Penetration-Testing für Einsteiger

9. November 2010

Outline

Ziel

- Das heutige Computerlabor will Euch das Thema Sicherheit näher bringen
- Es will zeigen, dass Ihr in einem einem Netzwerk (i.d.R.) nicht anonym seid
- Es will auch zeigen, wie Angreifer vorgehen

Warum?

- IT-Systeme sind nicht grundsätzlich sicher
- Entwickler machen Fehler (darum gibt es immer wieder Sicherheitsupdates)
- Benutzer konfigurieren ihre Rechner falsch
- Benutzer sind zuwenig vorsichtig (sh. den Erfolg von Phishing)
- Sicherheit wird vielfach immer noch als Produkt und nicht als Prozess gesehen
- Eine Firewall zu kaufen heisst noch lange nicht, dass damit alle Probleme erledigt sind...

Warum?

- Sicherheit hängt also stets von verschiedenen Faktoren ab
- Unerfahrene Leute stehen vor einem grossen Berg an Dingen, die sie beachten müssten...
- ... es dann aber (vorallem in Firmen) trotzdem nicht machen
- Deshalb gibt es seit wenigen Jahren den Beruf des «Penetration Testers», der im Auftrag nach Sicherheitslücken und Schwachstellen sucht
- In Anlehnung an diesen Beruf hat das Computerlabor von heute seinen Namen bekommen

Beispiel I: WEF-Hack

- In 2001 wurde das WEF erfolgreich angegriffen
- Das WEF hat persönliche Daten ihrer Teilnehmer (Telefon- und Kreditkartennummern, Adressen, und mehr) in einer Datenbank auf einem MS-SQL-Server gespeichert
- Der Administrator hat vergessen, dass Administratorenpasswort von MS-SQL zu ändern und beliess es beim Default-Passwort
- Jemand hat begonnen, sich das WEF-Netz näher anzusehen und hat diesen Datenbankserver gefunden (von aussen, denn der Server war vom Internet her erreichbar)
- Dann war es ganz einfach: Dokumentation von Microsoft nach dem Standardpasswort von MS-SQL absuchen und ausprobieren...

Beispiel I: WEF-Hack

- Dies alles braucht gar nicht mal soviele technische Kenntnisse
- Die Zeitung berichteten auch entsprechend darüber

Die Microsoft-Datenbank des Wef erlaubt bei naiver Installation jedem klugen Achtjährigen den Zutritt

`http://www.woz.ch/archiv/old/01/12/617.html`

Beispiel I: WEF-Hack

[...] gelang es dem Hacker-Kollektiv «Virtual Monkeywrench», praktisch die gesamte interne Wef-Datenbank mit über 102 000 Namen zu entführen: Daten von Shimon Peres' Flugplan bis zu Arafats Kreditkartennummer.

[...] (der Schaden durch Umtriebe nach dem Hack - so Wef-Direktor André Schneider - liegt bei zirka 200 000 Franken)

Beispiel I: WEF-Hack

Ihr auch vom Wef benutztes Datenbankprogramm «Micosoft SQL Server» lässt sich in der Version 7.0 anstandslos installieren - ohne das Passwort zu ändern. Zwar gibt es eine Warnung im Handbuch, aber keine bei der Installation. Damit bleibt der Benutzername auf «sa», das Passwort «» (Return) und zusätzlich der Port 1433 offen[...]

[...] Zu allem Überfluss garantiert dieser Zugang Spurlosigkeit: Aufgezeichnet werden nur alle NICHT erfolgreichen Eindringversuche.

