Auftragshacking – technischen Sicherheitslücken auf der Spur

Christoph Baumgartner

Agenda

- Fakten
- Definitionen
- Zweck und Nutzen
- Problematik
- Technische Sicherheitsüberprüfungen
- Untersuchungsobjekte
- Phasen eines Hackerangriffs
- Technische Angriffsmethoden
- Lessons learnt
- Massnahmen und Empfehlungen
- Kosten und Aufwand
- Beantwortung von Fragen
- Diverse Beilagen

Fakten

- **Information als Asset**
- **Geheimdienste** hören elektronische Kommunikation systematisch ab
  - **Echelon (NSA)**
  - **Carnivore (FBI)**
- **Hacker** verursachen **Schäden in Milliardenhöhe**
- **Malicious Mobile Code** und **mangelhafte Datensicherung** verursachen **hohe Kosten**
- 50 - 80% aller **Datendiebstähle** erfolgen **durch** organisationsinterne **Mitarbeiter**
- **Gesetzliche Rahmenbedingungen** zu Datenschutz und Aufbewahrungspflicht (Compliance) sind einzuhalten

Definitionen (im deutschsprachigen Raum)

- Als "**Skript Kiddie**" wird eine Person bezeichnet, welche über (relativ) **wenig Computer- und Netzwerkfachwissen** verfügt, aber unbedarft (**vollautomatisierte**) **Hackertools einsetzt** und damit teilweise massiven Schaden verursachen kann.
- Ein "**Hacker**"/ "**Cracker**" (auch "Black Hat" genannt) **bricht ohne Erlaubnis** des Systemeigners meist via Computernetze **in Computersysteme ein** oder knackt das Lizenzsystem von Computerprogrammen. Dafür umgeht er Sicherheits-mechanismen. Die Beweggründe sind Ehrgeiz, möglicher finanzieller Profit, Geltungssucht, Idealismus oder Zerstörungswille.
- Ein "**Ethical Hacker**" (auch "White Hat" genannt) ist ein Computer- und Netzwerkspezialist, welcher **im Auftrag des Systemeigners** nach **Systemverwundbarkeiten sucht**, welche ein "Hacker"/"Cracker" ausnutzen könnte.

