Was macht ein Pentester eigentlich den ganzen Tag?

...

June 9, 2018

tbl

WHOAMI

- Senior Security Consultant bei SCHUTZWERK GmbH
  - Technische und Konzeptionelle Security Assessments
  - Organisation von CTF Hacking Contests

- Lehrbeauftragter Hochschule Aalen
  - “Penetration Testing und Computerforensik”

- Kontakt
  - tblaesing@schutzwerk.com
    FFF2 800A 8959 7356 C896 6E16 8E47 0724 75FE 5EDE

Agenda

- Was ist ein Pentest?
- Wie ist der typische Ablauf?
- Welche Skills braucht man?
- Pentesting als Karriere?

Was ist ein Pentest?

Penetrationstest, kurz **Pentest**, ist der fachsprachliche Ausdruck für einen **umfassenden Sicherheitstest** einzelner Rechner oder Netzwerke jeglicher Größe. Unter einem Penetrationstest versteht die **Sicherheitsfachperson** in der Informationstechnik die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die ein **Angreifer** (ugs. „Hacker“) anwenden würde, um unautorisiert in das System einzudringen (Penetration).

Quelle: https://de.wikipedia.org/wiki/Penetrationstest_(Informatik)

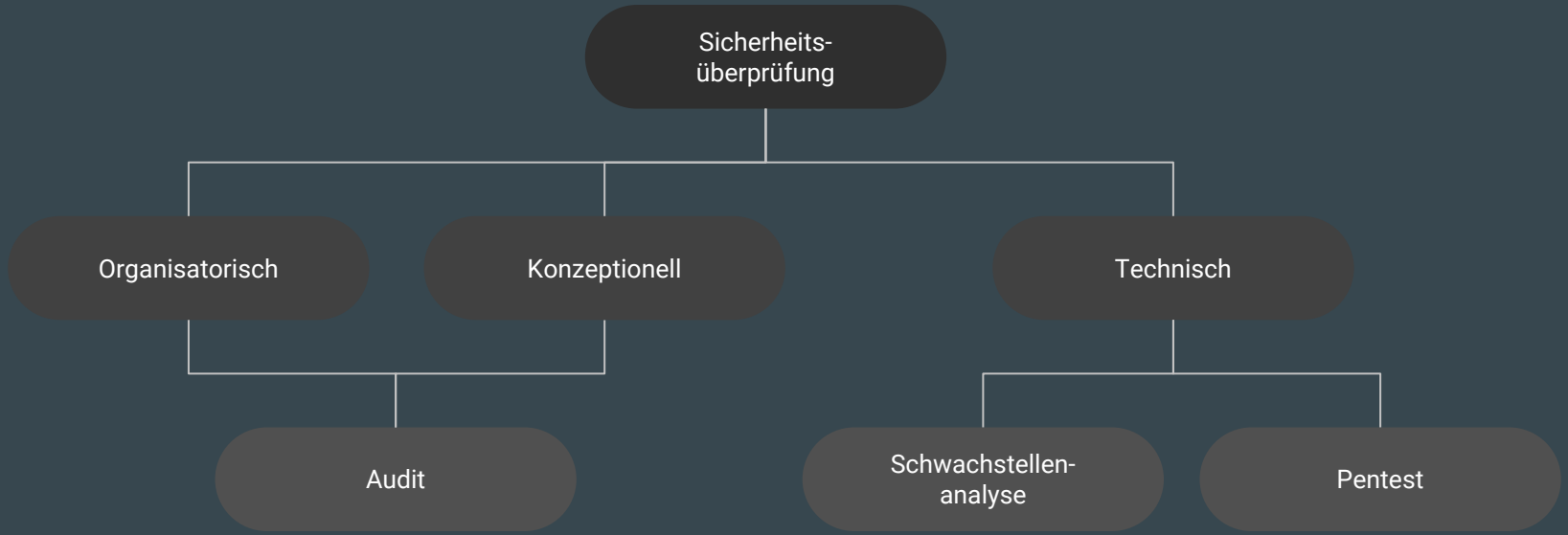
... oder in kurz

... hack all the stuff before the bad guys do it!

und was heißt das jetzt genau?

