The information security provider

Penetration Testing in der Praxis

Ralf Wienzek

Definition

- Penetrationstest

„A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user, kn[illegible]he process involves[illegible]otential vulnerab[illegible]er system configur[illegible] software flaws, or opera[illegible] countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.“

[Wikipedia]

Cut a long story short:

A penetration test is the process of actively evaluating your information security measures.

Übersicht: Begriffe

- **IT Security Audit**: Prüfung gegen eine Vorgabe (Policy, Standards, Guidelines); ohne Vorgabe: Prüfung gegen „Best Practice“
- **Network Scanning**: Identifizierung der erreichbaren Hosts und Dienste eines Netzwerks
- **Vulnerability Scanning**: Scanner prüft (meist automatisiert) auf Schwachstellen; viele False Positives; nur bekannte Schwachstellen
- **Security Scanning**: Vulnerability Scan mit manueller Verifikation der Meldungen
- **Penetration Test**: aktiver Versuch durch professionelle Tester, das Zielsystem zu kompromittieren; nicht nur technisch („Social Engineering“)
- **Ethical Hacking**: Marketing Begriff; beschreibt meist einen Pentest, bei dem alles erlaubt ist; impliziert zum Teil den Einsatz eines „domestizierten|guten|bekehrten“ Hackers (heute allerdings eher selten)
- **Red Team** / **Tiger Team**: Verdeckte Angreifer-Gruppe, d.h. IT-Personal ist nicht über Penetrationstest informiert; Ursprung: militärischer Sprachgebrauch
- **Blue Team**: Testgruppe, die offen prüft, d.h. IT-Personal ist informiert

Ziele & Motivation

- Ziele
  - Identifikation von Schwachstellen
  - Erhöhung der Sicherheit der technischen Systeme
  - Erhöhung der Sicherheit der organisatorischen und personellen Infrastruktur
  - Bestätigung der IT-Sicherheit durch externen Dritten

- Motivation
  - Gesetzliche Vorgaben
  - Teil einer Zertifizierung
  - Verbessertes Risikomanagement
  - Verantwortungsverlagerung

Hacker vs. Pentester

- Hacker
  - Beliebig viel Zeit / Ressourcen
  - Ausnutzen einer bestimmten Sicherheitslücke
  - Suche nach weiteren Lücken, um Rechte auszubauen

- Pentester
  - Nur begrenzt viel Zeit / Ressourcen
  - Identifizieren aller Sicherheitslücken
  - Beachtung von Rahmenbedingungen und Gesetzen

„Hacker-Paragraph“

- §202c StGB „Hacker-Paragraph“
  - *„Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er*
    - *Passworte oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
    - *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“*
      siehe: http://www.bmj.bund.de/media/archive/1317.pdf
  - Umsetzung der Cybercrime Konvention und des EU Rahmenbeschlusses über Angriffe auf Informationssysteme
  - Wurde am 25.05.2007 um 02:00 Uhr morgens verabschiedet
  - Sorgt momentan für Besorgnis bei Sicherheitsfirmen, die entsprechende Programme einsetzen

„Hacker-Paragraph“

- Aussage Brigitte Zypries
  - *„Dieser Straftatbestand erfasst selbstverständlich nicht die Arbeit von IT-Spezialisten, die im Auftrag ihres Unternehmens oder anderer Unternehmen IT-Sicherheitsprüfungen durchführen.“*

    [http://www.abgeordnetenwatch.de/brigitte_zypries-650-5639-117.html#fragen]
- Beschlussempfehlung und Bericht des Rechtsausschusses
  - *„Der Gesetzentwurf kriminalisiere nicht den branchenüblichen Einsatz von Hacker-Tools durch Netzwerkadministratoren, insbesondere wenn diese nur die Sicherheit des eigenen Datennetzes prüfen wollten.“*
  - *„Um Missverständnisse zu vermeiden, stelle der Rechtsausschuss klar, dass § 202c StGB hinsichtlich der Zweckbestimmung im Sinne des Artikels 6 des Europarats-Übereinkommens auszulegen sei. […] Die bloße Geeignetheit zur Begehung solcher Straftaten begründe keine Strafbarkeit. Die geforderte Zweckbestimmung müsse eine Eigenschaft des Computerprogramms in dem Sinne darstellen, dass es sich um sog. Schadsoftware handele.“*
  - *„Der Gesetzgeber werde die Auswirkungen der neuen Strafvorschriften genau zu beobachten haben. Sollten doch Programmentwickler und Firmen, die nicht aus krimineller Energie heraus handelten, durch diese neuen Strafvorschriften in Ermittlungsverfahren einbezogen werden, werde auf solche Entwicklungen zeitnah reagiert werden müssen.“*