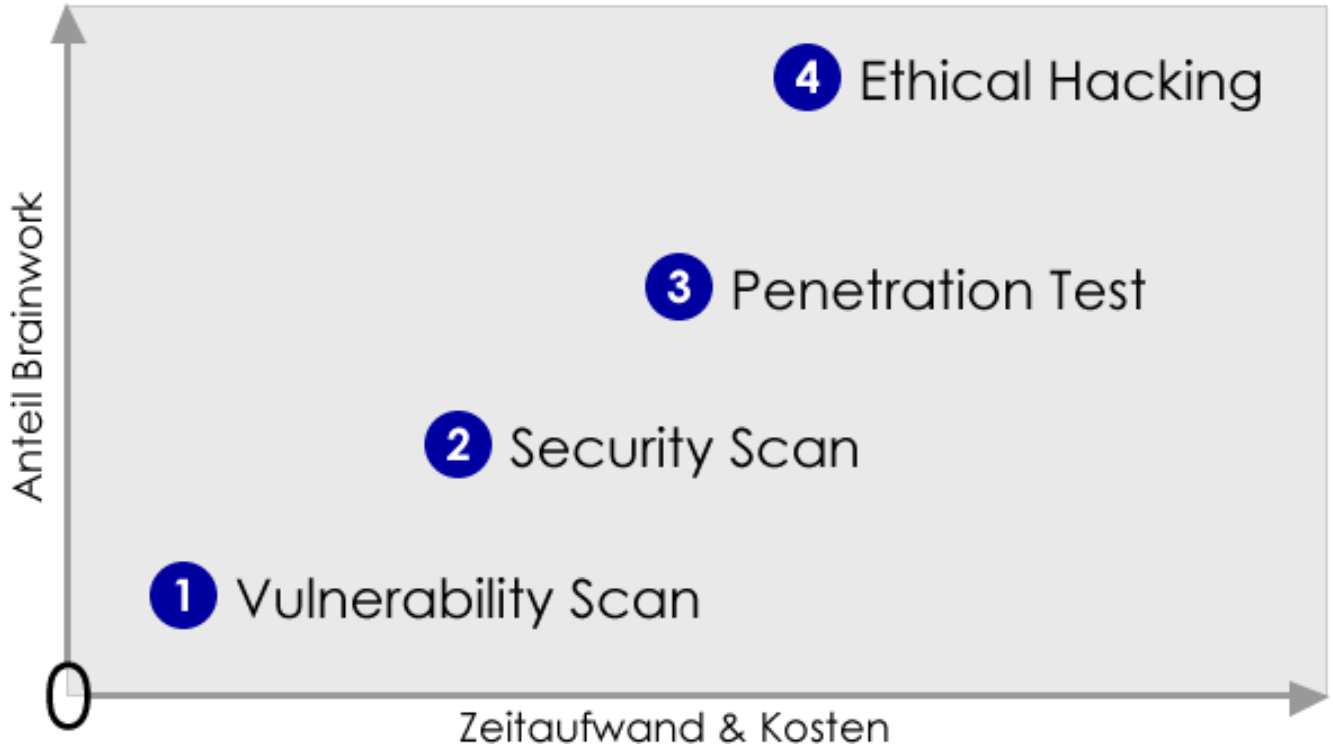
Ethical Hacking: Zweck und Nutzen

- **Unabhängige IT Security-Analyse** ermöglicht Qualitätssicherung
- **Erhöhung** des **Sicherheitsniveaus** ermöglicht **Kostensenkung** dank Prävention
- **Awareness** Building auf allen Stufen und **Know-how** Transfer
- **Argumentationsgrundlage** für zukünftige IT Security-Projekte
  - Fokus Technik: Systemhärtung, Systemintegration etc.
  - Fokus Organisation: Sicherheitskonzept, IT Bedrohungs- & Risikoanalyse, Policy etc.

Ethical Hacking: Problematik

- Methodik
  - Üblicherweise wird **nur das Ziel** (z.B. Speicherung einer bestimmten Datei auf einem Zielsystem), nicht aber der Weg zum Ziel **vorgegeben** => eine **Sicherheitslücke reicht zur Zielerreichung generell aus**, nach weiteren wird nicht gesucht.
- Ressourcen
  - „Hacker" / „Cracker" stehen nicht unter **Zeitdruck**.
  - „Ethical Hacker" (Auftragshacker) haben **beschränkte finanzielle und zeitliche Ressourcen**.

Technische Sicherheitsüberprüfungen 1



Terminologie angelehnt an:
OSSTMM (Open Source Security Testing Methodology Manual von ISECOM)

Technische Sicherheitsüberprüfungen 2

Merkmal	1 Vulnerability Scan	2 Security Scan	3 Penetration Test	4 Ethical Hacking
Aufspüren von Sicherheitslücken	voll-auto-matisiert	voll-auto-matisiert	teil-auto-matisiert / manuell	teil-auto-matisiert / manuell
Einsatz mehrerer Tools mit ähnlicher Funktionalität	nein	nein	ja	ja
manuelle Verifikation	nein	ja	ja	ja
Ausnützen von Sicherheitslücken	nein	nein	nein	ja
Modifikation des Untersuchungsobjekts	nein	nein	nein	ja