Beispiel II: Stuxnet

- Stuxnet ist ein Computerwurm, der im Juli 2010 das erste Mal entdeckt wurde
- Er nutzt Sicherheitslücken in Windows um sich zu verbreiten
- Diese Lücken waren zu diesem Zeitpunkt unbekannt und konnten deshalb nicht schnell behoben werden
- Zusätzlich nutzt Stuxnet gestohlene Signaturen von Realtek und JMicron

Beispiel II: Stuxnet

- Stuxnet konzentriert sich spezifisch auf die Infektion von Systemen mit Siemens WinCC
- Dies ist ein Prozessleitsystem für die Industrie
- Allerdings richtet der Wurm nicht in allen WinCC-Umgebung Schaden an...
- ... Experten gehen davon aus, dass er explizit zur Sabotage von iranischen Atomanlagen produziert wurde
- Und der Wurm hat es in der Tat auch geschafft, solche Systeme zu infizieren

Beispiel II: Stuxnet

- Um so weit zu kommen, muss der Wurm diverse und technisch sehr unterschiedliche Hürden überwinden
- Deshalb kann davon ausgegangen werden, dass Experten verschiedener Fachgebiete an der Entwicklung des Wurms mitgearbeitet haben
- Fachleute nehmen an, dass die Entwicklung des Wurmes einen siebenstelligen Betrag gekostet haben könnte und zudem sehr wahrscheinlich von staatlichen Kreisen initiiert wurde

Beispiel II: Stuxnet

http://www.toonpool.com/cartoons/Stuxnet%20Virus_99539

Beispiel II: Stuxnet

- Auch hier ist übrigens wieder eine Datenbank involviert
- WinCC hat fix einprogrammierte Zugangsdaten für seine Datenbank, die bei jeder Installation identisch sind
- Stuxnet kennt diese Zugangsdaten deshalb und muss eine Hürde weniger nehmen
- Administratoren können diese Lücke selber nicht schliessen, da Siemens die Zugangsdaten ja gerade eben fix einprogrammiert hat :-)

Beispiel II: Stuxnet

- Der Fall zeigt auf, dass ein «Cyberwar» tendenziell eher Realität als Fiktion ist
- Aber: auch die Industriespionage kann durch Angriffe profitieren
- Zudem sind ist auch eine Menge Geld im Spiel
- Es existiert ein Markt für unveröffentlichte Sicherheitslücken
- Wer bspw. in Windows eine ganz neue und unbekannte Sicherheitslücke entdeckt, kann diese für viel Geld verkaufen
- Der Preis bleibt natürlich nur so lange hoch, bis Microsoft einen Patch veröffentlicht hat – deshalb werden die Schwachstellen sehr gut behütet

