IT-SECURITY - Forum #2

Wie helfen Penetration Tests die Sicherheit zu erhöhen?

Andreas Wisler
Sicherheitsspezialist
Dipl. IT Ing. FH
GO OUT Production GmbH
andreas.wisler@goout.ch

IT-SECURITY - Forum #2

Probleme in der IT

- Netzwerk ist dynamisch gewachsen
- Mitarbeiter machen sich „selbständig“
- Keine Zeit für Dokumentation
- Stellenwechsel / Übergabe nicht optimal
- Software / Patches verändern System

Offene Ports von Software

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    andreas:http           andreas:0              LISTENING
  TCP    andreas:epmap          andreas:0              LISTENING
  TCP    andreas:https          andreas:0              LISTENING
  TCP    andreas:microsoft-ds   andreas:0              LISTENING
  TCP    andreas:1025           andreas:0              LISTENING
  TCP    andreas:1028           andreas:0              LISTENING
  TCP    andreas:1029           andreas:0              LISTENING
  TCP    andreas:1030           andreas:0              LISTENING
  TCP    andreas:1045           andreas:0              LISTENING
  TCP    andreas:1048           andreas:0              LISTENING
  TCP    andreas:1054           andreas:0              LISTENING
  TCP    andreas:1294           andreas:0              LISTENING
  TCP    andreas:1295           andreas:0              LISTENING
  TCP    andreas:pop3           andreas:0              LISTENING
  TCP    andreas:imap           andreas:0              LISTENING
  TCP    andreas:1027           andreas:0              LISTENING
  TCP    andreas:1038           andreas:0              LISTENING
  TCP    andreas:1045           andreas:1027           CLOSE_WAIT
  TCP    andreas:1048           andreas:1027           CLOSE_WAIT
  TCP    andreas:netbios-ssn    andreas:0              LISTENING
  TCP    andreas:1294           212.243.204.43:imap    ESTABLISHED
  TCP    andreas:1295           212.243.204.43:imap    ESTABLISHED
  UDP    andreas:microsoft-ds   *:*
  UDP    andreas:isakmp         *:*
  UDP    andreas:1032           *:*
  UDP    andreas:3456           *:*
  UDP    andreas:4500           *:*
  UDP    andreas:62514          *:*
  UDP    andreas:netbios-ns     *:*
  UDP    andreas:netbios-dgm    *:*
```

- Ausgabe mit „netstat –a“

Was steckt hinter den Ports?

- Ports 1 bis 1024 normiert
- Rest frei verwendbar
- Viele Trojaner verwenden bekannte Ports
- Überblick sehr schwer zu behalten.

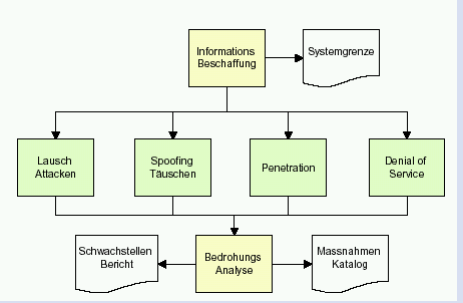
