gesetz, das zur Bekämpfung von Computerkriminalität gedacht ist. Intention des Gesetzgebers war es, beispielsweise den Schutz vor Virenschreibern oder Hackern zu verbessern, die in fremde Computer-Systeme eindringen. Mit dem neuen Paragrafen namens 202c StGB schießt die Bundesregierung aber weit über die EU-Vorgaben und vor allem über das Ziel hinaus, denn im neuen Regelwerk wird bereits das Vorbereiten von vermeintlichen Hacker-Angriffen unter Strafe gestellt. Wer also ein Programm schreibt, mit dem sich Sicherheitslücken ausfindig machen lassen, macht sich strafbar - aber auch, wer solche Programme verbreitet und besitzt.

Und wer eine Sicherheitslücke findet und diese veröffentlicht, fällt ebenfalls unter das neue Gesetz.

Rundumschlag gegen Hacker - und System-Administratoren

Natürlich besitzen und benutzen Hacker, die in fremde Systeme eindringen wollen, solche Tools und Programme - aber auch System-Administratoren, die auf diese Weise ihr Computernetzwerk auf Schwachstellen abklopfen, um die Lücken dann zu schließen. Die einen wollen mit Hilfe der Hackertools in Computer eindringen, die anderen wollen mit den gleichen Tools genau das verhindern - aber jetzt machen sich beide strafbar. Ob sich allerdings Hacker durch die Gesetzesänderung beeindrucken lassen, ist fraglich. Seit August stehen nun auch System-Administratoren mit einem Bein im Gefängnis.

Selbst Sicherheitsexperten auf der Suche nach Schwachstellen in Programmen müssen ihre gewohnte Praxis ändern. Üblicherweise informierten sie den Hersteller eines betroffenen Programms und veröffentlichten die Sicherheitslücke dann im Internet - wenn möglich versehen mit einer Anleitung zum provisorischen Stopfen. Natürlich erfuhren Hacker ebenfalls durch die Veröffentlichung von so einem Loch. Demgegenüber erhielten auf diese Weise aber auch Sicherheitsexperten und Programmierer die Gelegenheit, an Sicherheits-Updates zum Schließen der Lücke zu arbeiten.

Konsequenz: Erste Firmen wandern ab

Im neuen Paragraf ist allein entscheidend, ob ein Programm oder eine Information dazu genutzt werden *könnte*, in fremde Computer einzudringen. Es finden sich keine Ausnahmeregelungen, die den Einsatz für legale Zwecke erlauben, wie es Sicherheits-Experten und IT-Branchenverbände gefordert hatten. Der führende Spezialist für die verbreitete Computersprache PHP, Stefan Esser, hat daraus seine Konsequenzen gezogen. Er veröffentlicht keine Sicherheitslücken mehr. Andere Fachleute folgten seinem Beispiel. Auch Firmen, die auf ihren Webseiten Sicherheitstools anbieten, haben reagiert: Sie verlegten ihre Server und Programmier-Abteilungen ins Ausland und entzogen sich damit der deutschen Gerichtsbarkeit.

Wenn man das Gesetz streng auslegt, macht sich sogar jeder Besitzer eines Windows-PCs strafbar: dort sind die Programme "ping" und "tracert" installiert. Mit "ping" lässt sich feststellen, ob ein Rechner online, mit "tracert" über welche Wege er zu erreichen ist. Beides sind grundlegende Voraussetzungen, um einen Rechner anzugreifen. Mit einem Fuß im Gefängnis stehen neuerdings auch Linux-User. Bei einem Linux-Rechner sind in der Regel die Programme "nmap" und "tripwire" beziehungsweise dessen Nachfolger "Wireshark" installiert. "nmap" dient dazu, offene

"Türen" auf einem Rechner aufzuspüren. Mit den beiden anderen Programmen lässt sich der gesamte Netzwerk-Verkehr mitschneiden. System-Administratoren nutzen "nmap" beispielsweise zur Erkennung von Trojanern, da diese meist "Türen" öffnen, die normalerweise geschlossen sein sollten. Mit "tripwire" und "Wireshark" können sie ermitteln, ob Daten nach außen gehen, die nicht dafür bestimmt sind.

So kritisierte dann auch der SPD-Abweichler Jörg Tauss im Vorfeld der Abstimmung, dass der Wortlaut des Gesetzentwurfes zu einer "Kriminalisierung der heute millionenfach verwendeten Programme führe, welche auch für das Entdecken von Sicherheitslücken in IT-Systemen notwendig sind". Und Andy Müller-Maguhn vom Chaos Computer Club prognostizierte sogar: "Das Verbot des Besitzes von Computer-Sicherheitswerkzeugen öffnet auch dem Einsatz des Bundestrojaners Tür und Tor".

Alles nicht so schlimm - oder doch?

Das Bundesjustizministerium wiegelt ab: Selbstverständlich wolle man weder ganze Branchen und Berufsgruppen noch den privaten PC-Besitzer kriminalisieren. Dass ein um die Sicherheit bemühter System-Administrator nicht mit einem Hacker gleichzusetzen sei, sage einem doch schon der gesunde Menschenverstand. Aber wer schon einmal vor Gericht gestanden hat, weiß, dass Recht haben und Recht bekommen mit gesundem Menschenverstand wenig zu tun hat. Es gilt der Gesetzestext, und der lässt hier vermutlich wenig Spielraum für Interpretation.

"Tecchannel" will Klärung

Inwieweit das Gesetz Auslegungen zulässt, will das Magazin "Tecchannel" aus dem IDG Verlag klären. Es reichte bei der Staatsanwaltschaft Bonn Klage gegen das Bundesamt für Sicherheit in der Informationstechnik (BSI) wegen Verstoßes gegen Paragraf 202c StGB ein. Das BSI bietet auf seinen Internet-Seiten die Software BOSS (BSI OSS Security Suite) zum Download an. Pikanter Bestandteil der Security Suite ist - neben anderen Programmen, die unter das Hackergesetz fallen könnten - der Passwort-Cracker "John the Ripper", über dessen Einsatzzweck wohl keine Zweifel bestehen dürften. Zwar ist das vom BSI in die Suite eingebundene Programm ausgebremst, aber über einen direkten Link zur Hersteller-Seite kann sich jeder Besucher die voll funktionsfähige Version herunterladen - nach Ansicht von "Tecchannel" ein klarer Verstoß gegen den Paragrafen 202c.

Die Staatsanwaltschaft in Bonn (Sitz des BSI) hat nun zwei Möglichkeiten: Entweder wird der Anzeige nicht stattgegeben, weil das BSI nach Meinung der Staatsanwaltschaft keine strafbare

Handlung begeht, oder ihr wird stattgegeben und die Staatsanwaltschaft nimmt die Ermittlungen auf.

Für den Fall, dass der Anzeige nicht stattgegeben wird, rät "Tecchannel" den Betroffenen, sich am BSI zu orientieren: In einem seriösen Umfeld sei es demnach durchaus möglich, Sicherheits-tools anzubieten und zu benutzen. Im anderen Fall empfiehlt "Tecchannel", Selbstzensur zu üben - erst recht, wenn es zu einer Verurteilung kommt. Ein Freispruch des für die BOSS-CD Verantwortlichen brächte ebenfalls Klarheit, so das Magazin.