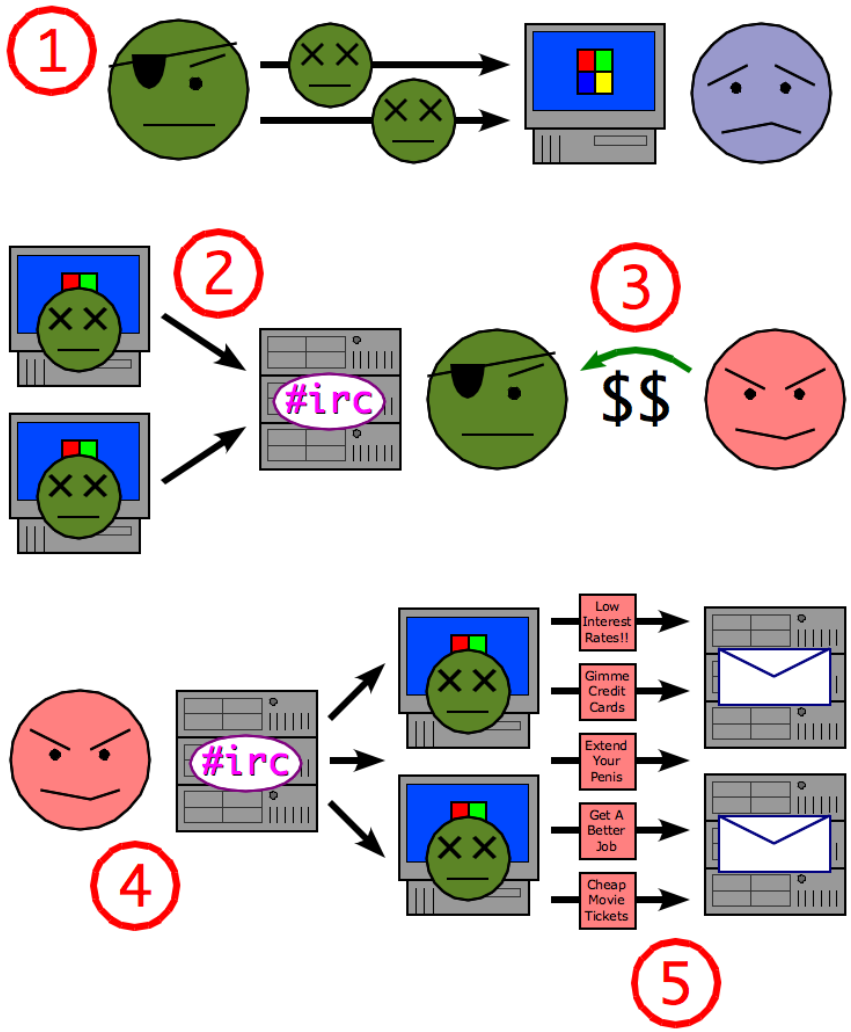
Beispiel III: Conficker

- Ein Wurm aus 2009, mit interessanten Fakten
  - 19. Januar: Über 9 Millionen betroffene Rechner
  - 08. Februar: Es wird bekannt, dass die französische Luftwaffe infiziert und mehrere Tage kaum einsatzfähig war (Dienstanweisungen gab es nur noch per Briefpost :-)).
  - 12. Februar: Microsoft setzt eine Belohnung von 250'000 USD aus, für denjenigen, der Hinweise zur Ergreifung des Conficker Entwicklers liefert
  - 13. Februar: Es wird bekannt, dass hunderte Rechner der Deutschen Bundeswehr infiziert sind

Beispiel IV: Scareware

- Die Angst vor Infektionen wird übrigens auch ausgenutzt
- Scareware ist Software, welche eine Bedrohung vorspiegelt
- Es gibt präparierte Virenscanner, welche eine Infektion vortäuschen und gegen Zahlung einer Gebühr eine Desinfektion anbieten
- Die Zahlung deaktiviert lediglich die Vortäuschung, etwas anderes ist nicht notwendig...
- Genau so tritt es immer wieder auf, dass im Internet angebotene «Cleaning-Tools» eben gerade Schadsoftware enthalten
- Ein Benutzer, der seinen Rechner sauber halten möchte, wird so über den Tisch gezogen

Beispiel V: Botnetze



http://de.wikipedia.org/w/index.php?title=Datei:Zombie-process.png&filetimestamp=20060728173916

Weitere Beispiele

- Die Liste der Beispiele lässt sich noch beliebig fortsetzen
  - Offene WLANs
  - Ausnutzung von Informationen aus sozialen Netzwerken
  - Phishing ist schon seit 2 bis 3 Jahren Dauerthema in den Medien
  - Betrügereien/Abofallen sind auch immer wieder Thema

Andere Betriebssysteme

- Die Beispiele waren sehr Windows-fixiert
- Was aber nicht heisst, dass die anderen Systeme grundsätzlich besser sind
- Experten gehen davon aus, dass die Verbreitung von Systemen wie Linux oder Mac OS X zu klein ist, als dass jemand darin die Möglichkeit sieht, durch Schadsoftware etwas zu erreichen
- Schlussendlich sind auch solche Angriffe nichts mehr als ein Geschäftsmodell (es wird investiert in die Entwicklung, mit dem Ziel etwas bestimmtes zu bekommen)