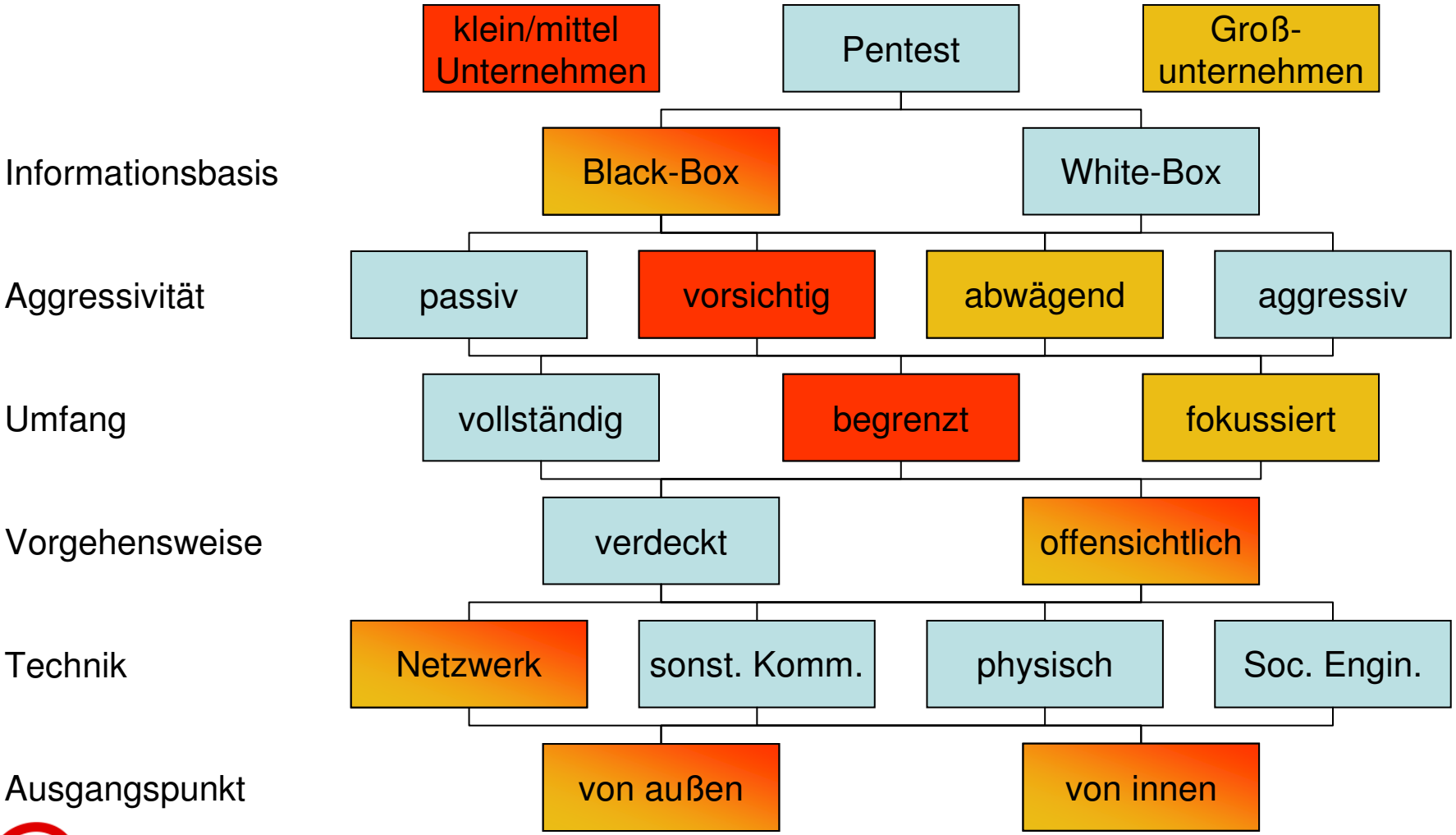
    [Deutscher Bundestag, Drucksache 16/5449]

„Hacker-Paragraph“

- Europarat: Übereinkommen über Computerkriminalität
  - Artikel 6, Absatz 2:

    „Dieser Artikel darf nicht so ausgelegt werden, als begründe er die strafrechtliche Verantwortlichkeit in Fällen, in denen das Herstellen, Verkaufen, Beschaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen oder der Besitz nach Absatz 1 nicht zum Zweck der Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat, sondern beispielsweise zum genehmigten Testen oder zum Schutz eines Computersystems erfolgt.“

