

## Security Audits - Fingerprinting

### Analyse und Sicherheitsbewertung von Computersystemen und Netzwerken

**Autor:**

Dr. Klaus Schmoltzi  
Warp9 GmbH  
Rothenburg 14 -16  
48143 Münster  
Email: kontakt@warp9.de

**Datum:**

31. Mai 2011

**Version:**

1.5



Jede Art von Kopie, Verteilung oder Veröffentlichung der Informationen in diesem Dokument in gedruckter oder elektronischer Form ist nicht gestattet, außer es liegt eine schriftliche Genehmigung der Warp9 GmbH vor.  
Dieses Dokument unterliegt dem ausschließlichen und unbeschränkten Nutzungs- und Urheberrecht.

© 2011 Warp9 GmbH, Münster

1. EINLEITUNG .....	3
2. DURCHFÜHRUNG VON SECURITY-AUDITS.....	3
3. VORTEILE DES FINGERPRINTINGS.....	6
4. GLOSSAR .....	6
5. IMPRESSUM .....	7

## 1. Einleitung

Den Betreibern von IT-Systemen im Internet und Intranet ist selten der Sicherheitsstand der aktuell eingesetzten Software bekannt. Falls wichtige Aktualisierungen (Updates) nicht eingespielt sind, können Computersysteme wie z.B. Webserver, Mailserver und Firewalls aber auch VPN-Verbindungen aus dem Internet heraus angegriffen werden. Ein Cracker kann mit entsprechenden Exploits in Systeme eindringen, Veränderungen vornehmen sowie Daten stehlen oder verändern.

Der bei einem erfolgreichen Angriff zu Buche schlagende Schaden kann im voraus nicht abgeschätzt werden, ist aber meistens immens. Dabei ist das Bedrohungspotential in den letzten Jahren stetig gewachsen. So ist die Computerkriminalität im Bereich „Ausspähen und Abfangen von Daten“ nach der *Polizeilichen Kriminalstatistik*<sup>1</sup> des Bundeskriminalamt (BKA) im Jahr 2010 um ca. 32 % gegenüber dem Vorjahr angestiegen. Die Gesamtzahl liegt mittlerweile bei 15.190 Fällen. Die Aufklärungsquote liegt bei nur 24 %!

Zu beachten ist außerdem, dass für Schäden, die einem Unternehmen aus der IT entstehen können, die jeweiligen IT-Verantwortlichen nach Lage des Einzelfalls auch persönlich haftbar sind. Zum Personenkreis der IT-Verantwortlichen gehören u.a. Vorstand, Geschäftsführer, Behördenleiter, IT-Leiter und IT-Mitarbeiter. Entsprechende Gegenmaßnahmen zu veranlassen ist daher auch aus dem Interesse der Verantwortlichen sinnvoll und notwendig.

Eine wichtige Maßnahme, um mögliche Angriffspunkte auf die vorhandenen IT-Infrastruktur aufzuzeigen, bietet ein Security-Audit. Security-Audits können in einer großen Spannweite durchgeführt werden. Um sich einen Überblick zu dem aktuellen Sicherheitszustand der IT-Systeme zu verschaffen, reicht oft schon ein Fingerprinting aus. Nach der Auswertung der dabei erhaltenen Ergebnisse, können weitere Schritte unternommen werden.

## 2. Durchführung von Security-Audits

Die Warp9 GmbH bietet Security-Audits (oft auch als Penetrationstests bezeichnet) für die komplette IT-Infrastruktur des Kunden an. Die Penetrationstests werden so durchgeführt, dass die Zielsysteme nicht beschädigt werden und die darauf laufenden Dienste weiterhin erreichbar sind. Stattdessen werden mit „sanften Mitteln“ Hinweise gesammelt, die sich auch ein potentieller Angreifer beschaffen kann, bevor er mit dem eigentlichen Angriff beginnt. Diese Herangehensweise wird allgemein als Fingerprinting bezeichnet.

Die Vorgehensweise des Audits orientiert sich dabei an den Standards, die vom Bundesinstitut für die Sicherheit in der Informationstechnologie (BSI) herausgegeben werden. Insbesondere wird die BSI Studie „Durchführungskonzept für Penetrationstest“<sup>2</sup> herangezogen.