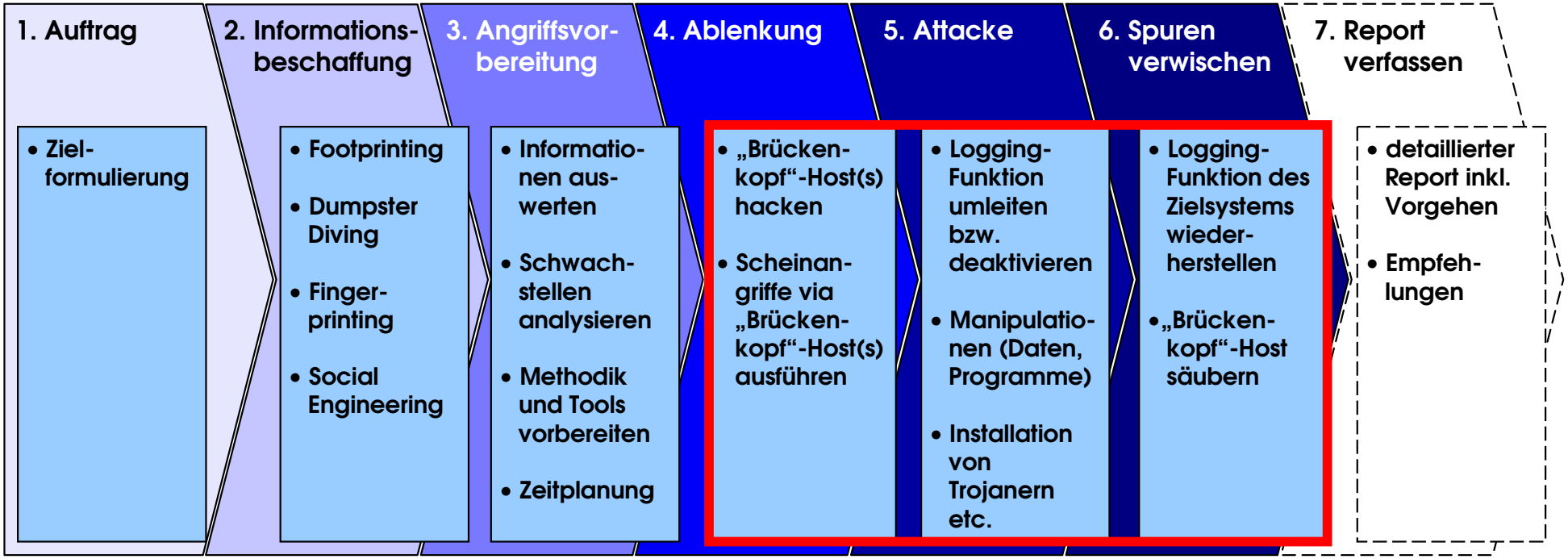
Technische Sicherheitsüberprüfungen 3

Merkmal	1 Vulnerability Scan	2 Security Scan	3 Penetration Test	4 Ethical Hacking
Ansatz	direkt	direkt	direkt	direkt / indirekt
Empfehlung technischer Massnahmen	ja	ja	ja	ja
Empfehlung organisatorischer Massnahmen	nein	nein	ja	ja

Untersuchungsobjekte

- Computernetzwerke
  - Externe Netze / DMZ (z.B. Firewall, Web-, FTP-, Mail-, DNS-, Terminal-server und weitere Netzwerkkomponenten) aus externer oder interner Sicht
  - LAN / WAN (z.B. Clients, Server, Peripheriegeräte und Netzwerkkomponenten)
  - Wireless LAN / Bluetooth
- Telefon / Fax / Handy / Modem
- Applikationen (z.B. n-Tier-Applikationen wie SAP, CRM und Branchenlösungen)
- (kombinierte) Systeme (z.B. verteilter Anti-Virenschutz)

Phasen eines Hackerangriffs



Phasen-dauer	Stunden bis Jahre	Tage bis Monate	Stunden bis Monate	Minuten bis Tage	Minuten bis Tage
Aktivitäts-dauer (en block, Schätzung)	**0.1 bis 10.0** (Personen-tage)	**2.0 bis 10.0** (Personen-tage)	**0.5 bis 5.0** (Personen-tage)	**0.1 bis 1.0** (Personen-tage)	**0.1 bis 1.0** (Personen-tage)

Technische Angriffsmethoden 1

Attacke	Zweck	Verhältnis Anzahl Angreifer : Opfer
Sniffing	▫ systematisches Abhören und Analysieren ▪ des Netzwerkverkehrs ▪ der Benutzerinteraktionen (auf Zielsystem) für Systemzugriff	1 : n
Log-on	▫ Systemzugriff erlangen	1 : 1
Shares einbinden	▫ Datendiebstahl ▫ Datenmanipulation ▫ Plazieren von Trojanern	1 : 1

Technische Angriffsmethoden 2

Attacke	Zweck	Verhältnis Anzahl Angreifer : Opfer
Brute Force	▫ systematisches Ausprobieren von User-ID/Passwortkombinationen für ▪ Systemzugriff ▪ Entschlüsselung von verschlüsselter Kommunikation	1 : 1
Buffer Overflow	▫ Ausführung von beliebigem manipuliertem Programm-Code oder Verfälschung von Daten ▫ evtl. negative Beeinträchtigung der Verfügbarkeit des angegriffenen Systems	1 : 1