- Vielfältige Bedrohungsszenarien
  - Motivierte Hackerangriffe (Wirtschafts- bzw. Konkurrenzspionage, Sabotage, Erpressung)
  - Schadsoftware (Würmer, Root-Kits, Bot-Netze etc.)
  - Unmotivierte Hackerangriffe (Spieltrieb, Missbrauch von Servern als Speicherplatz für illegale Daten oder zur Verschleierung illegaler Internet-Aktivitäten etc.)
  - Unmotivierte Angriffe bzw. fahrlässige Eingriffe durch Mitarbeiter oder Besucher (Spieltrieb, Fehlbedienung, unautorisierte IT-Administration)
- Mögliche Konsequenzen bei einem IT-Sicherheitsvorfall sind sehr vielfältig
  - Einbußen der Reputation (auch Verlust)
  - Straf-/Zivilrechtliche Konsequenzen
  - Finanzielle Einbußen (direkt und indirekt)
- IT-Sicherheit wichtig für viele Unternehmen und staatliche Einrichtungen
  - Wie kann man die getroffenen Sicherheits-Maßnahmen überprüfen?

Wie kann ich die Sicherheit meiner IT überprüfen?



Über Hüte und Boxen ... oder welche Art Pentest *machst* du?

Black-Box Test

- Keine Informationen über Testobjekt

Grey-Box Test

- Grundlegende Informationen über Testobjekt (z.B. IP-Adressen, URLs, SW Versionen, ...)

White-Box Test

- Vollständige Informationen über Testobjekt (z.B. Sourcecode, interne Dokumentation, ...)

Über Hüte und Boxen ... oder welche Art Pentester *bist* du?

Black Hat Tester

- Unabhängige Untersuchung und Ausnutzung von Lücken
- Keine Kollaboration mit Hersteller

Grey Hat Tester

- Unabhängige Untersuchung und Ausnutzung von Lücken
- Kollaboration mit Hersteller (z.B. Responsive Disclosure)

White Hat Tester

- Untersuchungen nur in direkter Absprache durch oder mit Auftraggeber/Hersteller

Phasen eines Pentests

01	**Vorbereitung**	• Rechtl. Rahmenbedingungen • Angebotserstellung • Kick-Off
02	**Durchführung**	• Identifizierung Angriffsflächen • Ausnutzen der Schwachstellen • Aufräumen nach Angriff
03	**Dokumentation**	• Risiko-Klassifizierung der Befunde • Erarbeitung passender Maßnahmen • Erstellung Abschlussbericht
04	**Nachbereitung**	• Abschlusspräsentation • Einleitung Gegenmaßnahmen • Ggf. Re-Test

Phasen eines Pentests

01	**Vorbereitung**	• Rechtl. Rahmenbedingungen • Angebotserstellung • Kick-Off
02	**Durchführung**	• Identifizierung Angriffsflächen • Ausnutzen der Schwachstellen • Aufräumen nach Angriff
03	**Dokumentation**	• Risiko-Klassifizierung der Befunde • Erarbeitung passender Maßnahmen • Erstellung Abschlussbericht
04	**Nachbereitung**	• Abschlusspräsentation • Einleitung Gegenmaßnahmen • Ggf. Re-Test

Rechtliche Voraussetzungen

- ∫ 202c StGB “Hackerparagraf”

  Nach ∫ 202c Abs. 1 Nr. 2 wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer eine Straftat nach

  ∫ 202a (Ausspähen von Daten) oder

  ∫ 202b (Abfangen von Daten) vorbereitet,

  indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht.
  (Quelle: https://dejure.org/gesetze/StGB/202c.html)

- Diskussionen zum Thema in 2007-2009
  - Ist denn jetzt Nmap, netcat, etc. verboten?
  - Was ist mit Linux Distributionen?
  - Reihenweise Verfassungsbeschwerden, Selbstanzeigen, ...

Rechtliche Voraussetzungen II

- Stellungsnahme vom „European Institute for Computer Antivirus Research“

  „Aus der Dokumentation sollte sich zweifelsfrei ergeben, dass die Software nicht beschafft wurde, um Straftaten zu begehen, sondern um gutartige Tätigkeiten auszuüben. Auch der Einsatz des Programms ist entsprechend – schriftlich und veränderungssicher – zu dokumentieren.“

  (Quelle: http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf)

- Pentests sind nur unter bestimmten Voraussetzungen legal
  - Zusätzlich Datenschutz- und Vertraulichkeitserklärungen
  - Daten in Zielsystem und von Mitarbeitern des Auftraggebers