Von Rainer Mersmann (Mersmann, 2007)

Quelle:
Mersmann, R. (24. September 2007). *Stern.de.* Abgerufen am 1. Mai 2010 von Stern.de: http://www.stern.de/digital/computer/hackerparagraf-auch-die-aufpasser-muessen-aufpassen-598457.html

Fragen und Aufgaben zum Text:

1. Welche Programme werden im Artikel erwähnt, bei denen bereits der Besitz in Deutschland strafbar ist.

2. Der Artikel beschreibt, dass bereits die Verwendung von Windows in Deutschland problematisch sein kann. Warum?

3. Beurteile den Hackerparagafen. Was spricht für und was gegen den Paragrafen?

03_Arbeitsblatt ARP untersuchen mit Wireshark

Für den nächsten Auftrag nutzen wir ein Programm, mit dem der ganze Netzwerkverkehr, egal ob kabelgebunden oder bei Wireless durch die Luft, mitgelesen werden kann: Wireshark (http://www.wireshark.org)

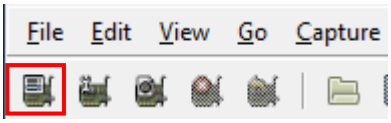
Dabei richten wir unser Augenmerk auf den Protokollablauf des ARP. Dies soll den in der Theorie besprochenen Ablauf nochmals verdeutlichen.

Selbstverständlich ist dabei die Untersuchung des ARP nur ein Beispiel für die vielen Untersuchungsmöglichkeiten des verwendeten NetzwerksniffersWireshark. Wie schnell man sich dabei allenfalls an der Grenze der Legalität bewegt, zeigt das Arbeitsblatt «**Hackerparagraf - Auch die Aufpasser müssen aufpassen**», das du als Hausaufgabe bearbeiten sollst.

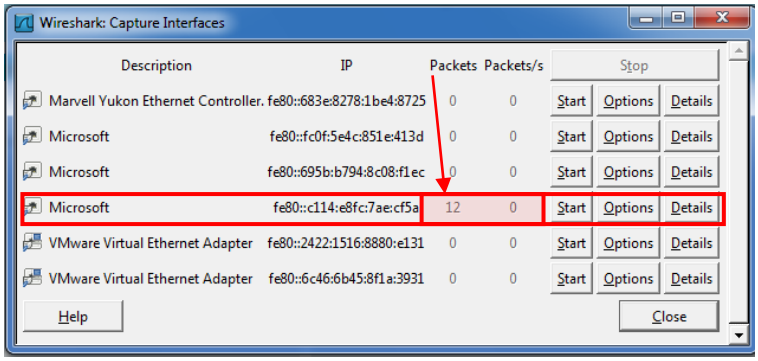
Installation von Wireshark

Wireshark ist für Windows, OS X und Linux erhältlich. Für die Installation unter Windows kann das entsprechendeInstallationsprogramm von http://www.wireshark.org/download.html heruntergeladen und mit den Standardeinstellungen ausgeführt werden. Dabei wird auch WinPcap installiert. WinPcap ermöglicht den Zugriff auf die Netzwerkkarte und muss mitinstalliert werden.

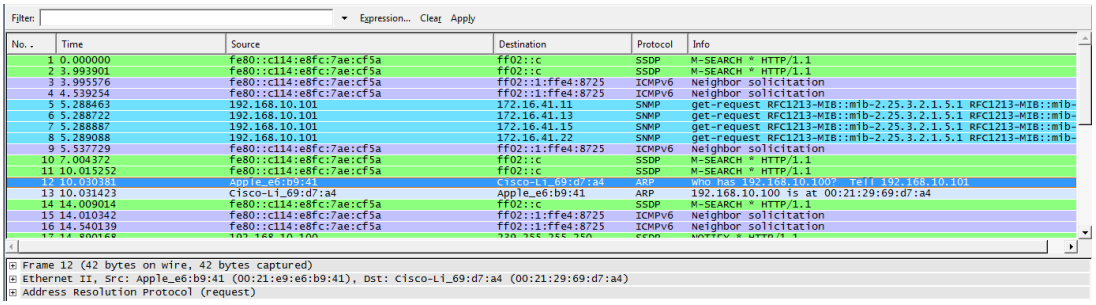
Mitlesen des Netzwerkverkehrs

1. Starte Wireshark
2. Über 

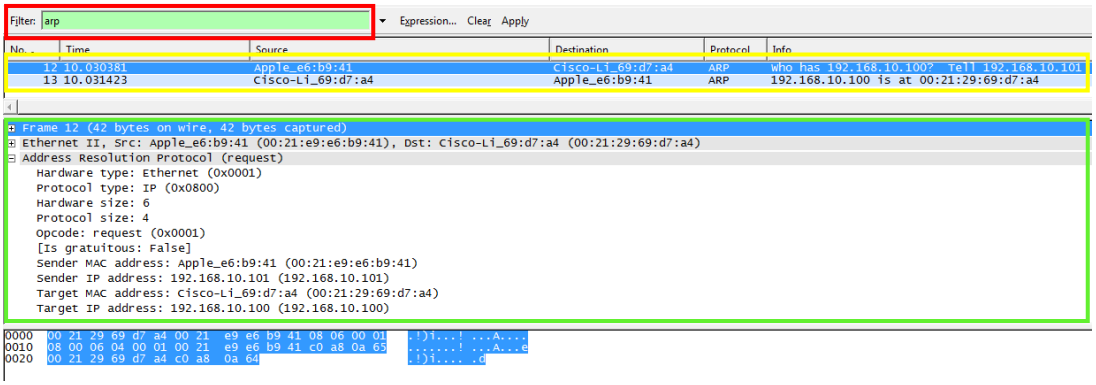
gelangst du in die Übersicht über die verschiedenen vorhandenen Netzwerkschnittstellen auf deinem PC.
3. Anhand der aktuell gezählten Datenpakete, welche über die Schnittstelle transportiert werden, kannst du die aktive Netzwerkkarte erkennen.



4. Mit einem Mausklick auf „Start“ wird das Mitschneiden des Datenverkehrs aktiviert.
5. Lass nun Wireshark rund eine Minute lang mitschneiden und beobachte, was protokolliert wird.
6. Da wirklich alles mitgeschnitten wird, sammelt sich sehr schnell ungeheuer viel an. So könnte es bei dir aussehen:



7. Durch die Eingabe von „arp“ (mit Enter bestätigen) im Filter grenzen wir unsere Resultate ein und finden auch sofort das gesuchte Protokoll:



Die in diesem Beispiel gezeigte Abfolge ist typisch für den ARP-Protokollablauf und du solltest eine vergleichbare Situation in deiner Aufzeichnung finden können.

8. Im Protokollfenster findest du die verschiedenen beteiligten Protokolle. Durch einen Mausklick auf das + werden die Details sichtbar.
9. Wie würdest du einem Laien den ARP-Protokoll-Ablauferklären? Versuche dein Vorwissen über IP- und MAC-Adressen mit einzubeziehen. Verfasse deine Version des Protokollablaufes.

04_Arbeitsblatt Mit ARP den ARP-Cache manipulieren

1. Starte die Command-Shell cmd.exe
2. Mit dem Befehlt „arp –a“ kannst du dir die ARP-Tabelle, das heisst den Inhalt des ARP-Caches anzeigen lassen.

```
C:\Windows\system32>arp -a

Schnittstelle: 192.168.10.101 --- 0xc
  Internetadresse       Physische Adresse     Typ
  192.168.10.100        00-21-29-69-d7-a4     dynamisch
  239.255.255.250       01-00-5e-7f-ff-fa     statisch
```

   Du kannst zwei Eintragstypen ausmachen: dynamische und statische. Die dynamischen werden durch die ARP-Auflösung erstellt und sind nicht veränderbar. Die statischen können manipuliert werden.
3. Mit „arp /?“ werden alle möglichen Befehlsparameter aufgelistet.
   Was bewirkt die Eingabe „arp –s“?