Legal Disclaimer

- Es lässt sich unterscheiden zwischen «nur ansehen» oder «testen»
- Das «nur ansehen» (wie wir es später bspw. in der WHOIS-Datenbank machen) ist rechtlich unbedenklich
- Das «testen» hingehen gilt juristisch gesehen bereits als Angriff und ist somit Straftat (Ausnahme: Der Eigentümer des zu testenden Systemes hat sein Einverständnis gegeben)
- Deshalb der Disclaimer: Keine Scans oder Tests an fremden Systemen vornehmen
- Denkt auch daran: Wenn ihr Scans oder Tests von einem fremden Internetanschluss aus macht, zieht ihr einen Dritten mit rein

Anonymität in Netzwerken

- Der normale Anwender denkt sich oft, im Internet anonym zu sein
- Dies stimmt jedoch nur bedingt
- Jeder Computer im Netzwerk hat eine eigene IP-Adresse und es lässt sich natürlich prüfen, ob hinter einer bestimmten IP-Adresse ein aktives Gerät steckt
- IP-Adresse: 4 durch Punkte getrennte Zahlen (Octets) im Bereich von 0 - 255; gibt einen Adressraum von 0.0.0.0 - 255.255.255.255
- Dieser Adressraum wird durch eine Netzmaske dann in kleinere Ranges aufgeteilt

Anonymität in Netzwerken

- Es muss zwischen öffentlichen und privaten IP-Adressen unterschieden werden
- Die Öffentlichen sind weltweit eindeutig und in Datenbanken registriert
- Private sind nur für innerhalb eines lokalen Netzwerkes gültig und lauten
  - 10.0.0.0 - 10.255.255.255
  - 169.254.0.0 - 169.254.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255
- Da lokale Netzwerke frei aus diesen Bereichen Adressen wählen dürfen, ist eine private Adresse auch immer nur innerhalb desselben lokalen Netzes eindeutig

Das lokale Netzwerk

- Wir können herausfinden, welchen IP-Adressbereich unser lokales Netzwerk hat
- Wir können prüfen, hinter welcher Adresse ein aktives Gerät steckt

```
1  linux:~$ ifconfig eth0
2  eth0      Link encap:Ethernet  HWaddr 00:24:8c:43:e1:↩
       e2
3            inet addr:192.168.0.50  Bcast:192.168.0.255
4                      Mask:255.255.255.0
5  [...]
6  linux:~$ ipcalc 192.168.0.50/255.255.255.0
7  [...]
8  Network:    192.168.0.0/24
9  HostMin:    192.168.0.1
10 HostMax:    192.168.0.254
11 [...]
```

ICMP Echo Request

- Zu den Standard-Protokollen gehört ICMP
- Dieses definiert einen *Echo Request*, der mit einem *Echo Reply* beantwortet wird
- `ping` sendet solche Echo Requests und zeigt an, ob Echo Replies empfangen wurden
- `ping` kann mit Ctrl-C abgebrochen werden

```
1 linux:~$ ping 192.168.0.1
2 PING 192.168.0.1 (192.168.0.1): 56 data bytes
3 64 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time↩
      =4.437 ms
4 64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time↩
      =4.437 ms
```

ping

- `ipcalc` hat `HostMin` und `HostMax` ausgegeben, die tiefste und höchste Adresse im lokalen Netz
- Es kann also versucht werden, alle diese Adresse anzupingen und zu sehen welche Rechner im lokalen Netz antworten
- Achtung: Ein Rechner kann konfiguriert werden, den Echo Request zu ignorieren - in diesem Fall gibt `ping` keine Ausgabe für diesen Rechner aus
- Deshalb ist dieses Verfahren nicht absolut zuverlässig

ping mit Scanner

- Der `ping` kann auch automatisiert werden mit einem Scanner wie `nmap`
- Dazu wird nmap im Modus *ping scan* gestartet
- Dazu wird die `ipcalc Network`-Ausgabe benötigt

```
1 linux:~$ nmap -sP 192.168.0.0/24
2 Starting Nmap 5.00 ( http://nmap.org ) at ↩
      2010-02-03 10:53 CET
3 Host 192.168.0.1 (192.168.0.1) is up (0.0015s ↩
      latency).
4 Host 192.168.0.12 (192.168.0.12) is up (0.0023s ↩
      latency).
5 Host 192.168.0.50 (192.168.0.50) is up (0.0080s ↩
      latency).
6 Nmap done: 256 IP addresses (3 hosts up) scanned in↩
       2.62 seconds
```