Implikationen auf Angebotserstellung

- Projektbeschreibung
  - Zusammenfassung der aktuellen Situation
  - Zu Beauftragende Dienstleistungen (z.B. PenTest, Schwachstellenanalyse, WASA, MASA, ...)
- Projektaufwände und -kosten
  - Kosten für gewählte Dienstleistungen und Aufwände
- Leistungsbeschreibung
  - Verwendete Werkzeuge/Standards, Vorgehensweise
- Rechtliche Rahmenbedingungen
  - Notwendigkeit der Gegenzeichnung aller Benötigten Unterlagen (z.B. Prüfgenehmigung, ...)
- Informationen über Projektleiter/Pentester
  - Sollte kein direktes Anstellungsverhältnis vorliegen, sollte das erwähnt werden

Kick-Off

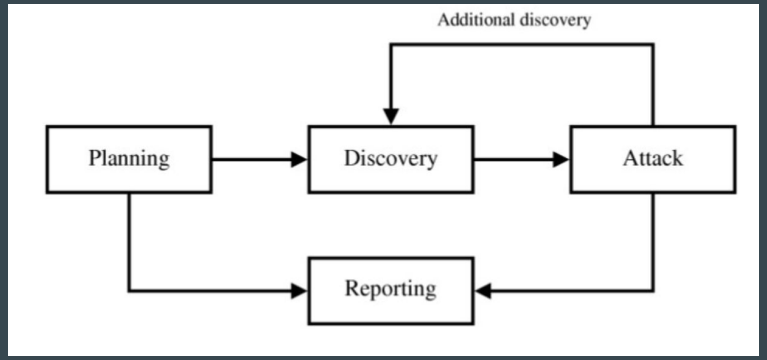
- Erläuterung des Untersuchungsobjekts durch den Auftraggeber
- Definition und Bewertung der relevanten Bedrohungsszenarien (Angriffe, Systemausfälle etc.) und ggf. Ableitung besonderer Prüfungsschwerpunkte
- Klärung rechtlicher Rahmenbedingungen (Datenschutz, Genehmigung des Assessments durch eventuell involvierte Dritte etc.)
- Klärung technischer Rahmenbedingungen (IDS, WAF, Datensicherung, Besonderheiten bei kritischen Produktivsystemen etc.)
- Aufnahme besonderer Anforderungen und Wünsche
- Definition des Projektverlaufs, der Verantwortlichkeiten und der Termine

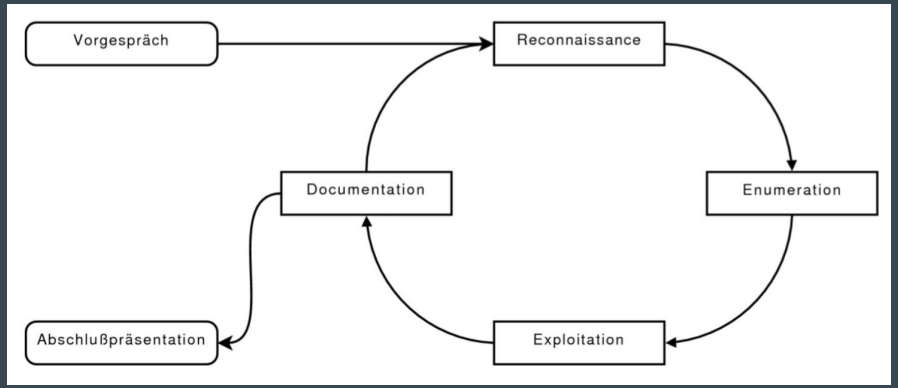
Phasen eines Pentests

01	Vorbereitung	• Rechtl. Rahmenbedingungen • Angebotserstellung • Kick-Off
02	**Durchführung**	• Identifizierung Angriffsflächen • Ausnutzen der Schwachstellen • Aufräumen nach Angriff
03	Dokumentation	• Risiko-Klassifizierung der Befunde • Erarbeitung passender Maßnahmen • Erstellung Abschlussbericht
04	Nachbereitung	• Abschlusspräsentation • Einleitung Gegenmaßnahmen • Ggf. Re-Test

