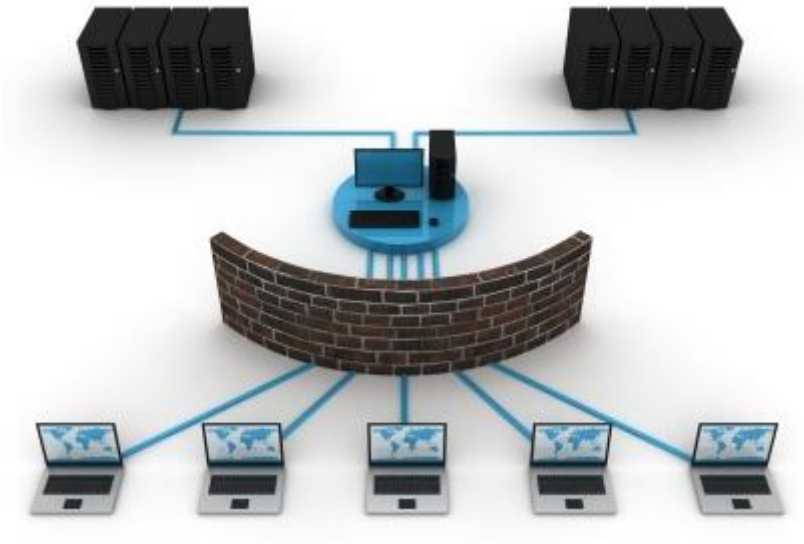
Lösungen

Grundlagen der Netzwerktechnik

Sicherheitsaspekte im LAN



Übersicht

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?
   Die IP ist eine im jeweiligen Netzwerk eindeutige Nummer. Wie beim Telefon macht sie es möglich, dass Geräte adressiert und erreicht werden können. Sie wird dazu verwendet, Daten vom Sender zum Empfänger zu transportieren. _____
   _____

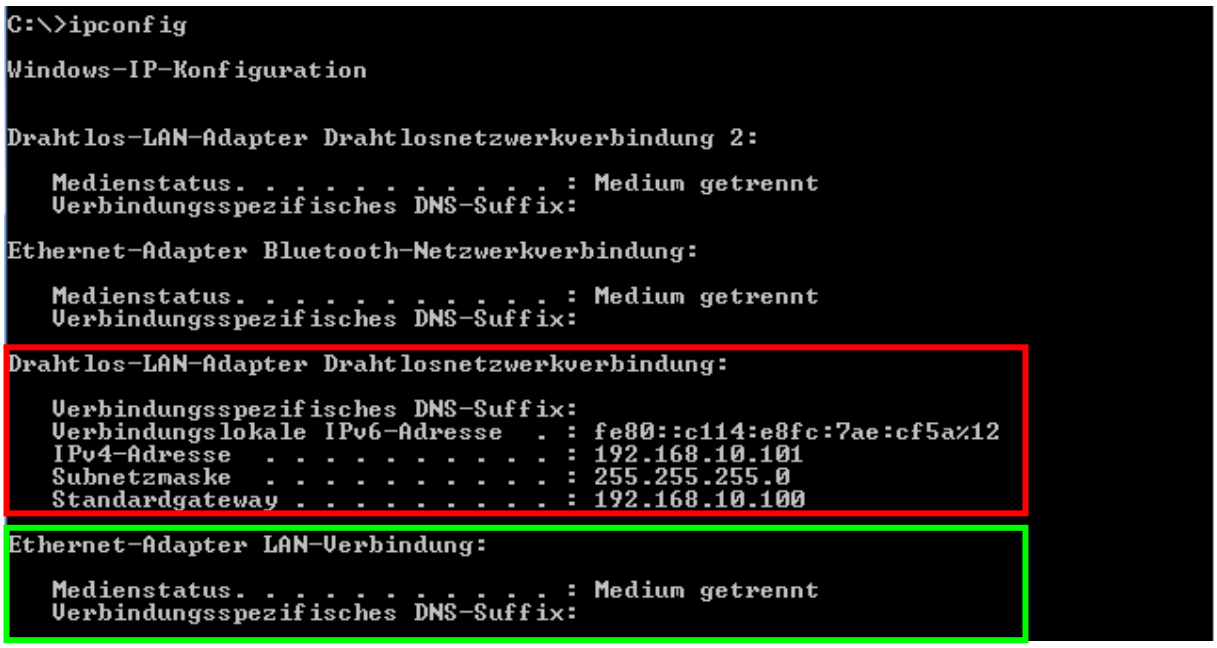
2. Zähle mindestens zwei alltägliche Analogien zur IP-Adresse auf.
   Telefonnummer, AHV-Nummer, Postanschrift, PLZ_____
   _____