23	tcp	RTB666	[trojan] RTB 666
23	tcp	TelnetPro	[trojan] Telnet Pro
23	tcp	TinyTelnetServer	[trojan] Tiny Telnet Server - TI
23	tcp	TruvaAtl	[trojan] Truva Atl
24	tcp	B02KControlPort	[trojan] Back Orifice 2000 (B02K
24	tcp	priv-mail	any private mail system
24	udp	priv-mail	any private mail system
25	tcp	smtp	Simple Mail Transfer
25	udp	smtp	Simple Mail Transfer
25	tcp	Ajan	[trojan] Ajan
25	tcp	Antigen	[trojan] Antigen
25	tcp	Barok	[trojan] Barok
25	tcp	BSE	[trojan] BSE
25	tcp	EmailPasswordSender	[trojan] Email Password Sender -
25	tcp	EPSII	[trojan] EPS II
25	tcp	Gip	[trojan] Gip
25	tcp	Gris	[trojan] Gris
25	tcp	Happy99	[trojan] Happy99
25	tcp	Hpteammail	[trojan] Hpteam mail
25	tcp	Hybris	[trojan] Hybris
25	tcp	Iloveyou	[trojan] I love you
25	tcp	Kuang2	[trojan] Kuang2
25	tcp	MagicHorse	[trojan] Magic Horse
25	tcp	MBTMailBombingTrojan	[trojan] MBT (Mail Bombing Troje
25	tcp	MBT	[trojan] MBT (Mail Bombing Troje
25	tcp	MoscowEmailtrojan	[trojan] Moscow Email trojan
25	tcp	Naebi	[trojan] Naebi
25	tcp	NewAptworm	[trojan] NewApt worm
25	tcp	ProMailtrojan	[trojan] ProMail trojan
25	tcp	Shtirlitz	[trojan] Shtirlitz
25	tcp	Stealth	[trojan] Stealth
25	tcp	Stukach	[trojan] Stukach
25	tcp	Tapiras	[trojan] Tapiras
25	tcp	Terminator	[trojan] Terminator
25	tcp	WinPC	[trojan] WinPC
25	tcp	WinSpy	[trojan] WinSpy
26	tcp	altavista-fw97	AltaVista Firewall97
27	tcp	altavista-fw97	AltaVista Firewall97
27	tcp	nsw-fe	NSW User System FE
27	udp	nsw-fe	NSW User System FE

- Liste unter: http://www.gosecurity.ch/anleitungen/ports.asp

IT-SECURITY - Forum #2

Ablauf eines Penetration Tests

1) Informationssuche im Internet
2) IP-Scan, Port-Scan
3) Informationen über offene Ports suchen
4) Schwachstellen der Applikationen suchen
5) Ausnutzen der Schwachstellen
6) Bericht mit Gefahren und Massnahmen



IT-SECURITY - Forum #2

1. Informationssuche

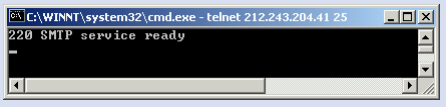
- Was findet Google und andere Suchmaschinen über diese Firma (Mitarbeiter: Kader, Angestellte; Partnerschaften, …)
- IP-Adressen (http://sunny.nic.com/cgi-bin/whois)
- DNS-Informationen (http://www.switch.ch/id/search-domain.html)
- DNS File auslesen (http://www.ip-plus.ch/tools/dig_dns_set.en.html)

2. IP-Scan

- Welche IP-Adressen antworten?
- Was steckt hinter welcher Adresse?
- Lässt sich feststellen, wie das Netzwerk aufgebaut ist?
- Welches sind die interessanten Ziele?

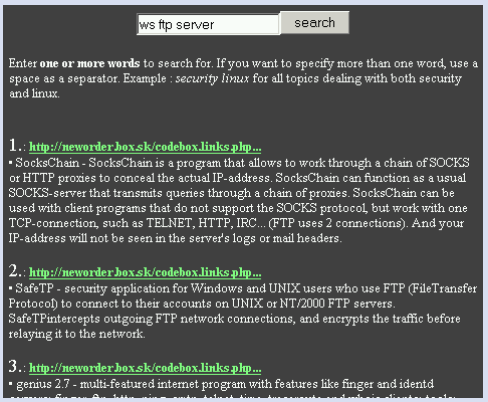
3. Port-Scan

- Aktive IP-Adressen nach offenen Ports absuchen