Technische Angriffsmethoden 3

Attacke	Zweck	Verhältnis Anzahl Angreifer : Opfer
Cross-Site Scripting	▫ Ausnutzen vertrauenswürdiger Websites zum Ausspionieren des angegriffenen Systems	1 : n
SQL Injection	▫ Ausspionieren oder manipulieren der angegriffenen Datenbank	1 : 1
Remote Administration Tool (RAT)	▫ Remote-Kontrolle des angegriffenen Systems ▪ Datendiebstahl ▪ Datenmodifikation ▪ evtl. Verwendung als „Brückenkopf"-Host	1 : 1

Technische Angriffsmethoden 4

Attacke	Zweck	Verhältnis Anzahl Angreifer : Opfer
Denial of Service (DoS)	▫ negative Beeinträchtigung der Verfügbarkeit des angegriffenen Systems	1 : 1
(Distributed) Denial of Service (DDoS)	▫ negative Beeinträchtigung der Verfügbarkeit des angegriffenen Systems ▫ koordinierte, zeitgleiche Attacke mehrerer Angreifer	n : 1

Lessons learnt

- gravierendste Sicherheitslücken:
  - Webserver
  - Mailserver
  - Anti-Viren-Schutz (kombinierte Systeme)
  - PC (mit Administrationsberechtigung)
  - Modem
  - Drucker
- Papier ist geduldig: Vertrauen ist gut, Kontrolle ist besser
- gravierende Sicherheitslücken asap schliessen und Massnahmen dokumentieren

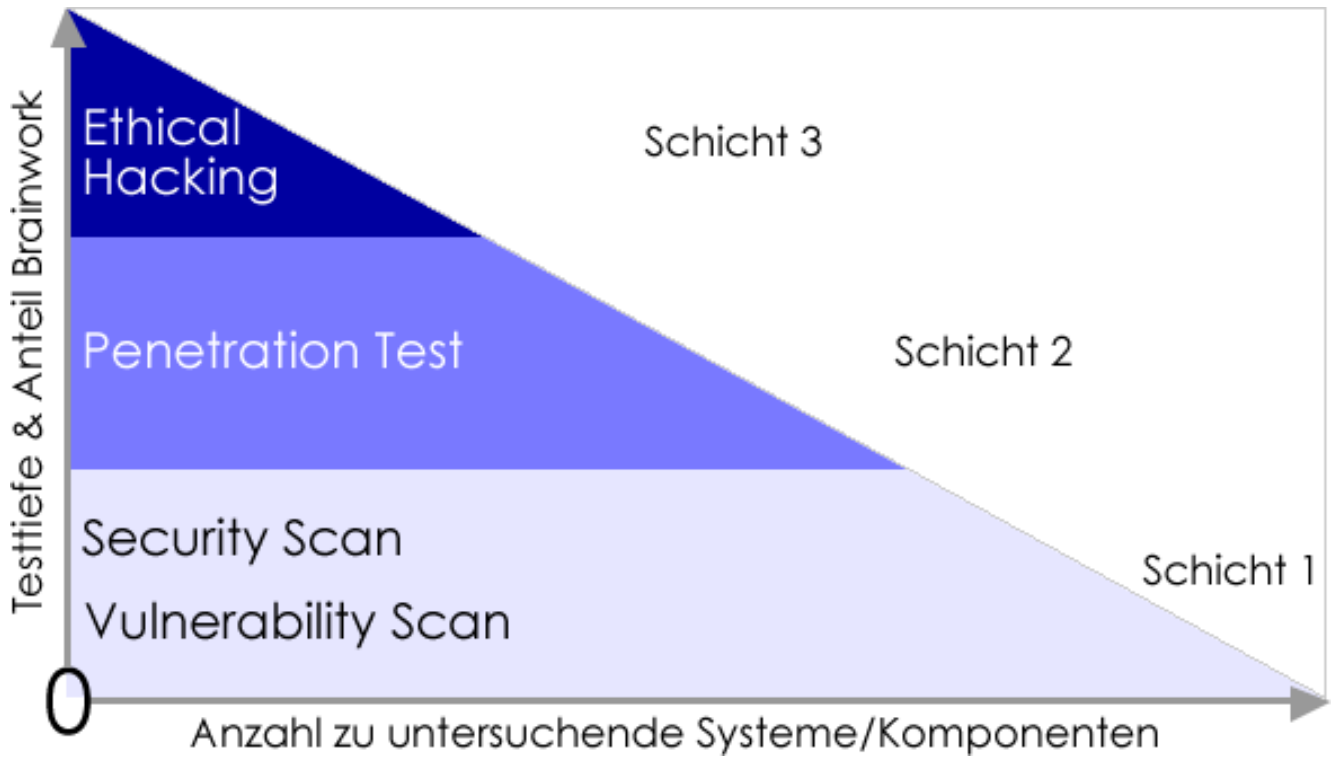
Organisatorische Massnahmen gegen Hacker