   _____

   _____

   _____

   _____
4. Mit „netsh interface ip delete arpcache“ kann der ganze ARP-Cache gelöscht werden.
   Gelingt es dir?
   Erscheint eine Fehlermeldung?
   Wenn ja, wie lautet sie?

   _____

   _____

   _____

   Findest du heraus, wie man das Problem umgeht? Beschreibe deine Lösung:

   _____

   _____

   _____
5. Überprüfe den Inhalt des Caches nach erfolgreichem Löschen.
   Wenn es bereits wieder einen Eintrag in der Tabelle hat, dann war das ARP schneller als du und hat bereits wieder eine erfolgreiche Anfrage gemacht.
6. Versuche einen einzelnen Eintrag zu löschen. Mit welchem Befehl ist das möglich?

   _____

7. Versuche nun einen Eintrag einzufügen. Notiere hier deinen genauen Befehl:

   _____

8. Kontrolliere anschliessend die ARP-Tabelle. Hast du deinen Eintrag gefunden?
9. Was zeigen dir diese Versuche? Notiere dir hier deine Überlegungen:

   _____

   _____

   _____

   _____

   _____

   _____

   _____

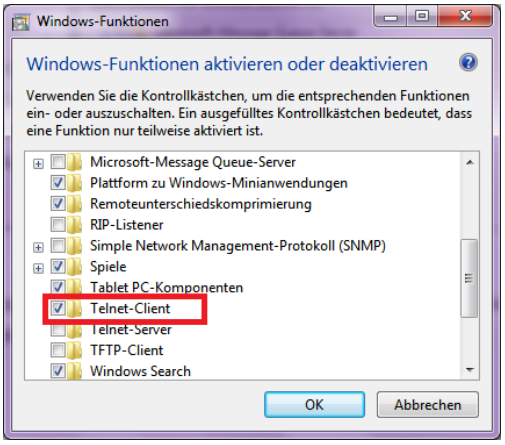
   Bespreche deine Notizen mit deinem Banknachbarn.

05_Arbeitsblatt Ports, Dienste und Protokolle

Mit dem Programm Telnet kann auf sehr einfache Art und Weise das Funktionieren von Diensten, Ports und Protokollen gezeigt werden.
Bei Windows7 ist dieses allerdings nicht standardmässig aktiviert.

Aktivierung von Telnet

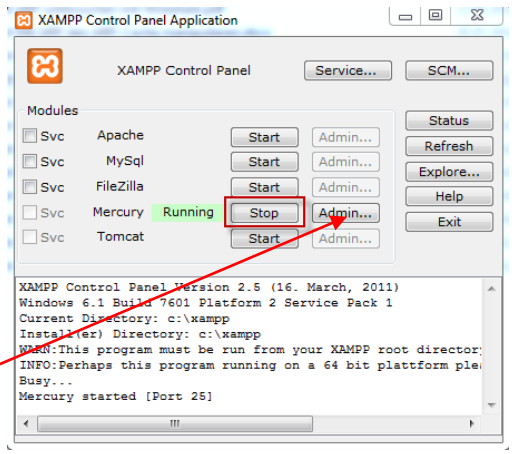
Geh auf Start→ Systemsteuerung → Programme und Funktionen → Windows Funktionen aktivieren oder deaktivieren. Aktiviere hier den Telnet-Client.



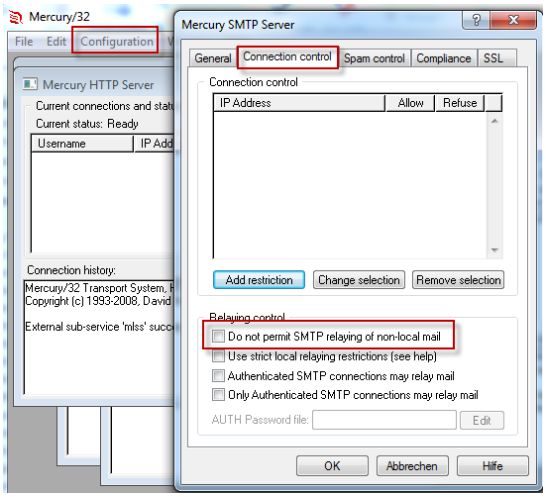
Mail über Telnet

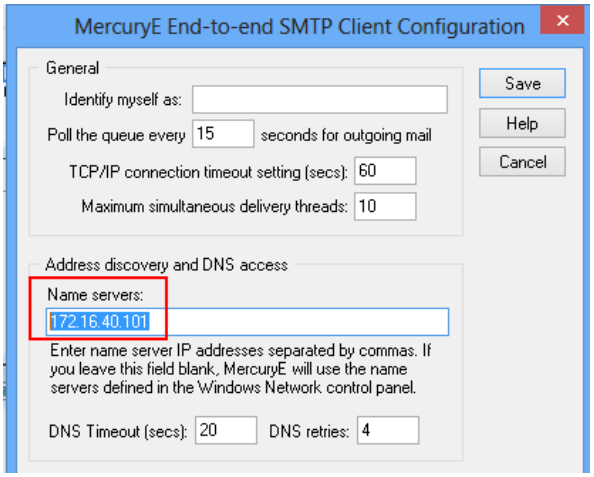
Da die meisten Mailserver umfangreiche Sicherheitsmassnahmen, wie Verschlüsselung, Authentifizierung usw. eingebaut haben, nutzen wir als Testserver einen eigenen Mailserver, den wir direkt auf unseren PCs installieren. Dieser ist dann über den Namen «localhost» aufrufbar.

Dazu installieren wir XAMPP (http://www.apachefriends.org/de/xampp-windows.html) mit den Standardeinstellungen und starten anschliessend den «Mercury-Server».
Nun müssen wir aber den Mailserver noch so konfigurieren, dass er den Versand von Mails an nicht lokale Empfänger zulässt. So also , dass ein Mail auch an «barack.obama@usa.gov» möglich wäre. Dazu geht man auf die Adminoberfläche des Mercury-Mailservers.



Dort wählt mandas Menü «Configuration» und da den Menüpunkt «MercuryS SMTP Server».
Im folgenden Fenster wählt man das Register «Connection Control» und deaktiviert «Do not permit SMTP relaying of non-local mail».
Schliesslich muss noch unter «MercuryS SMTP Client» der Namensserver eingetragen werden:





Somit steht uns ein vollwertiger Mailserver zur Verfügung. Nun viel Spass beim Mailen über Telnet.

Jede Zeile muss mit Enter abgeschlossen werden. Die Reihenfolge ist bis auf den Befehl „HELP“ zwingend – so verlangt es das Protokoll.

telnet *Mailserver* **25**	Aktiviert den Mail Dienst des Servers über SMTP. Die Zahl 25 steht für den verwendeten Port.
HELO *Mailserver*	Client meldet sich an
HELP	Alle Befehle, die der Dienst zur Verfügung stellt
MAIL FROM: *Absender*	Der Absender des Mails festlegen. Versuche es hier mit einer Fantasieadresse z.B. hase@fuchs.ch
RCPT TO: <*Empfänger***>**	Empfänger des Mails festlegen. Trage deine Email-Adresse hier ein. Damit kannst du auch überprüfen, ob dein Mail schlussendlich ankommt. Achte auf die <>. Die Empfängeradresse muss mit Spitzklammern umschlossen sein.
DATA	Anfang des Datenblocks
Daten eingeben	
.	«.» auf einer separaten Zeile schliesst die Eingabe ab.
Quit	Client meldet sich ab

Alles OK? Dann überprüfe, ob dein Mail auch angekommen ist.