Das Internet

- Die beiden Beispiel waren für das lokale Netzwerk mit privaten IP-Adressen
- Im Internet werden öffentliche Adressen benutzt, die beantragt und registriert werden müssen
- Es gibt den öffentlichen Datenbankservice *WHOIS*, in dem diese öffentlichen IP-Adressen registriert und nachschlagbar sind
- WHOIS wird auch benutzt um die Registrierungsinformationen von Domainnamen zugänglich zu machen
- Im lokalen Netz gab `ipcalc` die `HostMin` und `HostMax` Angabe aus, im Internet können wir dazu WHOIS befragen

IP-Adresse ausfindig machen

- Wenn wir wissen möchten, in welchem Netz ein bestimmter Webserver steht, benötigen wir zuerst seine IP-Adresse
- Dazu müssen wir einen Lookup im DNS durchführen

```
1 linux:~$ host www.bdwm.ch
2 www.bdwm.ch is an alias for herakles.nextage.ch.
3 herakles.nextage.ch has address 62.2.247.215
```

IP-Adresse ausfindig machen

- Wir sehen darin, dass *www.bdwm.ch* ein Alias (`CNAME`) für *herakles.nextage.ch* ist
- Für diesen ist dann eine IP-Adresse eingetragen (`A`)
- Wer näher wissen will, wie DNS funktioniert und was CNAME und A bedeutet:
  `http://de.wikipedia.org/wiki/Domain_Name_System`
  `http://de.wikipedia.org/wiki/Resource_Record`
- Nun können wir 62.2.247.215 mit WHOIS nachschlagen
- Es gibt Dutzende von WHOIS-Servern im Internet, da verschiedene IP-Adressbereiche von unterschiedlichen Organisationen verwaltet werden
- `gwhois` ist praktisch, da es je nach Suchparameter selbstständig herausfindet, welcher WHOIS-Server zu befragen ist

WHOIS Abfrage

```
1  linux:~$ gwhois 62.2.247.215
2  Process query: '62.2.247.215'
3  Query recognized as IPv4.
4  Querying whois.ripe.net:43 with whois.
5  [...]
6  inetnum:          62.2.247.192 - 62.2.247.255
7  netname:          NEXTSTAGE2-NET
8  descr:            nextage GmbH Interaktive Medien
9  descr:            Fanghoefli 14, 6014 Littau
10 country:          CH
11 admin-c:          CL1831-RIPE
12 tech-c:           CAN6-RIPE
13 status:           ASSIGNED PA
14 mnt-by:           AS8404-MNT
15 source:           RIPE # Filtered
16 [...]
```

Erkenntnis aus der Ausgabe

- Wir sehen, dass die BDWM-Webseite offensichtlich von einer Firma namens *nextage GmbH* betrieben wird
- Wir sehen, dass die nextage GmbH ein Netz mit dem Range 62.2.247.192 - 62.2.247.255 nutzt
- Daneben könnte die Firma natürlich noch weitere, zusätzliche Netze besitzen (`NEXTSTAGE2-NET`)
- Die Ausgabe geht aber noch weiter...