- Werden Scans erkannt und blockiert?
- Sind die Standardports offen?
  (HTTP = 80, SMTP = 25, etc.)
- Finden sich eigene Applikationen?
- Kann die Version ausgelesen werden (Header-Informationen)
  z.B.



4. Schwachstellen

- Jede Applikation auf Schwachstellen untersuchen.
  z.B. bei Astalavista.com:



- Schwachstellen auch mit Social Engineering suchen

5. Schwachstellen ausnützen

- Gefundene Schwachstellen ausnützen:
  - CGI-Skripts
  - SQL Abfragen (siehe folgende Folie)
  - Schwachstellen der Software
- Passworte „knacken“ mit:
  - Standard-Passworte
  - Dictionary Attack
  - Brute Force

5. Schwachstellen ausnützen II

- Beispiel SQL Abfrage:

Eingabe von:

Benutzername = ´or true or ´
Passwort = ´ or true or ´

ergibt den folgenden SQL-Befehl:

SELECT * FROM user WHERE
name=´´ **or true or** ´´ AND pwd = ´´ **or true or** ´´

Mit dem Ergebnis:

Login erlaubt mit den Rechten des ersten Benutzers

6. Bericht

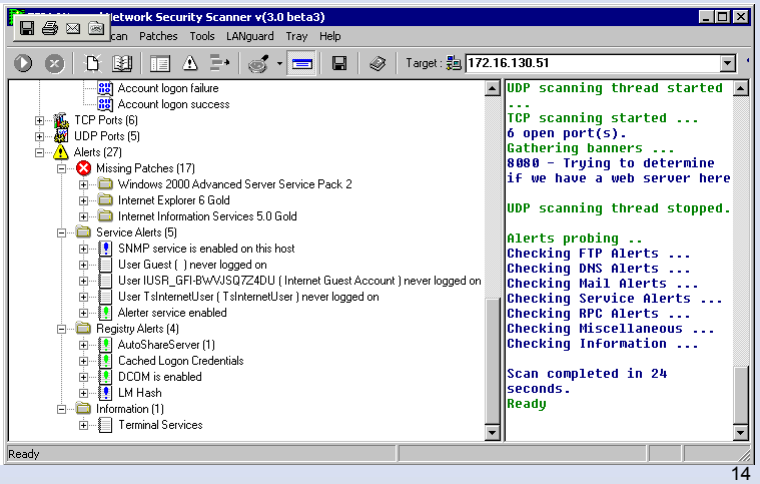
- Gefundene Schwachstellen auflisten
- Gefahren zu den Schwachstellen aufzeigen
- Gegenmassnahmen zeigen
- Präsentation des Testes

Tools für den Administrator

- Automatisierte Tests für den Administrator:
  - Online:
    - Symantec Security Check: http://security.symantec.com
    - Perisec: http://www.perisec.com/
  - Offline:
    - ISS Internet Scanner http://www.iss.net
    - Retina http://www.eeye.com
    - Nessus http://www.nessus.org
    - SARA (früher SATAN) http://www-arc.com/sara/
    - TIGER / TARA http://www-arc.com/tara/
    - TITAN (Solaris) http://www.fish.com/titan

Tools für den Administrator II

  - Offline:
    - GFI LANguard Network Security Scanner:



IT-SECURITY - Forum #2

IT-SECURITY - Forum #2

Tools für den Administrator III

- Probieren Sie sich als „Hacker“:
  http://scifi.pages.at/hackits/
- Oder wem das zu einfach war:
  http://quiz.ngsec.biz:8080

IT-SECURITY - Forum #2

Nutzen

- **Übersicht**
  Aufnahme der IST-Situation
- **Informationsgewinn**
  Exakte Einschätzung der Gefährdungen durch Hacker und Cracker
- **Entscheidungssicherheit**
  Empfehlungen für effektive Schutzmassnahmen gegen externe Angriffe
- **Objektivität**
  Fundierte Analyse nach objektiven Kriterien

Nutzen

- **Qualität**
  Systematische, umfangreiche und tiefgründige Tests durch hochrangige, erfahrene Experten
- **Neutralität**
  Herstellerunabhängige Analyse und Beratung
- **Praxisnähe**
  Orientierung an den praktischen Aktivitäten der Hacker-und Cracker-Szene