Neben dem Erleben eines Protokollablaufs sollte dir diese Übung auch noch einen Hinweis auf ein Sicherheitsproblem geben. Was meinst du? _____

_____

_____

_____

_____

HTTP über Telnet

Bei diesem Beispiel stellen wir eine http-Verbindung auf. Natürlich kann unsere Konsole kein HTML darstellen. Trotzdem werden wir den Code übermittelt kriegen. Das Problem bei diesem Beispiel ist, dass du den Cursor während der Eingabe nicht mehr sehen wirst. Du darfst dich also nicht vertippen, sonst musst du von vorne anfangen. Achtung: Nach der letzten Eingabe musst du 2x die ENTER Taste drücken. Auch auf die Leerschläge musst du achten, sonst bricht die Verbindung ab. Das Protokoll ist da sehr strikt. Das Einzige was kein Problem darstellt, ist, wenn du alles klein schreibst.

`telnet www.wmisargans.ch 80`	Aktiviert den HTTP Diensts des Servers über den Port 80
`GET /index.html HTTP/1.1`	→ ENTER
`HOST: www.wmisargans.ch`	→ ENTER
`CONNECTION: close`	→ ENTER
`USER-AGENT: Mozilla`	→ ENTER→ ENTER

Telnet über Telnet

Hier noch eine «Lustige» Anwendung von Telnet. Lass dich überraschen.

`telnet towel.blinkenlights.nl 23`	Aktiviert den Telnet Dienst des Servers

06_Arbeitsblatt Schichtenmodell / Hybridmodell

1. Erkläre stichwortartig jede Schicht und zähle wenn möglich Beispiele für Protokolle, Dienste, Ports oder cmd-Befehle auf, die auf dieser Schicht «liegen».

Schicht	Aufgabe	Beispiel
Anwendung		
Transport		
Netzwerk		
Sicherung		
Physikalische		

2. Probier das cmd-Programm «nslookup» aus. Finde heraus, welche IP-Adresse die NZZ hat. Welcher Dienst verbirgt sich dahinter? Zu welcher Schicht gehört er?

07_Arbeitsblatt Portscan

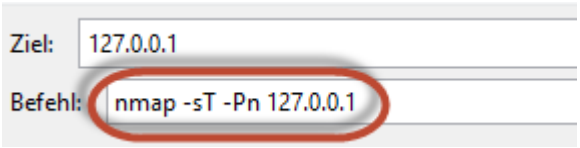
Zuerst wollen wir bei unserem System feststellen, welche Ports auf unserem Computer geöffnet sind. Führe dazu das Programm «netstat» mit dem Parameter «–a» von der Konsole aus.

Um nun auch die Ports von fremden Systemen abzuhorchen, verwenden wir das Programm «nmap» respektive «Zenmap» welches nmap eine grafische Opberfläche spendiert. Es ermöglicht uns ganze Netze nach offenen Ports zu durchsuchen, listet uns die verwendeten Betriebssysteme auf und stellt sogar grafisch die Netzwerkstruktur dar.

Installierst das Programm «nmap»[1] auf deinem Rechner.

Ports des eigenen PC's

Führe zuerst einen Portscan deines eigenen PC's durch. Dazu musst du die Zieladresse deines Computers eingeben. Die IP des eigenen Computers ist immer 127.0.0.1. Der Selbstscan auf localhost klappt nur, wenn du zwei Optionen angibst: -sT (TCP connectscan) und -Pn (Nmap soll ohne den Ping-Befehl scannen). Du gibst auf deinem Windows-PC also folgendes ein: nmap -sT -Pn 127.0.0.1. Und dann wartest du!



Bei meinem Selbsttest wurde das folgende Resultat nach vier Minuten ausgespukt:

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-04-02 17:19 Mitteleuropäische Sommerzeit
Nmap scan report for localhost (127.0.0.1)
Host is up (1.0s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1030/tcp open  iad1
2869/tcp open  icslap
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 255.65 seconds
```

Informiere dich im Internet über die folgenden Ports: 80, 21, 25, 443.
Protokolliere in der Tabelle.

[1] http://nmap.org/dist/nmap-5.30BETA1-setup.exe

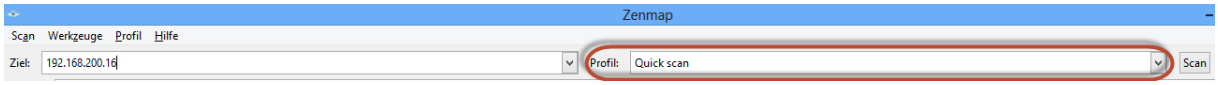
Wähle anschliessend einen der offenen Ports auf deinem System und mach dich darüber schlau. Am meisten hilft die Suche nach dem Service (Dienst), der hinter dem Port steckt. Beim Port 445 z.B. microsoft-ds

Portnummer	**Zweck**

Welche Ports sind nun bei dir vorhanden? Findest du alle «WellKnown Ports»? Erkennst du noch andere Ports?

Portscan des Nachbarn

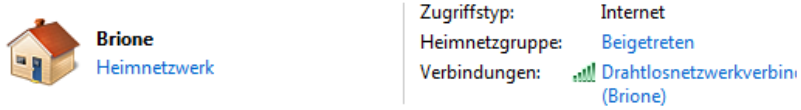
Bildet eine Zweiergruppe und tauscht eure IP-Adressen aus. Führt einen Portscan des Nachbarn durch.
Verwendet hier als Einstellung Quick Scan:



Achtet beim ersten Durchgang darauf, dass die Netzwerkart auf «Heimnetzwerk» eingestellt ist:

Für Windows 7:

Start – Systemsteuerung – Netzwerk- und Freigabezenter



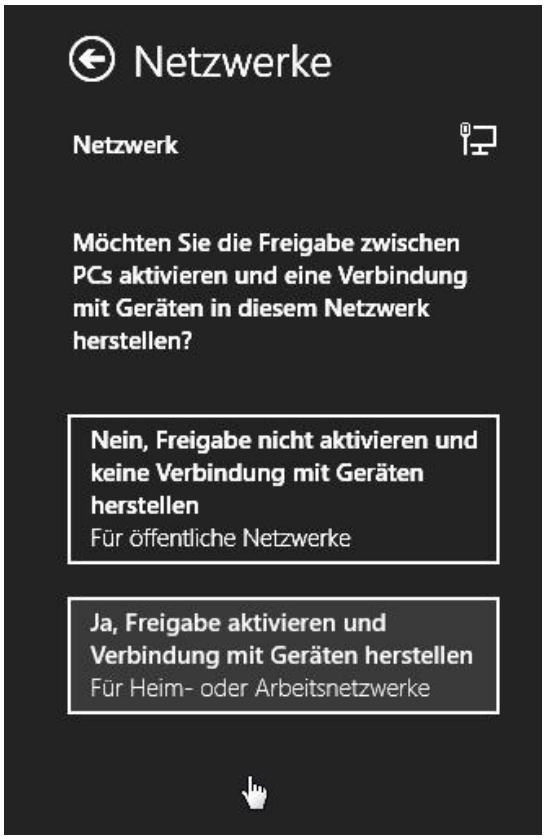
Durch Klicken auf die Netzwerkart kann sie ausgewählt werden.

Für Windows 8:

Vom Desktop aus:

- Linksklick auf das Netzwerkzeichen
- Es öffnet sich rechts die Netzwerkleiste

- Rechtsklick auf Verbunden
- Und auf das aufgehende Popup klicken.



- Nun kann man zwischen öffentliche Netzwerke oder Für Heim- oder Arbeitsnetzwerke auswählen.

Ändert diese Einstellung beim zweiten Durchgang auf «öffentliches Netzwerk».

Diskutiert die Ergebnisse in der Gruppe.

Firewall

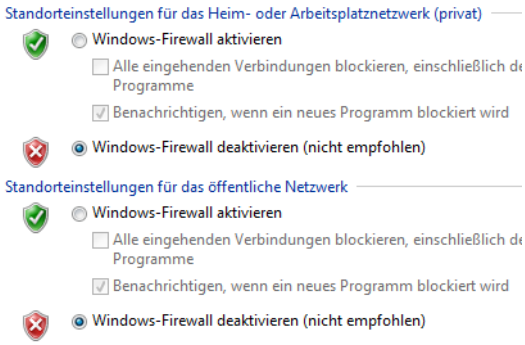
Führt die letzte Übung mit eingeschalteter bzw. ausgeschalteter Firewall durch.

Unter Windows 7:

Start – Systemsteuerung – Windows-Firewall. Links oben findet man die Schaltfläche

.

Deaktiviere die Firewall für alle Netzwerke:



Was stellt ihr fest? Welche Aufgabe hat die Firewall?

Anmerkung:

Mit Zenmap können auch ganze Netzwerke gescannt werden:

Bsp. Eingabe 192.168.1.0/24

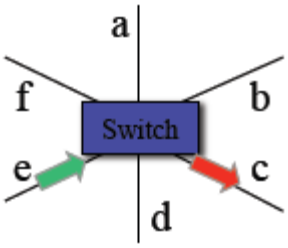
Das bedeutet, dass die ersten drei Byte (3x8bit=24bit) das Netzwerksegment festlegen.

Hier wird also 192.168.1.1-192.168.1.255 durchforscht.

08_ Arbeitsblatt Warriors of the net – Fragen zum Film

1. Welche Aufgaben hat der Router?

2. Was macht der Switch? Das Bild könnte dir helfen.



3. Was passiert mit Datenpaketen, die nicht ankommen?

4. Im Zusammenhang mit der Firewall wird im Film von Eingängen gesprochen. Wie heissen die Eingänge in der Fachsprache? _____

5. Wozu dient der Eingang 80? _____

6. Wozu dient der Eingang 25? _____

09_Arbeitsblatt ARP Cache Poisoning - Man-in-the-middle-attack

Achtung!

Dieses Arbeitsblatt befähigt dich, sensible Daten wie Benutzernamen und Kennwörter im Netzwerk abzufangen.