Der Provider von nextage

```
1  [...]
2  route:          62.2.0.0/16
3  descr:          cablecom GmbH NOC
4  descr:          CH-8021 Zuerich
5  descr:          Switzerland
6  origin:         AS8404
7  mnt-by:         AS8404-MNT
8  source:         RIPE # Filtered
```

Der Provider von nextage

- So wie es aussieht, gehört der Block von nextage in das Netz 62.2.0.0/16 rein, welches zu Cablecom gehört
- Cablecom hat bei der offiziellen Registrierungsstelle den Block 62.2.0.0/16 (gemäss ipcalc = 62.2.0.0 - 62.2.255.255) registriert
- nextage ist Kunde von Cablecom und hat von Cablecom 62.2.247.192/26 (= 62.2.247.192 - 62.2.247.255) zugewiesen erhalten
- nextage wird wohl nicht von Cablecom loskommen, ohne ihr gesamtes Netz neu numerieren zu müssen

Fazit

- Wir sind in einem Netzwerk gar nicht so anonym wie wir immer denken
- Wir haben mit WHOIS sehr schnell interessante Informationen gefunden und auch sehen können, wer mit wem zusammenarbeitet
- Wir könnten natürlich auch ausprobieren, welche Rechner innerhalb des nextage Netzes auf den `ping` antworten um schnell zu sehen wo überall angegriffen werden könnte
- Der Test mit dem `ping` ist zwar nicht absolut zuverlässig - wenn wir aber sehen, dass im nextage Netz der Echo Request normal abgearbeitet wird, können wir schon Rückschlüsse über die Security-Awareness ihrer Techniker ziehen
- Reminder: Gemäss Legal Disclaimer werden wir dies jetzt nicht praktisch ausprobieren (können)

Fazit

- Gezielte Angriffe beginnen in der Regel damit, sich zuerst ein Bild zu machen
  - Welche Netze?
  - Wie grosse Netze?
  - Wer ist der Owner des Netzes?
- Daraus lässt sich bestimmen, wie weiter fortgefahren wird

DNS Reverse Lookups

- Optimal wäre es, wenn wir noch weitere Informationen über das Netz indirekt bekommen könnten
- indirekt = über einen Datenbankservice wie bei WHOIS
- indirekt = vereinbar mit dem Legal Disclaimer
- Wir haben mit DNS vorhin einen Namen in eine IP übersetzt - geht dies auch rückwärts?

DNS Reverse Lookups

```
1  linux:~$ host 62.2.247.215
2  215.247.2.62.in-addr.arpa domain name pointer ↩
       herakles.nextage.ch.
```

DNS Reverse Lookups

- Der `PTR` (Pointer) gibt an, ob und welchen Reverse-Lookup ein Systemadministrator für eine IP-Adresse im DNS eingetragen hat
- Diese Reverse-Lookups sind optional, ein Administrator kann sich entscheiden für alle oder nur Teile seiner Systeme keine Reverse-Lookups einzutragen
- Forward (Name zu Adresse) und Reverse (Adresse zu Namen) müssen sich nicht zwingend entsprechen
- Effizienter wird es für uns, wenn wir einen Scanner benutzen
- `nmap` bietet einen *List Scan* an

nmap List Scan

```
1  linux:~$ nmap -sL 62.2.247.215/26
2  [...]
3  Host nx-gw01-vpn.nextage.ch (62.2.247.198) not ↩
       scanned
4  Host nx-gw02-vpn.nextage.ch (62.2.247.199) not ↩
       scanned
5  Host nx-gw03-vpn.nextage.ch (62.2.247.200) not ↩
       scanned
6  [...]
7  Host mail.nextage.ch (62.2.247.211) not scanned
8  [...]
9  Nmap done: 64 IP addresses (0 hosts up) scanned in ↩
       4.03 seconds
```

Interpretation

- Wir sehen viele Reverse-Lookups
- Wir sehen, dass im Netz auch solche Systeme mit `vpn` oder `mail` im Namen vorhanden sind
- Ein Angreifer würde sich jetzt wohl denken, dass ein VPN- oder ein Mail-Server möglicherweise vielversprechende Ziele sind