3. Wie ist die IPv4 Adresse aufgebaut?
   Aus vier Zahlen, die wiederum je aus 8Bits aufgebaut sind und durch einen Punkt voneinander getrennt sind. Es lassen sich als Zahlen zwischen 0 und 255 darstellen.
   Bsp. 130.094.122.195 Binär: 10000010 01011110 01111010 11000011 _____

4. Worin liegt der grundsätzliche Unterschied zwischen IPv4 und IPv6?
   Im Gegensatz zu IPv4 mit 32 Bit-Darstellung verwendet IPv6 128 Bit. Dadurch lassen sich viel mehr verschiedene IP-Nummern generieren. (2^{128}) _____
   _____

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.
   Es sollte nicht funktionieren, da standardmässig die Firewall ab Windows XP kein ICMP-Echo Request zulässt.
   Diese Option muss in den Optionen der Firewall bewusst aktiviert werden.

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

02_"Hackerparagraf":

Auch die Aufpasser müssen aufpassen

Fragen und Aufgaben zum Text:

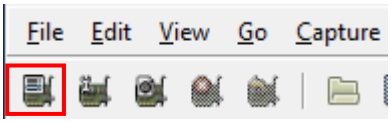
1. Welche Programme werden im Artikel erwähnt, bei denen bereits der Besitz in Deutschland strafbar ist.
   nmap, wireshark, tracert, ping, John the Ripper, BOSS, Tripwire _____

2. Der Artikel beschreibt, dass bereits die Verwendung von Windows in Deutschland problematisch sein kann. Warum?
   Da die vorinstallierten Programme ping und tracert auch zu Missbrauchszwecken eingesetzt werden können. Mit "ping" lässt sich feststellen, ob ein Rechner online, mit "tracert" über welche Wege er zu erreichen ist. _____

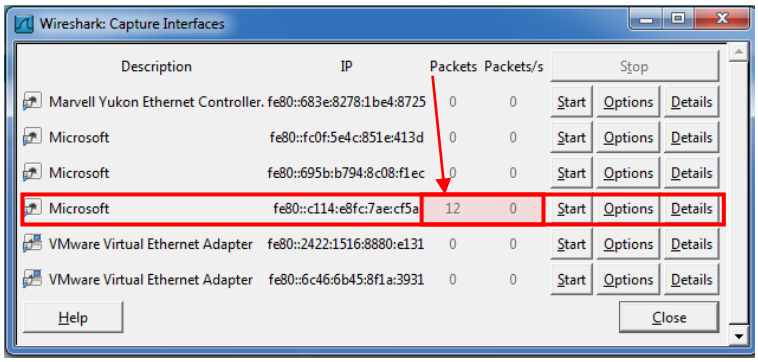
3. Beurteile den Hackerparagafen. Was spricht für und was gegen den Paragrafen?