- Security-Awareness der Mitarbeiter fördern
- Security-Konzept und -Policies
- Umgang mit „verdächtiger" E-Mail
  - echten Mail-Absender in Microsoft Outlook überprüfen
  - bei Verdacht Absender anfragen (lieber vor- als nachsehen)
- SWAT/CERT-TEAM (Modell Betriebsfeuerwehr)
- regelmässige Nachkontrollen (organisatorische und technische Sicherheitsüberprüfungen)

Technische Massnahmen gegen Hacker

- Firewall, Anti-Viren-System, Intrusion Detection/Prevention System, Proxy, Honeypot/Honeynet
- so wenig User-Rechte (Tatorte: Internet Browser und File Sharing) wie möglich
- nicht benötigte Dienste deaktivieren bzw. deinstallieren
- regelmässig
  - Security-Patching
  - Aktualisierung der Virendefinitionen
  - System-Reboot
- Banner-Spoofing einrichten

Empfehlung: Nutzenoptimierung



Jede nachfolgende Schicht baut auf den Erkenntnissen / Ergebnissen der vorhergehenden Schicht auf.

Weitere Empfehlungen

- Management Attention
- Projektleitung durch Auftraggeber
- Teamwork sichert Projekterfolg
- präzise Projektplanung:
  - Rollendefinition (inkl. Notfallplan)
  - Mitarbeiterinformation
  - …
- nachvollziehbare Methodik des Auftragnehmers
- White-Box-Approach (Offenlegung des Untersuchungsobjekts) anstatt Black-Box-Approach
- Beim indirekten Ansatz des Ethical Hackings: Schutz des (un-) freiwilligen Komplizen vor den Folgen seines Handelns

Kosten und Aufwand

- externe Kosten (seriöse Durchführung):
  - Minimum: CHF 5`000
  - Maximum: offen
  - Durchschnitt: CHF 15`000 – 30`000
- Zeitaufwand seitens Auftraggeber:
  - Minimum: 30 Minuten pro Testtag
  - Besser: Bereitschaftsdienst Kontaktperson und Systemadministratoren während der Durchführung aller Tests
  - Zusätzlich: Umsetzung der Massnahmen

Beantwortung von Fragen

Besten Dank für Ihr Interesse!
Gerne beantworte ich Ihre Fragen:

Christoph Baumgartner

lic. oec. publ., OPST
CEO / Senior Consultant

info@oneconsult.com
+41 (0)79 421 20 01

OneConsult®

OneConsult GmbH
Zürcherstrasse 73
8800 Thalwil
Schweiz

info@oneconsult.com
Tel. +41 (0)43 443 52 52
Fax +41 (0)43 443 52 62

…mit Sicherheit bessere Lösungen

Schweizerisches Strafgesetzbuch (SR 311.0)

http://www.admin.ch/ch/d/sr/311_0/

Art. 143

Unbefugte Datenbeschaffung

[1] Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

[2] Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Art. 143bis

Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

OSSTMM – Methode und Standard

OSSTMM (Open Source Security Testing Methodology Manual, von ISECOM), http://www.osstmm.org, seit 2001

- am weitesten genutzte, offene Methodik zur Durchführung und Dokumentation technischer Sicherheitsüberprüfungen
- Verhaltenskodex für Tester
- Formulare
- Verschiedene Zertifizierungsmöglichkeiten
  - OPSE (OSSTMM Professional Security Expert)
  - OPST (OSSTMM Professional Security Tester)
  - OPSA (OSSTMM Professional Security Analyst)

Tools (Open Source und Freeware)

- Ports und Dienste: Portscanner Nmap
- Security Scanner
  - Nessus
  - GFILanguard
  - Nikto (spez. Scanner für Webserver)
- generelle OSSTMM-konforme Hilfs-Tools
  - (t)ethereal / tcpdump
  - Telnet
  - Dig/Whois
  - Netcat (Netzwerk Multitool)
  - Ettercap (ARP-Multitool)
  - Remote Administration Tools (Back Doors, Trojaner)
  - Eigenentwicklungen (Skripts und Tools)
  - etc.