Ohne Wissen und Billigung der betroffenen Person ist diese Handlung strafbar!

Es geht hier nicht darum, dich zu einem Cracker auszubilden!

Vielmehr sollst du auf die möglichen Risiken und Nebenwirkungen im Umgang mit dem Internet sensibilisiert werden und Schutzmassnahmen erkennen.

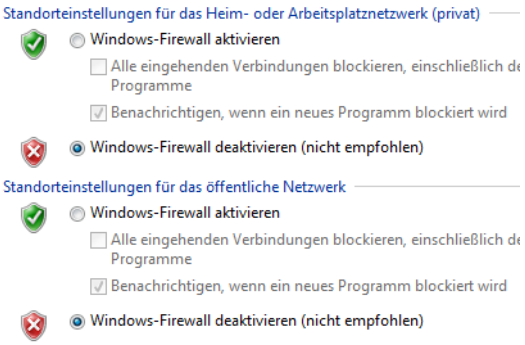
Die Anweisungen auf dieser Anleitung müssen strickte eingehalten werden.

Vorbereitung

1. Bildet 2-er Teams.
2. Schliesst eure Computer ans Internet an.
3. Bestimmt untereinander, welcher PC Opfer und wer Angreifer ist.
4. Im Normalfall erhalten die Computer über den Server der Schule eine IP.
   Verantwortlich dafür ist das DHCP, das Dynamic Host Configuration Protocol.
   Bestimmt die IP der Geräte und tragt die Nummern hier ein:
   IP Opfer: _____
   IP Angreifer: _____
5. Das Opfer soll sich als erstes die eigene ARP-Tabelle anschauen und speichern (alternativ ARP-Tabelle offen lassen oder Screenshot machen)
6. Microsoft Security Essentials respektive Windows Defender und auch andere Antivirensoftware reagieren sofort bei der Installation von „Cain & Abel“ und melden ein HackTool.
   Deaktiviere auf dem Angreifer-PC die Antiviren-Software. Sollte das nicht möglich sein, dann deinstalliere sie.
   Windows 7: Start – Systemsteuerung – Programme und Funktionen
   Windows 8: Windows Defender öffnen – Register Einstellungen – Administrator – Haken bei Windows Defender aktivieren entfernen.

7. Deaktiviere auf dem Angreifer-PC die Firewall. Nur so ist Cain & Abel voll funktionsfähig. Unter Windows 7: Start – Systemsteuerung – Windows-Firewall. Links oben findet man die Schaltfläche 

. Deaktiviere die Firewall für alle Netzwerke:



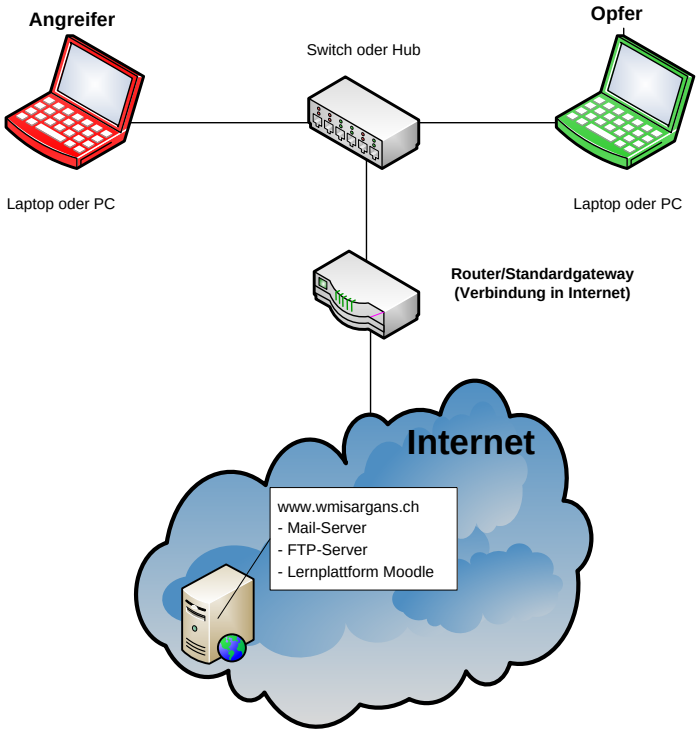
Windows 8: einfach Firewall eingeben und dann sieht es so aus wie bei Windows 7.

8. Installiert das Programm „Cain & Abel“ (http://www.oxid.it/). Im Schulnetz ist die Download-Seite im Normalfall gesperrt. Die Installationspacket ist auf dem gemeinsamen Netzlaufwerk bereitgestellt.

   Grundsätzlich kann dem Assistenten bei der Installation gefolgt werden. Die Installation erfordert zusätzlich die Installation von WinPcap. Wenn Wireshark auf dem PC installiert ist, dann ist dieses Packet, welches den Zugriff auf die Netzwerkkarte ermöglicht, bereits installiert.

9. Eure Netzwerksituation sieht nun so aus (s. unten). Über einen Switch seid ihr über den Verbindungsknoten eurer Schule mit dem Internet verbunden. Dieser Knoten wird oft als Modem oder Router bezeichnet. In den Netzwerkeinstellungen ist seine IP aber unter dem Begriff Standardgateway zu finden. Dieser Begriffswirrwarr ist sehr verwirrend. Finde gleich mit ipconfig die IP des Gateways heraus und notiere sie hier.

   IP Router: _____

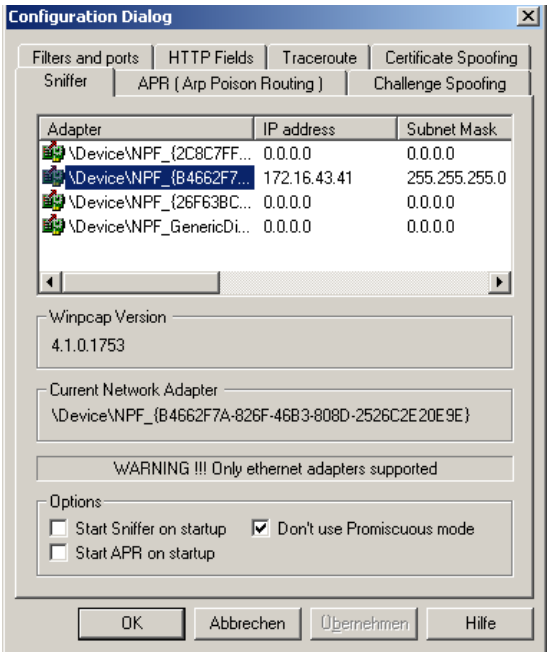


Es ist zudem gut möglich, dass du auch den hier abgebildeten Switch nicht direkt siehst. Oft ist der Switch in einem Kasten untergebracht und nur die Netzwerkkabel führen zu den einzelnen Arbeitsplätzen.