03_Arbeitsblatt ARP untersuchen mit Wireshark

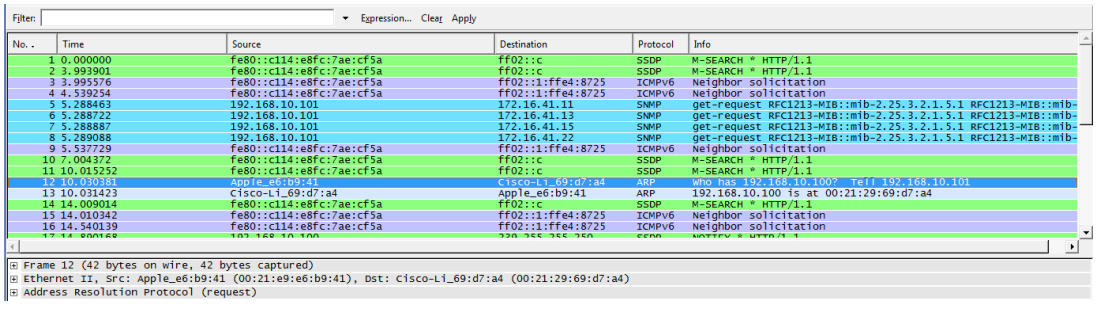
Mitlesen des Netzwerkverkehrs

1. Starte Wireshark
2. Über 

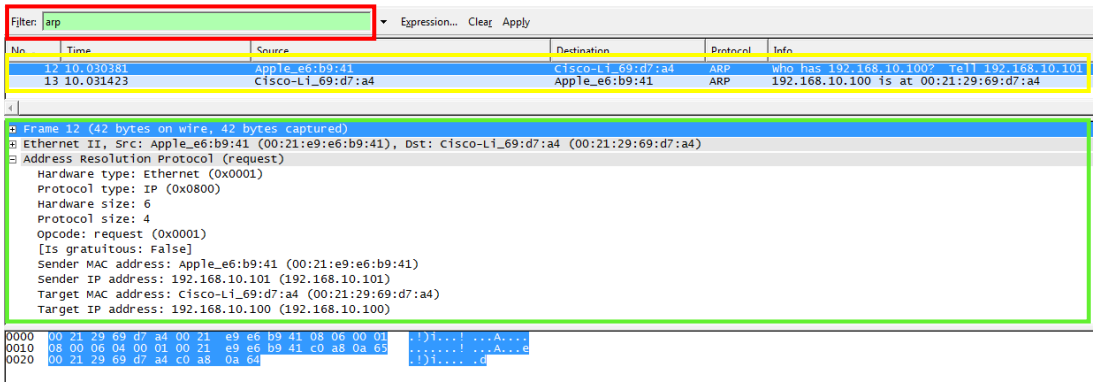
gelangst du in die Übersicht über die verschiedenen vorhandenen Netzwerkschnittstellen auf deinem PC.
3. Anhand der aktuell gezählten Datenpakete, welche über die Schnittstelle transportiert werden, kannst du die aktive Netzwerkkarte erkennen.



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. 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 nun die verschiedenen beteiligten Protokolle. Durch einen Mausklick auf das + werden die Details sichtbar.
9. Beschreibe nun mit deinen Worten den ARP-Protokoll-Ablauf und versuche dein Vorwissen über IP- und MAC-Adressen mit einzubeziehen.

Das Ziel des ARP ist es, von jeder IP im Netzwerk die dazugehörige MAC-Adresse zu erhalten und daraus eine Zuordnungstabelle zu erstellen. Die MAC-Adressen sind deshalb so zentral, da sie im Gegensatz zur IP-Adresse weltweit eindeutig sind und somit erst sicherstellen, dass die Datenpakete das Ziel auch erreichen.

Damit nun die ARP-Tabelle erstellt werden kann, sendet jedes Gerät im Netzwerk an alle Geräte Anfragen im Stil „Wer hat die IP 192.168.10.100, ich habe die IP 192.168.10.101“ aus. Fühlt sich ein Gerät im Netzwerk angesprochen, d.h. es hat die entsprechende IP, dann sendet es an das Anfragegerät seine IP mit der dazugehörigen MAC-Adresse zurück. Die Einträge im ARP-Cache können statisch oder dynamisch sein. Statische Einträge können manuell hinzugefügt und gelöscht werden. Dynamische Einträge werden durch die ARP-Adressauflösung erzeugt.

Jeder dynamische Eintrag bekommt einen Zeitstempel. Ist er nach zwei Minuten nicht mehr abgerufen worden, wird der Eintrag gelöscht. Wird eine Adresse auch nach zwei Minuten noch benutzt, wird der Eintrag erst nach zehn Minuten gelöscht. Ist der ARP-Cache für neue Einträge zu klein, werden alte Einträge entfernt.

Wird die Hardware neu gestartet oder ausgeschaltet, wird der ARP-Cache gelöscht. Es gehen dabei auch die statischen Einträge verloren.