Für die Durchführung eines Security-Audits gibt es prinzipiell mehrere Möglichkeiten, wie sie anhand der Abbildung 1 dargestellt sind:

---

<sup>1</sup> [http://www.bka.de/pks/pks2010/download/pks2010\\_imk\\_kurzbericht.pdf](http://www.bka.de/pks/pks2010/download/pks2010_imk_kurzbericht.pdf)

<sup>2</sup> <http://www.bsi.bund.de/literat/studien/pentest/penetrationstest.pdf>

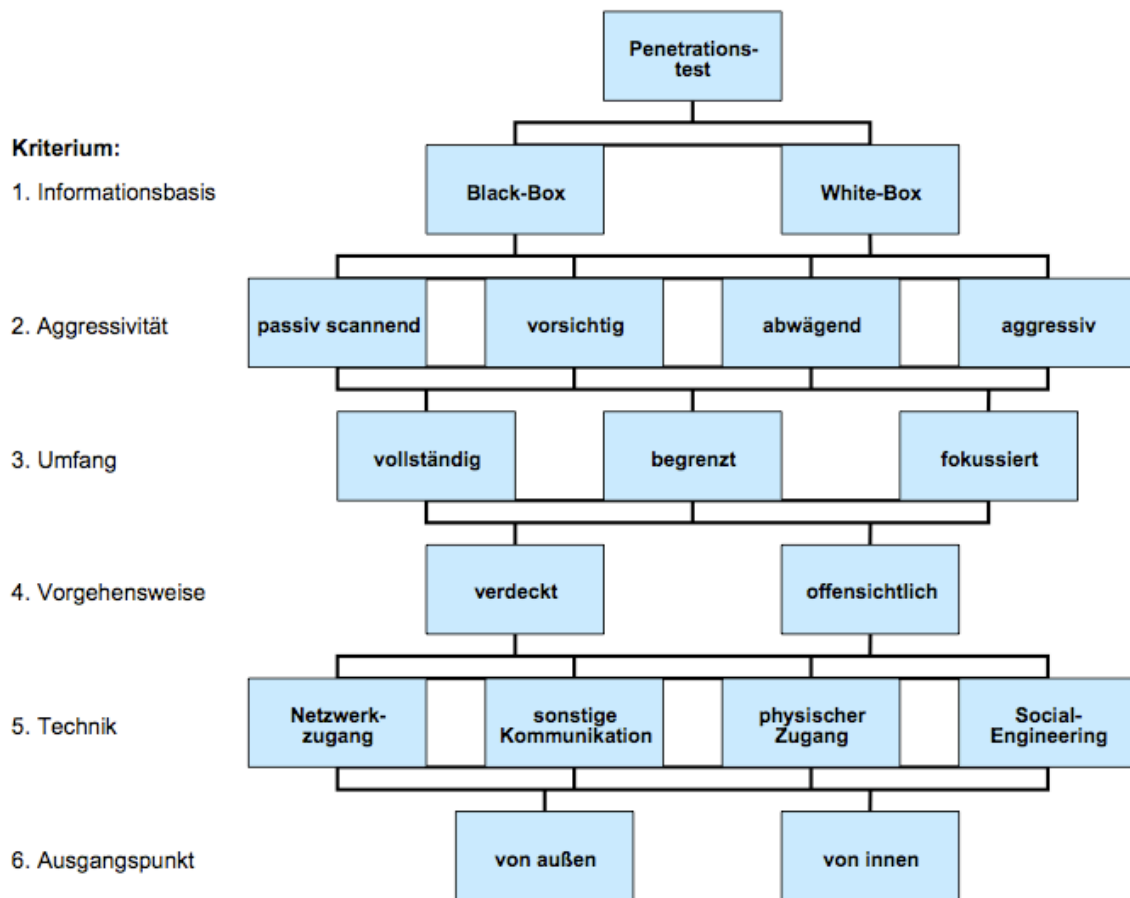


Abbildung 1: Durchführung eines Security-Audits nach BSI-Vorgaben

In Absprache mit dem Auftraggeber wird zwischen folgenden Alternativen gewählt:

- Informationsbasis: **Black-Box oder White-Box**
- Aggressivität: **passiv bis vorsichtig**
- Umfang: **vollständig, begrenzt, fokussiert**
- Vorgehensweise: **verdeckt oder offensichtlich**
- Technik: **Netzwerkzugang**
- Ausgangspunkt: **von außen oder von innen**

Der jeweils verwendete Schwachstellenscanner versucht die Versionsnummer der für die Bereitstellung eines Dienstes (z.B. Mail- oder Webdienst) installierten Software (z.B. Sendmail, Postfix, Exchange, Apache, Microsoft IIS) zu detektieren (Fingerprinting). Anhand der festgestellten Versionsnummer wird anschließend durch eine Datenbankabfrage nach einer potentiellen Schwachstelle gesucht.

Im diesem Schritt wird nicht versucht eine herausgefundene Schwachstelle auch per Exploit auszunutzen! Dies wird erst (falls gewünscht) in einem zweiten Schritt nach Absprache mit dem Auftraggeber durchgeführt.

Generell wird das Fingerprinting von einem Rechner aus dem Internet heraus durchgeführt, so wie es in Abbildung 2 dargestellt ist.