Für eure Arbeit steht ein Server im Internet zur Verfügung: wmisargans.ch
Darauf ist ein Mail-Server, ein FTP-Server und die Lernplattform Moodle eingerichtet. Ein FTP-Server stellt einfach eine Dateiablage im Internet zur Verfügung. Man kann darauf ganz einfach mit dem Windows Explorer zugreifen.

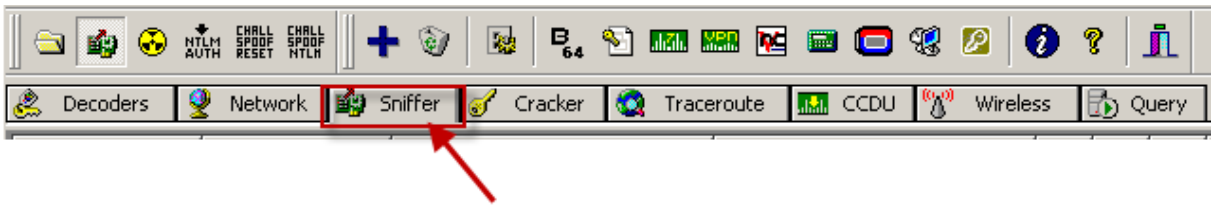
Der Angriff

1. Cain & Abel starten
2. Auf Configure 

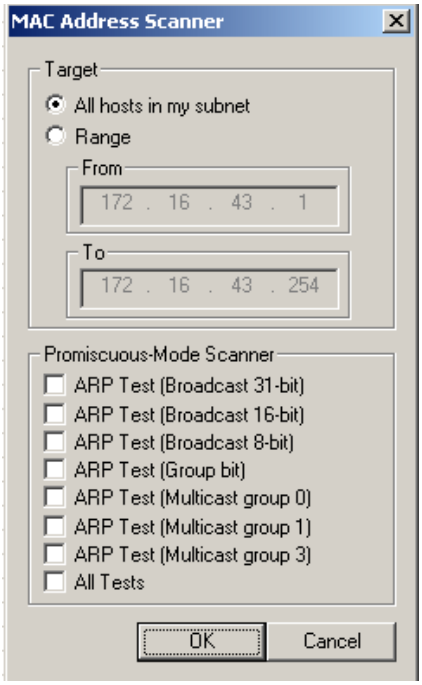
klicken.
3. Wähle im Register Sniffer den Netzwerkadapter aus, bei dem deine IP steht (IP Angreifer).In diesem Beispiel 172.16.43.41. Bestätige mit OK.



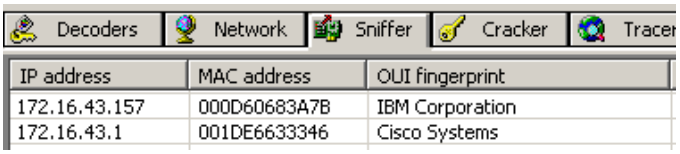
4. Sniffer  starten
5. In Register Sniffer wechseln



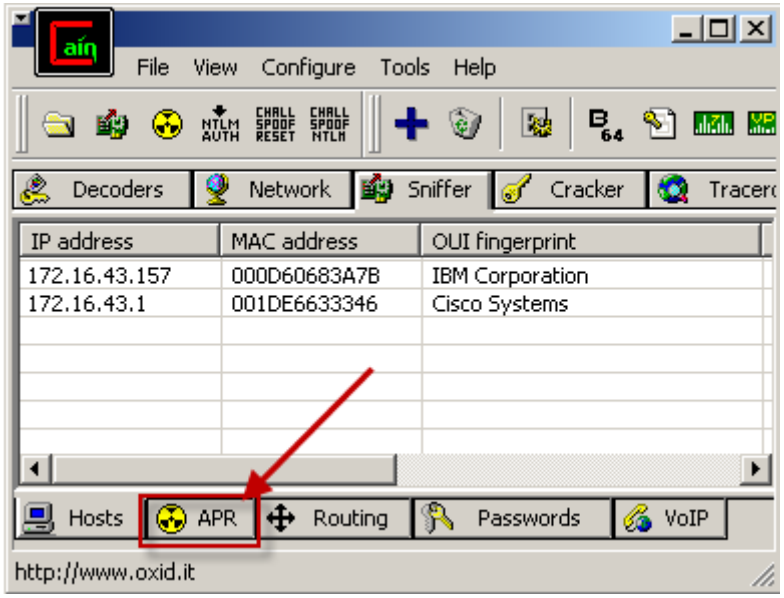
6. Auf  klicken und Netzwerk nach potentiellen Opfern durchsuchen. Mit OK starten.



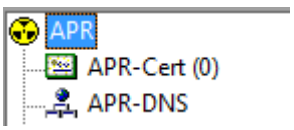
In diesem Beispiel zeigt es die IP und die MAC-Adresse des Opfer-PCs und des Routers (mit der 1 am Schluss) an.



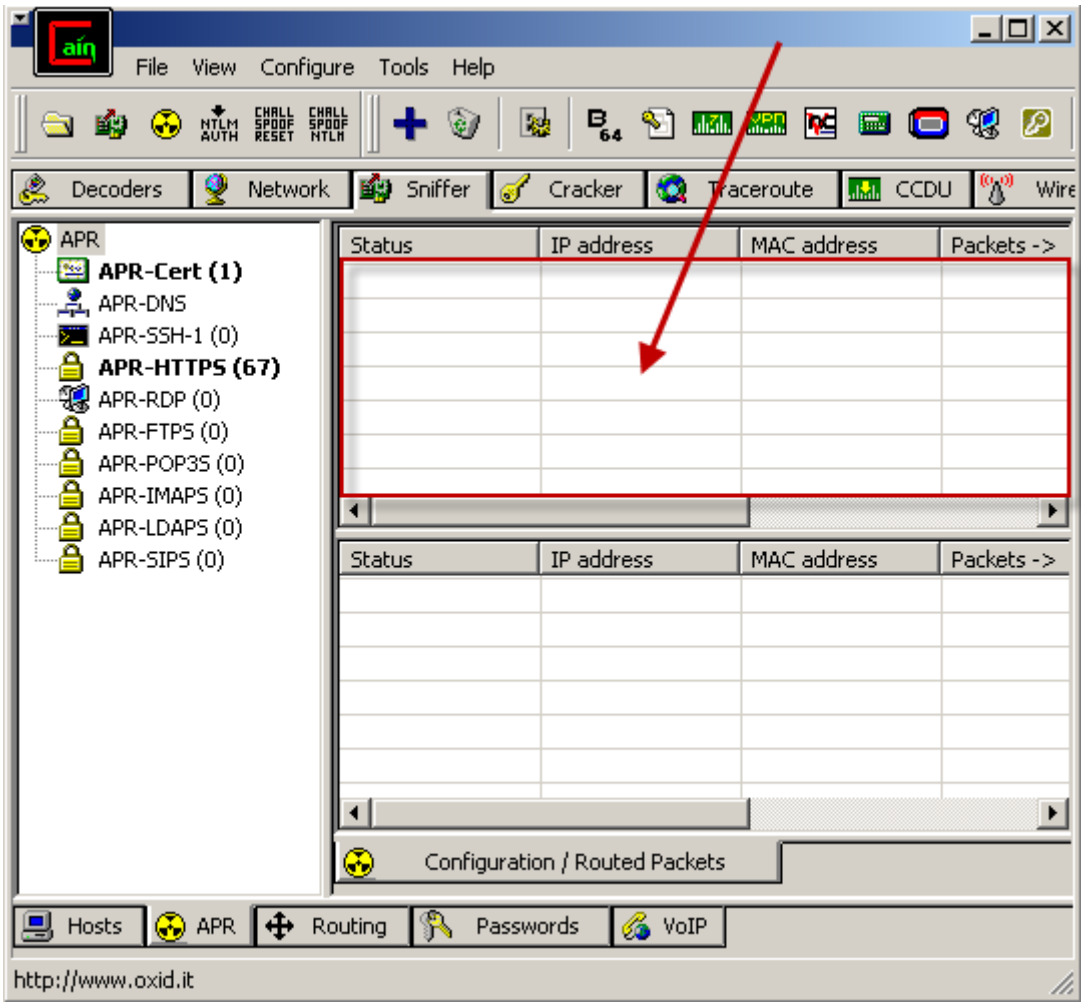
7. In Register APR wechseln:



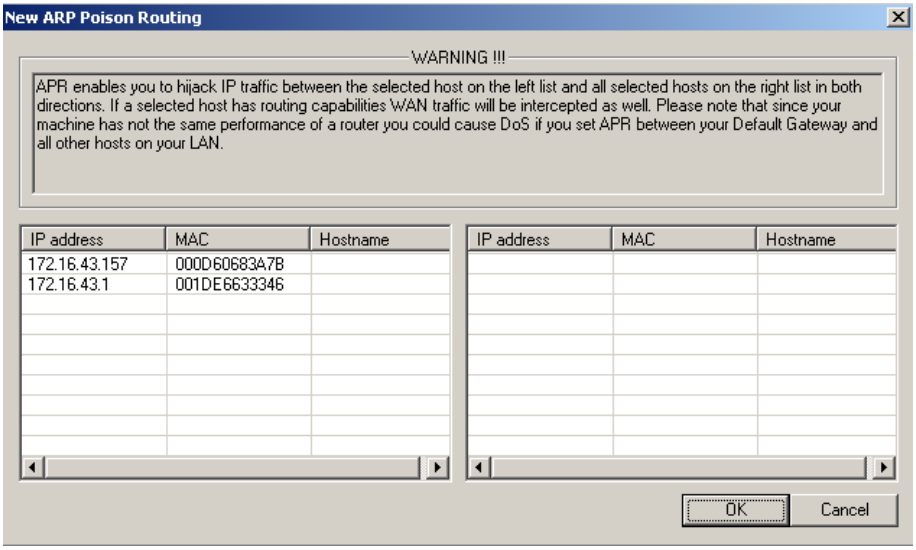
8. Darauf achten, dass im folgenden Fenster APR an der Wurzel des Baumes angewählt ist.



9. In rot eingerahmten Bereich klicken:

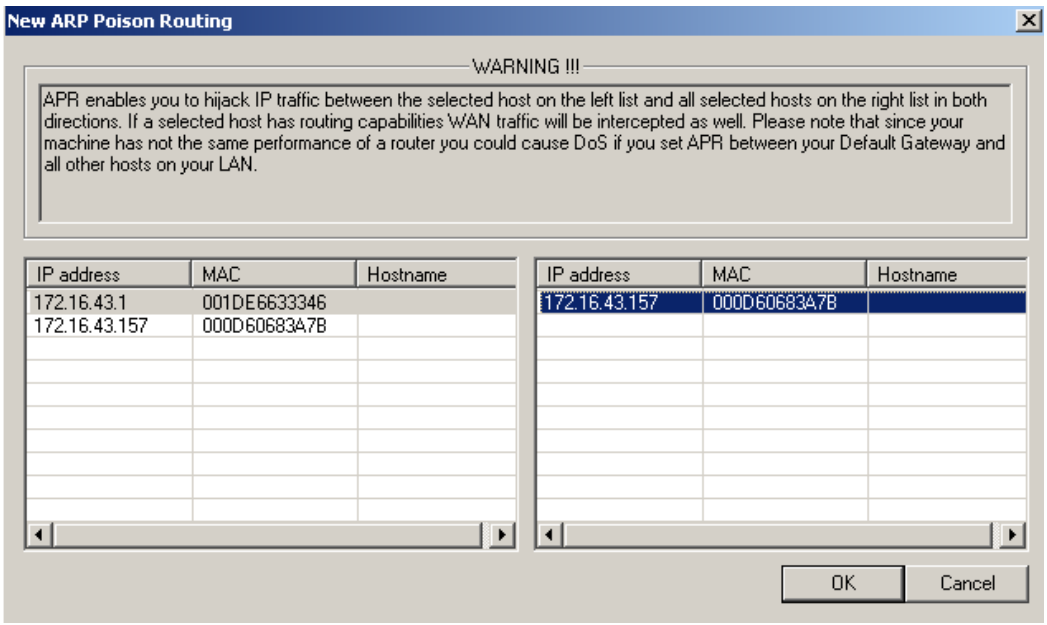


10.  wählen – das folgenden Fenster erscheint:



11. Nun links die IP des Routers (Standardgateway) auswählen. In diesem Beispiel ist das 172.16.43.1.

12. Sobald auf der linken Seite der Router bestimmt ist, werden alle restlichen IPs auf der rechten Seite angezeigt:

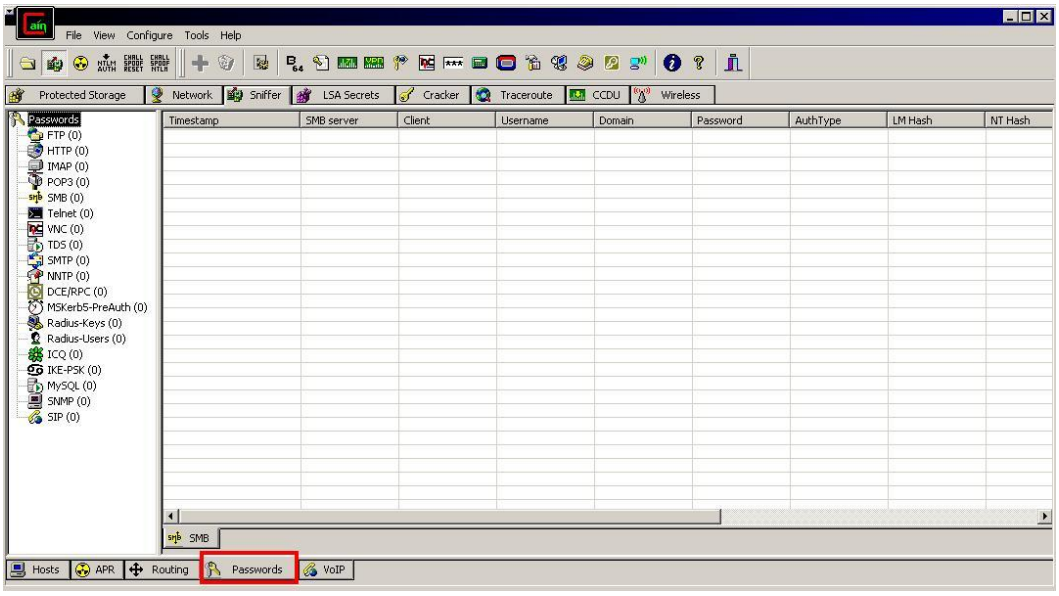


13. Jetzt kann rechts der Opfer-PC ausgesucht werden. Achte auf die richtige IP! OK drücken.

14. Sobald nun in der Symbolleiste  angeklickt wird, startet die Man-in-the-middle-attack.

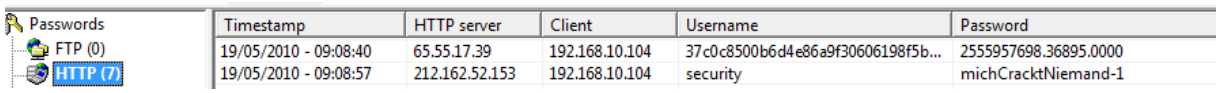
Kurz gesagt, die Daten vom Router laufen über den eigenen Angreifer zum Opfer und die Daten vom Opfer laufen über den gleichen Angreifer zum Router. Bei Erfolg steht der Status dann auf "Poisoning".

15. Cain fängt somit den ganzen Traffic ab und teilt z.B. Passwörter in die dazu passenden Sektionen auf:



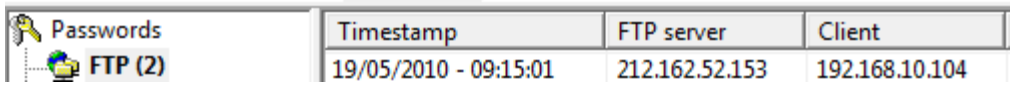
16. als nächstes **muss man mit dem Opfer-PC arbeiten.**
17. Sehr populär im Bildungsumfeld ist die Lernplattform Moodle. Meistens muss man sich für die Nutzung der Lernmodule auf der Plattform anmelden und sehr oft verwenden die Benutzer überall die gleichen Kennwörter!

    Probiere selbst. Melde dich auf http://moodle.wmisargans.ch mit dem Benutzernamen „security“ und dem Kennwort „michCracktNiemand-1“ an. Überprüfe auf dem Angreifer, ob er sich jetzt auch anmelden könnte.



18. Nun greifen wir per FTP, dem File Transfer Protokoll, auf eine Dateiablage im Internet zu. Öffne den Windows Explorer. Gib in die Adresszeile ftp.wmisargans.ch ein.

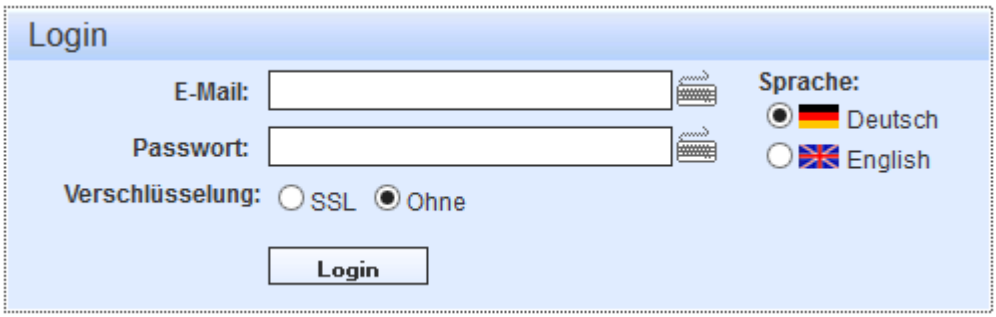
    Bei der folgenden Eingabeaufforderung ist der Benutzername „sarganschsecurity“ und das Kennwort ist einmal mehr „michCracktNiemand-1“.