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“?

   Fügt einen Hosteintrag hinzu und ordnet die Internetadresse der physikalischen Adresse zu. Die physikalische Adresse wird durch 6 hexadezimale, durch Bindestrich getrennte Bytes angegeben. Der Eintrag ist permanent.

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?

   Für den angeforderten Vorgang sind erhöhte Rechte erforderlich (Als Administrator ausführen).
   Diese Meldung erscheint ab Windows Vista.

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

   Windows-Button, Suchfeld cmd eingeben. Auf das Programm cmd.exe rechtsklicken und „Als Administrator ausführen“ wählen.

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?
   arp 192.168.10.100 –d d.h. arp –d
7. Versuche nun einen Eintrag einzufügen. Notiere hier deinen genauen Befehl:
   arp 192.168.10.1 00-21-29-68-d6-a3 –s
8. Kontrolliere anschliessend die ARP-Tabelle. Hast du deinen Eintrag gefunden?
9. Was zeigen dir diese Versuche? Notiere dir hier deine Überlegungen:
   Die Versuche zeigen, dass sich grundsätzlich die Zuweisung von MAC- und IP-Adresse beliebig manipulieren lässt. In der Unterrichtseinheit mit Cain & Abel wird genau das ausgenutzt, um den Netzwerkverkehr eines anderen Computers über den Angreifer-PC umzuleiten und dort alles mitzulesen.

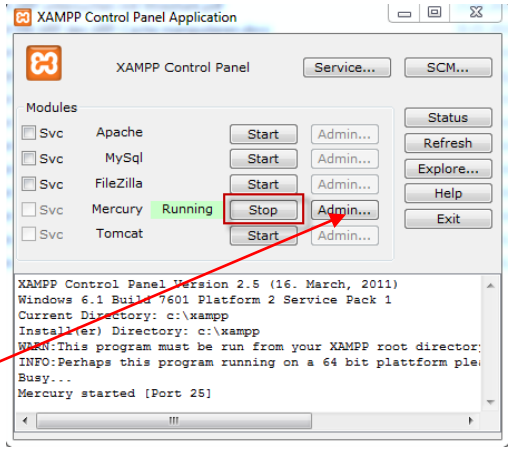
Bespreche deine Notizen mit deinem Banknachbarn.

05_Arbeitsblatt Ports, Dienste und Protokolle

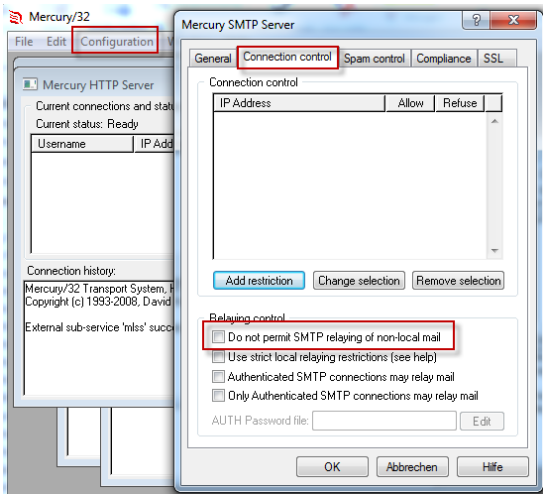
Mail über Telnet

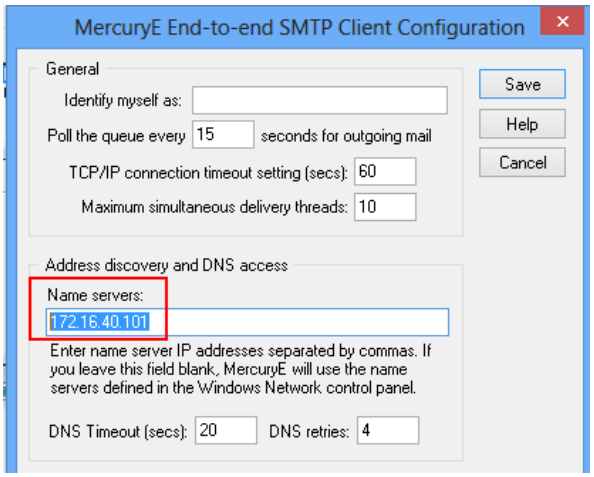
Da die meisten Mailserver umfangreiche Sicherheitsmassnahmen, wie Verschlüsselung, Authentifizierung usw. eingebaut haben, nutzen wir als Testserver einen eigenen Mailserver, den wir direkt auf unseren PCs installieren. Dieser ist dann über den Namen «localhost» (bei Bluewin wäre das «smtpauth.bluewin.ch» und bei Educanet2 «mail.educanet2.ch») 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. Verwende hier als Adresse localhost, das ist der Name deines Rechners.
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
Dateneingeben	
.	«.» 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?