Fazit

- Auch die DNS-Reverse-Lookups waren nichts anderes als eine öffentliche Datenbank, die wir abgefragt haben
- Mit den gezeigten Tests können wir schnell beurteilen, was in einem Netz interessant sein könnte
- Wir erhalten insgesamt einen noch besseren Überblick über das Ziel

Übung

WHOIS lässt sich auch auf Domains anwenden

```
1   linux:~$ gwhois bdwm.ch
```

Zugriff auf Rechner

- Dank der IP-Adresse hat jeder Rechner eine eindeutige Adresse und kann sich in eine bestehende Netzwerkinfrastruktur einfügen
- Damit wird ein Rechner adressiert – aber noch nicht verschiedene Dienste auf dem Rechner
- Nehmen wir an, ein Rechner hat einen Web- und Mailserver gleichzeitig aktiv - neben der IP-Adresse muss ein Sender auch angeben können, welcher der beiden Dienste angesprochen werden soll

Protokolle und Port-Nummern

- Normalerweise werden Daten nicht direkt in dem IP-Protokoll transportiert
- In IP drin kommen Protokolle wie TCP oder UDP zum Einsatz
- Die beiden kennen das Konzept von Port-Nummern
- Bei Port-Nummern gibt es Standardzuweisungen
- Wenn im Webbrowser eine `http://` Adresse eingegeben wird, nutzt der Webbrowser den Port 80 (Standardport von HTTP)
- Ausnahme: In der Adresse wird vom Benutzer manuell ein abweichender Port angegeben (`http://webserver:666/`)

Protokolle und Port-Nummer

- Viele Standardports lassen sich in `/etc/services` nachschlagen

```
1  linux:~$ grep smtp /etc/services
2  smtp 25/tcp mail
3  ssmtp 465/tcp smtps # SMTP over SSL
```

Scan von Diensten

- Wir konnten vorher einen ganzen Netzwerkblock anpingen
- Dies funktioniert auch auf TCP-Ebene
- Port 0 - 65535 wird für einen bestimmten Rechner durchprobiert und wir werten aus, wo wir Antwort bekommen
- Besonders interessant ist dies um herauszufinden, welche Dienste ein Rechner anbietet
- Hierbei geht es nicht nur um Server; auch auf Desktop-Systemen sind im Normalfall Komponenten installiert, die auf einem Port hören

Ein TCP-SYN-Scan

```
1  linux:~$ sudo nmap -sS -PN 10.144.0.3
2  Starting Nmap 5.00 ( http://nmap.org ) at ↩
       2010-02-03 17:35 CET
3  Interesting ports on 10.144.0.3 (10.144.0.3):
4  Not shown: 996 closed ports
5  PORT      STATE SERVICE
6  22/tcp    open  ssh
7  80/tcp    open  http
8  443/tcp   open  https
9  49152/tcp open  unknown
10 MAC Address: 00:26:0B:DC:4A:88 (Cisco Systems)
11
12 Nmap done: 1 IP address (1 host up) scanned in 0.47↩
       seconds
```

Ein TCP-Syn-Scan

- Im vorherigen Beispiel wurde ein Wireless-Access-Point gescannt
- Je nachdem, in was für einem Netz ihr seid, könnt ihr durch die beschriebenen Techniken solche Geräte finden
- Ich sehe, dass dieser offensichtlich auf vier Ports hört
- Port 49152 kommt mir ganz unbekannt vor....