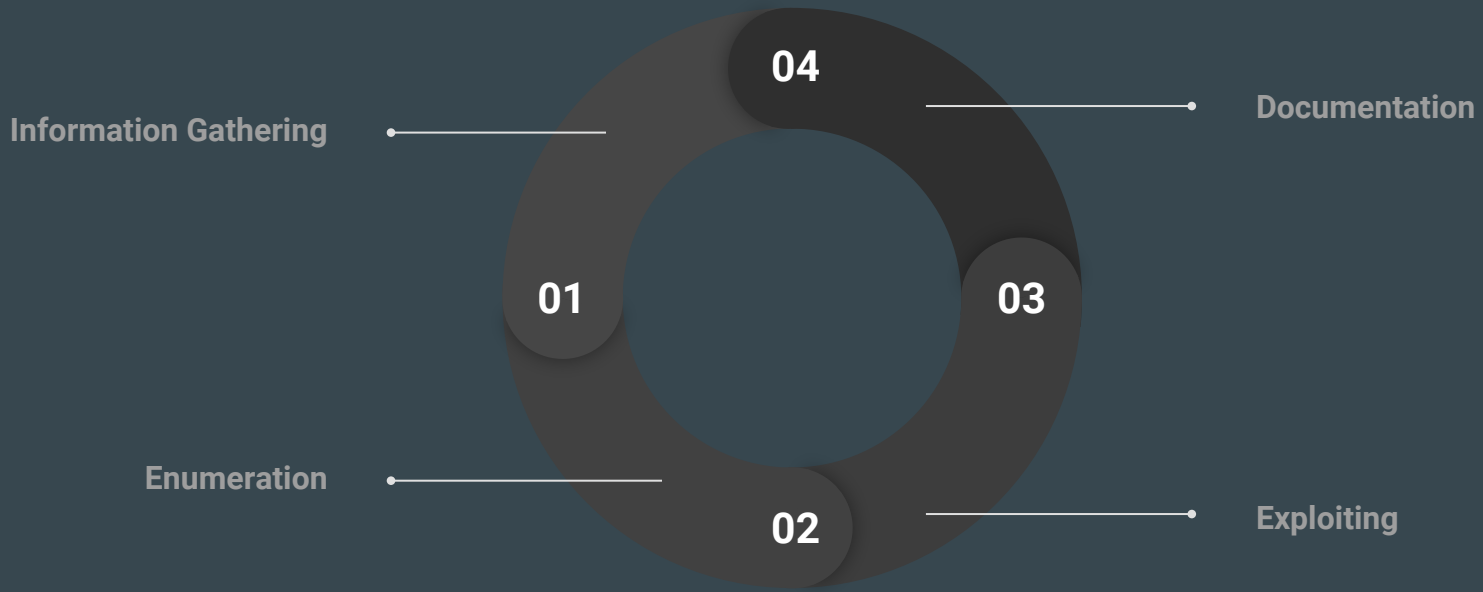
Standards zur Durchführung

- BSI
- Ptes
- OSSTMM
- ISSAF
- NIST
- OWASP
- ...





Ablauf des eigentlichen Pentests



Phasen eines Pentests

01	**Vorbereitung**	• Rechtl. Rahmenbedingungen • Angebotserstellung • Kick-Off
02	**Durchführung**	• Identifizierung Angriffsflächen • Ausnutzen der Schwachstellen • Aufräumen nach Angriff
03	**Dokumentation**	• Risiko-Klassifizierung der Befunde • Erarbeitung passender Maßnahmen • Erstellung Abschlussbericht
04	**Nachbereitung**	• Abschlusspräsentation • Einleitung Gegenmaßnahmen • Ggf. Re-Test

Doku the Hell out of ...

- Grundlage für Datensammlung und Berichtswesen ist Modularisierung
  - Überblick behalten
  - Informationen verwalten und (wieder)verwenden
  - Aufbereitung für eventuellen Austausch
- Interne Dokumentation vs offizieller Abschlussbericht
  - Dokumentation während des Pentests
  - Dokumentation für Auftraggeber
- Dokumentation ist ein sehr dynamisches Thema
  - Aufbau und Stil sind sehr variabel
  - Einhaltung der Best-Practices
  - Aushängeschild für Unternehmen