Mit dem Programm telnet ist es einfach möglich Emails zu fälschen und Emails unter falschem Namen zu versenden. Mitunter ein Mittel, um Spam zu generieren.

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	Anwendungen, die ihre Daten versenden wollen, «liegen» in der Anwendungsschicht und nehmen die Dienste der Transportschicht in Anspruch. Sie kümmern sich nicht weiter um die Kommunikation.	http (80), ftp (20,21), smtp (25), nslookup, ping
Transport	Zerstückelung / Segmentierung der Daten. Jedes Segment erhält Ziel- und Quelladresse sowie eine Laufnummer	TCP-Paket, TCP, UDP
Netzwerk	Ist für die korrekte Weiterleitung der Datenpakete zuständig. Die entsprechende IP-Adresse wird dem Paket angehängt	ICMP, IP
Sicherung	Ist für die fehlerfreie Übertragung zuständig. Fügt Prüfziffern hinzu und versendet verlorengegangene Pakete neu. Hängt die MAC-Adresse ans Paket.	ARP
Physikalische	Sorgt dafür, dass die Datenpakete über die physikalische Leitung übertragen werden.	Bluetooth, LAN, W-LAN

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?

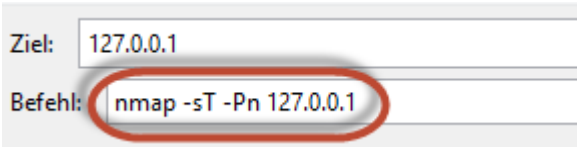
- Nslookup (Name Server lookup) macht die Auflösung zwischen Webadresse und IP-Adresse. Dabei benutzt das Programm den DNS-(Domain Name Service) Dienst. Der DNS-Dienst ist ein weltweiter Verzeichnisdienst, der die vergebenen Namen verwaltet. Der DNS-Dienst gehört zur Anwendungsschicht.

- > nslookup nzz.ch → Server: nzz.ch, Address: 212.71.125.130

07_Arbeitsblatt Portscan

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.

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
110	pop3, Übertragungsprotokoll, über welches ein ClientE-Mails von einem E-Mail-Server abholen kann
23	telnet, Netzwerkprotokoll basierend auf zeichenorientiertem Datenaustausch.

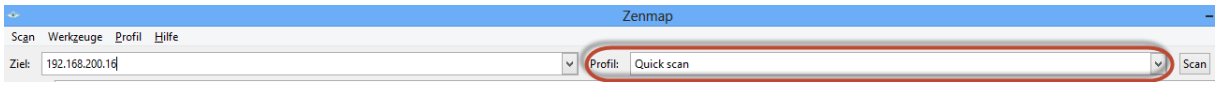
445	The SMB (Server Message Block) protocolisusedamongotherthingsforfilesharing
1025	**Network File System** ist ein von Sun Microsystems entwickeltes Protokoll, das den Zugriff auf Dateien über ein Netzwerk ermöglicht. Dabei werden die Dateien nicht wie z. B. bei FTP übertragen, sondern die Benutzer können auf Dateien, die sich auf einem entfernten Rechner befinden, so zugreifen, als ob sie auf ihrer lokalen Festplatte abgespeichert wären.
135	msrpc Microsoft Remote Procedure Call ->Aufruf einer fernen Prozedur Die am weitesten verbreitete Variante ist das *ONC RPC (Open Network Computing Remote Procedure Call)*, das vielfach auch als Sun RPC bezeichnet wird. ONC RPC wurde ursprünglich durch Sun Microsystems für das *Network File System (NFS)* entwickelt. Ablauf: Die Kommunikation beginnt, indem der Client eine Anfrage an einen bekannten Server schickt und auf die Antwort wartet. In der Anfrage gibt der Client an, welche Funktion mit welchen Parametern ausgeführt werden soll. Der Server bearbeitet die Anfrage und schickt die Antwort an den Client zurück. Nach Empfang der Nachricht kann der Client seine Verarbeitung fortführen.