    Du darfst dir ruhig den Inhalt der gefundenen Datei anschauen.

19. Webmail: Besuche die Seite http://webmail.all-inkl.com

    Das ist die Loginseite eines Online-Maildienstes wie Gmail oder Yahoo usw.



    Wähle hier die Option Ohne und gib Benutzernamen und Kennwort von oben ein.

    Findest du nun in Cain & Abel die Daten? _____

    Und was passiert, wenn du die Option SSL aktivierst? _____

    _____

    Wofür steht SSL?_____

20. Als letztes sollt ihr euch bei den untenstehenden Diensten anmelden. Dabei spielt es keine Rolle, ob ihr auch sonst Nutzer dieser Dienste seid und ein Nutzerkonto besitzt. Ihr könnt die Anmeldefelder auch mit fiktiven Daten füllen.

    http://www.facebook.com/ Anmeldung bei Facebook

    https://accounts.google.com/ Anmeldung bei Google (z.B. für GMail)

    Was zeigt dir Cain & Abel nach diesem Versuch?

Verarbeitung

Bespreche mit deinem Teamkollegen resp. deiner Teamkollegin die folgenden Fragen und halte die Antworten schriftlich fest.

1. Untersucht die ARP-Tabelle des Opfers. Was fällt dir auf? Vergleiche sie mit der ursprünglichen ARP-Tabelle.

2. Versuche zu erklären, wie es möglich ist, dass der Angreifer alle diese Daten mitlesen kann? Warum gehen die Daten über den Computer des Angreifers?

3. Weshalb können die Daten im Klartext gelesen werden?

4. Gegen welchen der oben durchgespielten Angriffe würde dich eine Firewall schützen?

5. Du hast in den vielen verschiedenen Versuchen sicher erkannt, dass wenn man unbedacht das Internet mit all seinen Möglichkeiten nutzt, ein recht grosses Risiko eingeht. Der letzte Versuch sollte dir gezeigt haben, dass die Sicherheit massgeblich erhöht werden kann. Beim Anmelden auf Facebook und Google konntet ihr keine Kennwörter abfangen. Versuche zu erklären, warum das nicht möglich war.

6. Kevin Mitnick, einst der meist gesuchte Mann des FBI, weil er zig Netzwerke gehackt hatte, erkannte schon vor über 20 Jahren, dass es nicht primär technisches Know-how braucht, um erfolgreich in Computersysteme einzudringen. Viel einfacher ist es die Schwachstelle Mensch auszunutzen. (Mitnick & Simon, 2006)
   Was können wir alle tun, um im Umgang mit modernen Technologien die Sicherheit zu erhöhen?

   _____

   _____

   _____

   _____

   _____

   _____

   _____

7. **Schliesslich auch noch ein, zwei technische Fragen:**
   Finde heraus auf welcher Netzwerkschicht die Protokolle FTP und DHCP eingeordnet werden.

   _____

   Welche Ports nutzen sie?_____

8. Untersuche mit Hilfe des Internets den Unterschied zwischen Router und Gateway.

   _____

   _____

   _____

   _____

Quellen:

Mitnick, K., & Simon, W. (2006). *Die Kunst der Täuschung - Risikofaktor Mensch.* Heidelberg: mitp .

TrEaZeR. (24. Mai 2007). *Cain & Abel im WLAN - So gehts*. Abgerufen am 19. Mai 2010 von Wardriving-Forum.de: http://www.wardriving-forum.de/forum/showthread.php?t=62096