Ausrichtung und Aufbau des Berichts

- Zielgruppe
  - Management
    - Oberes Management (CEO, CFO, CISO, ...)
    - Technisches Management (Abteilungsleiter, Überwachung der Maßnahmen-Umsetzung)
  - Techniker (Umsetzung der Maßnahmen)
  - Drittfirmen (Outsourcing-Partner, andere Pentester, ...)
- Häufig sollen alle Zielgruppen abgedeckt werden
  - Unterschiedlicher Aufbau, Umfang, Detailtiefe und Ausrichtung
  - Prosatext vs Übersichts-Tabellen
  - Graifken und Diagramme
- Neutrale und unabhängige Darstellung der Sachverhalte
  - Diplomatischer Abstand zu Befunden, wissenschaftliche Herangehensweise
  - Aggressive Schreibweise hat mögliche Blockierung bei der Beseitigung zur Folge
- Berichtsgenerierung vs Händisches Schreiben

Abschlussbericht

- Folgende Themen sollten von einem Abschlussbericht abgedeckt werden
  - Deckblatt
  - Management Summary
  - Einleitung (inkl. Projektbeschreibung)
  - Vorgehensweise und Erläuterung Risikoklassifizierung
  - Übersicht Befunde
  - Detailbeschreibung Befunde (inkl. Maßnahmen)
  - (Zusammenfassung)
- Bericht sollte auch alle rechtlich relevanten Aspekte abdecken
  - Wer sind die Verantwortlichen auf beiden Seiten?
  - Was wurde genau gemacht und von wem?
  - Mit welchem Ergebnis?
- https://github.com/juliocesarfort/public-pentesting-reports

Darstellung der Befunde

- Was wurde gefunden?
  - Allgemeine Beschreibung des Sachverhalts
  - Hier noch keine Risikoabschätzung!
- Wie wurde es gefunden und ausgenutzt?
  - Beschreibung der technischen Details/PoC und des möglichen Risikos
  - Ggf. Angabe der Tool-Konfiguration
  - Einfügen von Screenshots
- Was kann zur Beseitigung der Problematik getan werden?
  - Beschreibung möglicher Maßnahmen
  - Hinweise auf andere Quellen (z.B. OWASP TOP10 Mitigation)
- Risikobewertung im Kontext des Kunden

Bewertung Kritikalität

- Für was werden solche Bewertungen verwendet?
  - Entscheidungsgrundlage für Patch- und Konfigurationsmanagement
  - Im Rahmen einer Zertifizierungen, z.B. ISO 27k, PCI-DSS, SOX, ...
  - Prüfung durch Revision/Audit des Unternehmens
- Möglichkeiten der Bewertung
  - Qualitativ (Kritisch, Hoch, Mittel, Niedrig)
  - CVSS Score (Wert zwischen 1-10)
  - DREAD (Wert zwischen 1-10)
  - ...
- Meistens werden Schwachstellen qualitativ bewertet
  - Kunde hat einfache Aussage und kann entsprechend reagieren
    - Problem der Ungenauigkeit, z.B. SSL Heartbleed: E-Commerce Unternehmen vs. Webpräsenz „Tante Emma“-Laden

Phasen eines Pentests

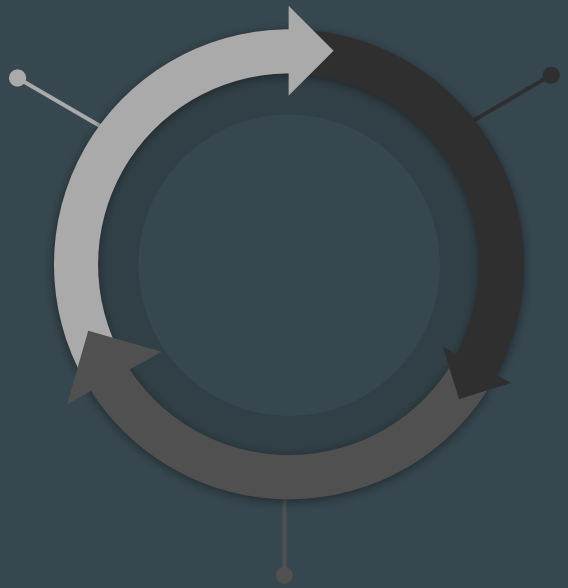
01	**Vorbereitung**	• Rechtl. Rahmenbedingungen • Angebotserstellung • Kick-Off
02	**Durchführung**	• Identifizierung Angriffsflächen • Ausnutzen der Schwachstellen • Aufräumen nach Angriff
03	**Dokumentation**	• Risiko-Klassifizierung der Befunde • Erarbeitung passender Maßnahmen • Erstellung Abschlussbericht
04	**Nachbereitung**	• Abschlusspräsentation • Einleitung Gegenmaßnahmen • Ggf. Re-Test

Skillsssssssssssss...