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

Portscan des Nachbarn

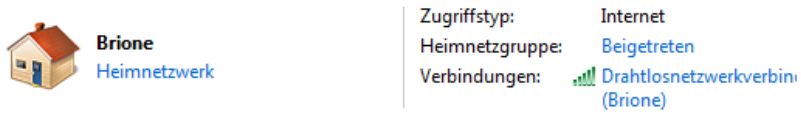
Bildet eine Zweiergruppe und tauscht eure IP-Adressen aus. Führt einen Portscan des Nachbarn durch.

Verwendet hier als Einstellung Quick Scan:



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

Start – Systemsteuerung – Netzwerk- und Freigabezenter



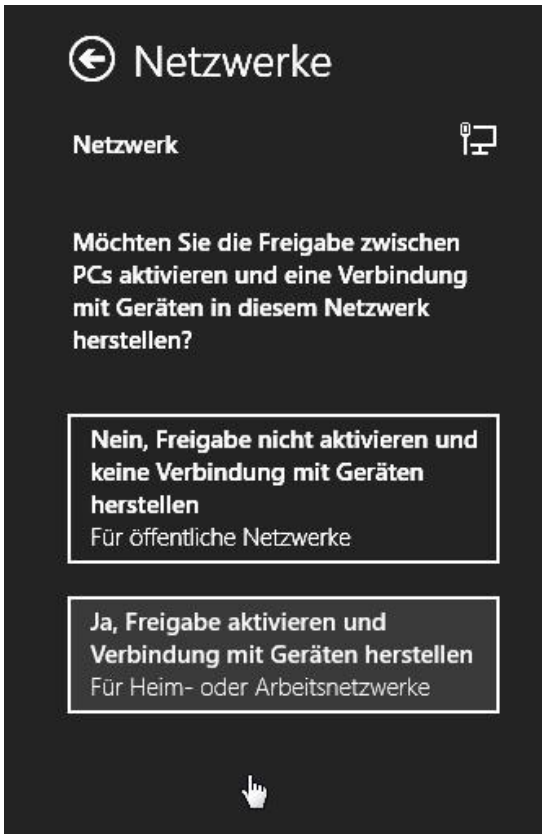
Durch Klicken auf die Netzwerkart kann sie ausgewählt werden.

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.

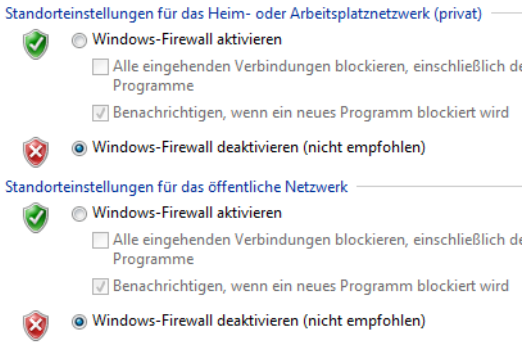
Firewall

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?

Die Firewall verwaltet die Ports und lässt entweder Datenverkehr zu oder blockiert ihn. _____

Durch das Deaktivieren der Firewall werden mehr Ports sichtbar. _____

_____

_____

_____

_____

_____

_____

_____

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.

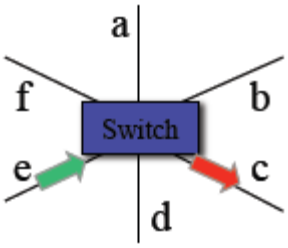
08_Arbeitsblatt Warriors of the net – Fragen zum Film

1. Welche Aufgaben hat der Router?

   Schaut nach, welche Adresse das Datenpaket hat und schickt es allenfalls auch an ein anderes Netzwerk.