Klassifikation



Allgemeines Vorgehen

- Standard Penetrationstest
  - Information Gathering (Reconnaissance)
  - Network Enumeration
  - Vulnerability Analysis
  - Exploiting
  - Privilege Escalation
  - Results Analysis and Reporting
- Weiteres
  - Andere Kommunikationsformen: War Dialing, War Driving
  - Social Engineering: Kontakt per Telefon, Email; Dumpster Diving
  - Physical: Zutritt zu Räumen; ungeschützte Netzwerkdosen

Information Gathering

- Ziel:
  - Verfügbare Informationen über das Ziel sammeln
  - Nutzung der Informationen für weitere Angriffe
- Harvesting
  - Informationssammlung für weitere Angriffe
  - Quellen: Web, Partner, Job-Börsen, CVs
- Google Hacking
  - Nutzung der umfangreichen Funktionalität von Google
  - Sehr gute Datenbank: http://johnny.ihackstuff.com/

Beispiel Metagoofil

- Metagoofil
  - Auslesen von Metainformationen aus öffentlichen Dokumenten
  - pdf, doc, xls, ppt, sdw, mdb, sdc, odp, ods
  - Google-Anfrage: „site:target.com filetype:pdf“
  - Download und Analyse der Ergebnisdokumente
  - Anwendung:

```
$ python metagoofil.py -d inf.fh-bonn-rhein-sieg.de -f all -l 20 -o
inf.fh-bonn-rhein-sieg.de.html -t .
```

  - Ergebnis

Network Enumeration

- Ziel:
  - Vollständiges Bild über das Netzwerk:
    Topologie, IP-Range
- Quellen:
  - Passiv: Abfrage öffentlicher Datenbanken
    - whois, DNS
  - Aktiv: Probepakete + Auswertung der Antwort
    - Zugriffspfade: traceroute, firewalk
    - Portscanner (z.B. nmap), OS Detection (z.B. sinFP), Service Scanner (z.B. amap)
    - Manueller Verbindungsaufbau

Network Enumeration: DNS

```
$ dig fh-bonn-rhein-sieg.de mx

; <<>> DiG 9.4.1-P1.1 <<>> fh-bonn-rhein-sieg.de mx
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63110
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 2

;; QUESTION SECTION:
;fh-bonn-rhein-sieg.de.          IN      MX

;; ANSWER SECTION:
fh-bonn-rhein-sieg.de.  3109    IN      MX      10 mx01.fh-bonn-rhein-sieg.de.

;; AUTHORITY SECTION:
fh-bonn-rhein-sieg.de.  1483    IN      NS      deneb.dfn.de.
fh-bonn-rhein-sieg.de.  1483    IN      NS      ns2.fh-bonn-rhein-sieg.de.
fh-bonn-rhein-sieg.de.  1483    IN      NS      ns1.fh-bonn-rhein-sieg.de.

;; ADDITIONAL SECTION:
mx01.fh-bonn-rhein-sieg.de. 3109 IN     A       194.95.64.101
deneb.dfn.de.           2590    IN      A       192.76.176.9
```

NMAP

```
$ nmap -p- -P0 -T4 -sS -sU -A -oA nmapResult -v -n 192.168.91.131
# Nmap 4.75 scan initiated Mon Nov 10 11:22:36 2008 as: nmap -p- -P0 -T4 -sS -sU -A -oA
nmapResult -v -n 192.168.91.131
Initiating OS detection (try #1) against 192.168.91.131
Interesting ports on 192.168.91.131:
Not shown: 131059 closed ports
PORT     STATE         SERVICE      VERSION
135/tcp  open          msrpc        Microsoft Windows RPC
139/tcp  open          netbios-ssn
445/tcp  open          microsoft-ds Microsoft Windows XP microsoft-ds
123/udp  open          ntp          Microsoft NTP
137/udp  open          netbios-ns   Microsoft Windows NT netbios-ssn (workgroup: WORKGROUP)
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1025/udp open|filtered blackjack
1900/udp open|filtered upnp
4500/udp open|filtered sae-urn
MAC Address: 00:0C:29:6B:08:61 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: VM-WINXPP; OS: Windows

Host script results:
|_ NBSTAT: NetBIOS name: VM-WINXPP, NetBIOS MAC: 00:0C:29:6B:08:61
|  Discover OS Version over NetBIOS and SMB: Windows XP
|_ Discover system time over SMB: 2008-11-22 18:53:40 UTC+1
```

Vulnerability Analysis

- Ziel:
  - Identifizierung möglicher Schwachstellen
- (Semi-)Automatische Analyse
  - Lediglich Ausgangspunkt für weitere Untersuchung
  - Vulnerability Scanner (Nessus, nikto, …)
- Manuelle Verifikation / Recherche
  - Überprüfung der Ergebnisse des Scans
  - Suche nach aktuellen Schwachstellen in öffentl. DB
- Nessus Resultat