Welche Skills brauchst du?

Technisch

- Administration von
  - Windows Desktop
  - Windows Domain
  - Linux und Unix
  - Netzwerk Infrastruktur
- Software Entwicklung
  - Scripting (Python, Powershell, ...)
  - Managed Langs (Dalvik, Java, .NET)
  - Unmanaged Langs (C/C++)



Nicht-Technisch

- Kommunikation (Verbal und Geschrieben)
  - E-Mails
  - Abschlussbericht
  - Präsentation
- Professionalität
  - Respekt gegenüber Anderen
  - Erwartungen an Personen/Meetings/...
  - Nicht-Techniker Kompatibilität
- Mindset
  - Never give up / “Try Harder”
  - Motivation etwas zu bewegen
- Ethisches Verhalten
  - White Hat vs. Black Hat
  - Verantwortung (z.B. kritische Infrastrukturen)

Offensiv/Defensiv

- System Enumeration und Fingerprinting
- Exploiting von Windows/Linux/Netzwerk-Systemen, Protokollen, Web applikationen, Software, ...
- Reverse Engineering, AV Evasion,
- Social Engineering

Karriere als Pentester?!

Corporate vs Consulting vs Freiberufler

- Vielfalt der Projekte und Menschen
  - Organisatorische vs Konzeptionelle vs Technische Projekte
  - Kleinere vs große Teams/Abteilungen
  - Aktualität der eingesetzten Technologien
  - Fort-/Weiterbildung
  - Karrierewege Technik vs Management
  - Unterschiede Gehalt/Lohn
- (Mehr-)Aufwand und Kosten
  - Werbung/Akquise/Networking/Steuer
- Bug Bounties
  - noch lukrativ?!
- Welche Freiheiten brauche ich?

Wohin von hier?

- Persönliche Einstellung und Motivation
  - “Learning Never Stops” / “TRY HARDER”
- Zertifizierungen
  - OSCP, OSCE, ...
  - CEH, CISSP
  - ...
- Technische Weiterbildung/Einstieg
  - CTFs/Wargames/HackMes (VulnHub, HackTheBox, ...)
  - YT/Screencasts/GitHub
- Aufbau Reputation
  - CVEs
  - Vorträge/Konferenzen
  - (Social-)Networking

Q & A

backup slides

Tools

Tooling

- Es gibt tausende verschiedene Tools
  - Welches Tool für welche Aufgabe?
  - Welche Version brauche ich in welcher Situation?
  - Ggf. Eigenentwicklung(en)

- Wissen > Tooling
  - Verstehen von Kern-Technologien wichtiger
  - Verstehen defensiver/offensiver Techniken

Tools zur Informationsgewinnung

- ${Suchmaschine}
  - Google, Bing, duckduckgo, ...
  - Social Networks (FB, Twitter, G+, aber auch: StackOverflow, ...)
  - Shodan
  - Geoip, Whois, Traceroute
- Meta-Daten
  - Gemeinsame Kommunikation, z.B. Mail-Header, Jabber, ICQ, WhatsApp, ...
  - Webseitenbesuche einer Domain die unter eigener Kontrolle ist: z.B. Download Lebenslauf.pdf
- NMap (+NSE)
- TheHarvester, Recon-ng
- Social Engineer Toolkit („SET“)

Tools zur Informationsgewinnung II

- DNS
  - host
  - dig
  - DNSRecon
- SMB/CIFS
  - nbtscan
  - enum4linux
- SNMP
  - onesixtyone
  - snmpcheck
  - snmpwalk
- HTTP
  - Nikto
  - sslscan
  - dirb
  - dirbuster
  - w3af

Tools zur Identifizierung von Schwachstellen

- Vulnerability Management
  - OpenVAS
  - Nessus
  - Nexpose
  - Qualys
- WebApp
  - Portswigger BurpSuite
  - OWASP ZAP
  - ProxyStrike
  - w3af
  - nikto
  - Dirb(uster)
  - SQLMap/SQLNinja/...
  - WPScan

Tools zur Privilege Escalation / Post-Exploitation

- local root exploits
- Konfigurationsfehler
- Passwords
  - Hydra
  - John the Ripper, Rainbow tables, (ocl)Hashcat, ...
- Credentials dumping
  - Mimikatz, groups.xml, unattend.xml, ...
- Anti-Antivirus
  - Veil-Framework
  - Shellter

Information Gathering