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

   Der Switch ist ein Netzwerkknoten, der die IP-Pakete auf ihren Weg leitet.



3. Was passiert mit Datenpaketen, die nicht ankommen?

   Wenn nicht rechtzeitig eine Quittung für das Paket eintrifft, wird ein Ersatzpaket gesendet.

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

5. Wozu dient der Eingang 80? Webserver

6. Wozu dient der Eingang 25? Mailsserver

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

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.

   Es werden in der ARP-Tabelle zwei identische MAC-Adressen aufgeführt. Die MAC-Adresse des Angreifers ist auch als MAC-Adresse des Gateways eingetragen.

2. Warum gehen die Daten des Opfers über den Computer des Angreifers?

   Gemäss ARP-Tabelle des Opfers entspricht die MAC-Adresse des Gateways der MAC-Adresse des Angreifers. Entsprechend werden alle Datenpakete über den Angreifer gesendet die eigentlich für den Router bestimmt sind. Das Programm «Cain & Abel» ist in der Lage die ARP-Tabelle des Opfers entsprechend zu manipulieren. Der Angreifer liest die Informationen und leitet sie dem richtigen Router weiter. Kommt eine Antwort aus dem Internet zurück, so wir sie vom Router an den Angreifer gesendet. Dieser kann wieder alle Informationen lesen und sie anschliessend dem Opfer zustellen. Dieser meint, dass die Informationen vom Router kommen.

3. Erforsche, wie es möglich ist, dass der Angreifer einen falschen Eintrag in die ARP-Tabelle des Opfers schreiben kann. Man bezeichnet übringens diese Art des Angriffes als ARP Cache Poisoning oder ARP-Spoofing.

   Um den Datenverkehr zwischen Host A und Host B abzuhören, sendet der Angreifer an Host A eine manipulierte ARP-Nachricht. In dieser ist nicht seine eigene IP-Adresse, sondern die von Host B enthalten, so dass Host A zukünftig die Pakete, die eigentlich für Host B bestimmt sind, an den Angreifer sendet. Dasselbe geschieht mit Host B, so dass dieser Pakete statt direkt an A nun ungewollt zum Angreifer sendet. Der Angreifer muss nun die von

A und B erhaltenen Pakete an den eigentlichen Empfänger weiterleiten, damit eine abhörbare Verbindung zustande kommen kann. Ist dies geschehen, so arbeitet der Angreifer unbemerkt als Zwischenstelle. Dieser Angriff wird als «Man in the middle» bezeichnet.

4. Weshalb können die Daten im Klartext gelesen werden?

Die Daten sind nicht verschlüsselt.

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

Eine Firewall nützt in dieser Situation nichts. Trotz Firewall ist die Manipulation der ARP-Tabelle des Opfers möglich.

6. 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.

Die Daten werden verschlüsselt. Bei Facebook und Google wird das Protokoll https („s“ steht für secure) verwendet. Dabei sind die Protokolle SSL (Secure Socket Layer) resp. TLS (Transport Layer Security) für die Verschlüsselung zuständig.

7. 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?

vertrauenswürdige Netze verwenden; öffentliche Netze meiden; die Nutzung jedes offenen (d.h. nicht verschlüsselten) WLANs ist risikobehaftet; das automatische Verbinden der Smartphone mit offenen Netzwerken unterbinden;…

8. **Schliesslich auch noch ein, zwei technische Fragen:**

   Finde heraus auf welcher Netzwerkschicht die Protokolle FTP und DHCP eingeordnet werden.

   Beide auf der Anwendungsschicht

   Welche Ports nutzen sie? FTP 21, DHCP 67 und 68

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

   Ein Router leitet IP-Pakete zwischen verschiedenen Netzwerksegmenten weiter. Ein Gateway ist ein Protokollvermittler. Es kann zwischen verschiedenen Protokollen übersetzen und somit Netzwerke mit unterschiedlichen Protokollen verbinden.

   Aus dieser Erklärung folgt, dass in diesem Beispiel viel mehr von einem Router die Rede sein müsste als von einem Gateway.