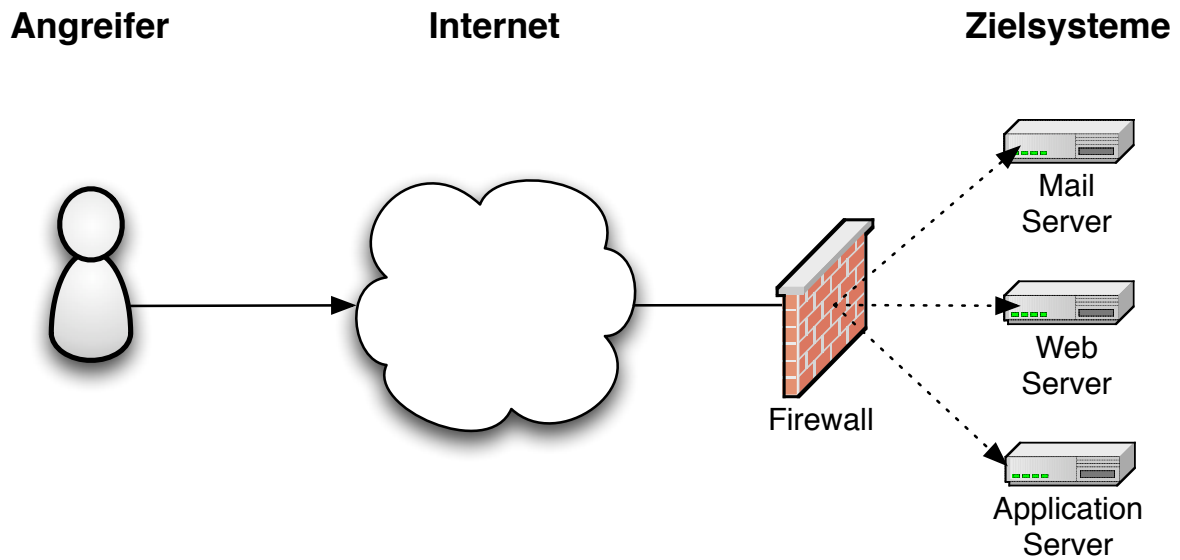


Abbildung 2: Angriffsszenario

Nach Abschluss des Security-Audits wird von der Warp9 GmbH ein aussagekräftiger Abschlussbericht erstellt und in einem Meeting werden dem Auftraggeber die Ergebnisse präsentiert.

### 3. Vorteile des Fingerprintings

Der vorsichtig durchgeführte Penetrationstest hat folgende Vorteile:

- Die gescannten Systeme werden nicht beschädigt.
- Anhand der Fingerprints wird nach Schwachstellen gesucht.
- Die gefundenen Schwachstellen können verifiziert und beseitigt werden.
- Härtere Tests (Exploits) werden nur nach Absprache mit dem Auftraggeber durchgeführt.
- Regelmäßige Wiederholungen des Fingerprintings ergeben einen guten Überblick, ob die eigene IT-Infrastruktur potentiellen Gefahren ausgeliefert ist.
- Durch die Auswertung der Ergebnisse wird die Sensibilität der jeweiligen Administratoren erhöht.
- Mögliche Haftungsrisiken für die IT-Verantwortlichen werden minimiert.

### 4. Glossar

**Cracker** – Eine Person, die ohne Erlaubnis in fremde Computersysteme eindringt

**Exploit** – Ein Skript oder Programm, das die Schwachstellen von anderen Programmen ausnutzt

**VPN** – Virtual Private Network ist die Zusammenschaltung von mehreren Netzen zu einem „virtuellen“ Netzwerk. Dies wird mit einer geeigneten Software realisiert, die die Verbindung zu den Netzen durch einen Tunnel (VPN-Tunnel) herstellt.

## 5. Impressum

**Firma:** Warp9 GmbH  
**Vertretungsberechtigte Geschäftsführer:** Dr. Klaus Schmoltzi  
**Sitz der Gesellschaft:** Rothenburg 14-16, 48143 Münster  
**Registergericht:** Amtsgericht Münster  
**Registernummer:** HRB 5465

**Umsatzsteuer-Identifikationsnummer gemäß § 27a Umsatzsteuergesetz:** DE201558029  
**Finanzamt Münster-Innenstadt:** 337 5911 0768

**Inhaltlich Verantwortliche gemäß § 6 MDSStV:** Dr. Klaus Schmoltzi

**Haftungshinweis:** Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der hier verlinkten URLs sind ausschließlich deren Betreiber verantwortlich.

Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen. Die Firma Warp9 GmbH richtet sich im Wesentlichen nach der Schreibweise der Hersteller. Andere hier genannte Produkte können Warenzeichen des jeweiligen Herstellers sein.

**Warp9®** und **Transwarp®** sind eingetragene Warenzeichen der Warp9 GmbH.

Warp9 GmbH  
Rothenburg 14 -16  
48143 Münster

Phone: +49 251 973 190  
Fax: +49 251 973 192 9  
E-Mail: [kontakt@warp9.de](mailto:kontakt@warp9.de)  
Internet: <http://warp9.de>