Zugriff auf einen Port

```
1  host:~# nc -v 10.144.0.3 49152
2  10.144.0.3 [10.144.0.3] 49152 (?) open
3  x
4  x
5  x
6  HTTP/0.0 400 Bad Request
7  SERVER: Linux/2.6.15--LSDK-7.1.3.23, UPnP/1.0, ↩
       Intel SDK for UPnP devices /1.2
8  CONTENT-LENGTH: 50
9  CONTENT-TYPE: text/html
10
11 <html><body><h1>400 Bad Request</h1></body></html>
```

Zugriff auf einen Port

- `nc` (Netcat) ist ein kleines Tool um eine Verbindung zu einem TCP-Port aufzubauen
- Bei der Verbindung sehen wir, dass keine Antwort kommt
- Schicken wir also zufällig etwas (in dem Fall 3 `x`)...
- ... der Access-Point antwortet mir darauf mit einer Fehlermeldung
- Scheinbar ist der Port 49152 ein Webserver, der (im Falle dieses Access Points) in der Dokumentation gar nicht erwähnt wird

Weitere Recherchen

- Auf dem Port, der probiert wurde, steht `UPnP` und `Intel SDK for UPnP devices`
- Es lässt sich jetzt auch recherchieren, was sich dahinter versteckt
- Es würde sich auch spezifisch recherchieren lassen, ob sich für Access Points dieses spezifischen Herstellers Schwachstellen finden lassen

Wieso ist das so wichtig?

- Oftmals ist auf einem Gerät oder einem Computer standardmässig etwas aktiviert
- Standard-Windows-Installationen haben bspw. die Netzwerk-Laufwerksverbindungen offen
- In einem Netz könnte also nach Windows-Rechnern mit diesen offenen Ports gesucht werden und probiert werden, ob sich mit Standardnutzernamen (bspw. «admin» und leeres Passwort) zu dem Rechner verbinden lässt
- Ebenso kann dies unter Linux passieren: installiert ihr (versehentlich) einen Apache-Webserver, kann auf diesen zugegriffen werden

Lokale Netze vs. öffentliche Netze

- Habt ihr Euren Rechner in einem lokalen/privaten Netz, dann ist vom Internet aus kein Zugriff darauf möglich
- Mit privaten IP-Adressen steht ihr in der Regel hinter einer Firewall
- Trotzdem ist es aber natürlich möglich, dass Personen im gleichen lokalen Netz Euren Computer finden können

Social Engineering

- Die bisher gezeigten Resultate lassen sich auch für Social Engineering Angriffe nutzen
- Dabei handelt es sich um keine technischen Angriffe
- Es werden dabei bestimmte Informationen genutzt, um andere Leute zu täuschen
- Bei den WHOIS-Abfragen waren auch Kontaktpersonen sichtbar
- Dies gibt eine (noch sehr wackelige) Grundlage für Telefonanrufe
- Leute direkt anzusprechen funktioniert meistens schneller als technische Lücken auszunutzen

Social Engineering

- Social Engineering ist deshalb so problematisch, weil zuwenig Awareness besteht
- Viele Leute sind bereit zu vertrauen, wenn das Gegenüber die erwarteten Informationen besitzt
- Wer also Kontaktdaten (und vorallem Abhängigkeiten von Organisationen!) kennt, hat gute Karten, um per Telefon an weitere Informationen zu kommen

Soziale Netzwerke

- Solche Social Engineering Angriffe lassen sich über soziale Netze weiter perfektionieren
- Mit der richtigen Suche bei Xing wird schnell klar, welche Leute in welcher Firma für was zuständig sind
- Es lassen sich damit in vielen Fällen komplette Firmenhierarchien ausfindig machen
- Zusätzlich lassen sich über HR-Auszüge auch komplette Firmengeschichten (Fusionen, Ein- und Austritt von Verwaltungsräten) nachverfolgen

Don't Panic

- Generell ist es nun natürlich wichtig, nicht Angst zu haben vor dem Medium IT
- Es hilft aber sehr, die richtige Awareness zu haben
- Zudem solltet ihr Euch bewusst sein, dass ihr bspw. beim Registrieren einer Domain ebenfalls per WHOIS gefunden werden könnt
- Andererseits kann es natürlich auch helfen, wenn man selber rasch Informationen über eine Firma sammeln kann (bspw. bevor man dort etwas kauft)

Fragen?