Schwachstellen-Suche

- Was tun, wenn eine Schwachstelle vermutet wird ?
  - CVE (Common Vulnerabilities and Exposures)
    - http://cve.mitre.org/
  - WVE (Wireless Vulnerabilities and Exposures)
    - http://www.wirelessve.org/
  - Informationsdatenbanken
    - OSVDB (http://osvdb.org/)
    - Milw0rm (http://www.milw0rm.com/)
    - SecurityForest (http://www.securityforest.com/wiki/index.php/Main_Page)
    - Packetstorm (http://packetstormsecurity.org/)
    - Bugtraq Archive (http://www.securityfocus.com/archive/1)
    - OffensiveComputing: (http://www.offensivecomputing.net/)

Exploiting

- Ziel:
  - Ausnutzen von Schwachstellen, um Zugang zu Informationen oder Systemen zu erhalten
- Password Cracking
  - Online:
    - Identifizierung einer Online-Seite mit Passwort-Authentifizierung
    - Anwendung Passwort-Cracker (z.B. medusa)
  - Offline:
    - Download einer Datei mit Passwort-Hashes
    - lokale Anwendung Passwort-Cracker (z.B. john)
- Exploitation Frameworks

Privilege Escalation

- Ziel:
  - Erlangung der vollständigen Kontrolle über möglichst viele Systeme
- Idee:
  - Bereits erlangter Zugriff ist Ausgangspunkt für Ausnutzung weiterer Schwachstellen
    - nur lokal ausnutzbare Schwachstellen zur Erweiterung der Nutzerrechte
    - Vertrauensbeziehungen zwischen Systemen zum Zugriff auf weitere Systeme

Results Analysis und Reporting

- Analyse der Ergebnisse der automatisierten Tools
  - Ein aufbereiteter Nessus-Scan ist zu wenig
    - Kunde könnte Nessus meist selbst ausführen
    - Viele False Positives enthalten
  - Alle Findings müssen verifiziert werden
    - False Positives kosten viel Zeit und Geld
    - False Positives machen den Tester unglaubwürdig
- Erstellen des Reports
  - Wann wurden welche Aktionen ausgeführt; welche Tools; welche IP
  - Pro Finding: Problembeschreibung, Beschreibung zur Verifizierung, Risikoeinschätzung, Gegenmaßnahmen, Ansprechpartner benennen
  - Executive Summary

Beispiele aus der Praxis

- Auftrag:
  - Web-Applikations-Pentest eines Telekommunikationsunternehmens
- Finding:
  - HTTP-PUT eingeschaltet
    ➔ Ablegen beliebiger Dateien auf dem Web-Server möglich
    ➔ Missbrauch als Porn/Warez-Server möglich
  - SQL-Injektion: Zugriff auf Admin-Schnittstelle
    ➔ Zugriff auf Benutzer-DB
    ➔ Auslesen persönlicher Informationen

Beispiele aus der Praxis

- Auftrag:
  - Pentest des Internetauftritts einer Versicherungsgesellschaft
- Finding:
  - Ungeschützter Zugriff auf phpMyAdmin
    ➔ Vollzugriff auf interne DB
  - Directory Traversal auf Web-Server, der als root läuft:
    http://www.target.com/../../../../etc/shadow
    ➔ Anzeige von /etc/shadow
    ➔ Passwörter mit john gecrackt (u.a. root)
    ➔ ssh-Login

Beispiele aus der Praxis

- Auftrag:
  - Interner Pentest eines ISP
- Finding:
  - Wireless Access Point im Office-Netz nur WEP-“geschützt“
    ➔ WEP-Schlüssel innerhalb von 2h
  - Offene Firewall von Office-Netz in Management-Netz
    ➔ Erreichbarkeit der Netz-Management-SW
  - Online-Passwort-Cracker
    ➔ Passwort über Nacht gefunden
  - Ungeschütztes Web-Management-Interface eines Druckers
    ➔ Abrufen alter Druckaufträge

Zusammenfassung

- Regelmäßige Penetrationstests sind ein wichtiger Baustein zur Bestimmung des allgemeinen Sicherheitsniveaus
- Wichtig: detaillierte „Rules of Engagement“ definieren
- Sicherheitsniveau der getesteten Systeme in der Regel nicht so schlecht; manchmal jedoch erschreckend

Vortragender

Dipl.-Inform.
Ralf Wienzek

Security Consultant

atsec information security GmbH
Riehler Str. 21
D - 50668 Köln
www.atsec.com

Tel: +49 (0) 221 579 62 49
Fax: +49 (0) 221 579 62 50
Mobile: +49 (0) 172 824 67 38
e-mail: ralf@atsec.com