SVS Bachelor-Projekt Network Security

Blatt 4: Sniffing und Scanning

Louis Kobras
6658699

Utz Pöhlmann
6663579

1 Vertrautmachen mit der Umgebung

1.2

SurfingVM hatte keine Internetverbindung; Reparatur mithilfe des Zurücksetzens der Datei `/etc/udev/rules.d/70-persistent-net.rules` und Reboot beider VMs (wie nach Aufgabeninfo).

- **Standartgateway: 192.168.254.1**
- IP: 192.168.254.44
- **DNS-Nameserver: 10.1.1.1** (ermittelt mit `route -n`, bestätigt mit `nslookup ubuntu.com`)

1.3

- Netzwerkkarte 1: eth0, 172.16.137.222
- Netzwerkkarte 2: eth1, 192.168.254.1
- VMWare-Standart-Gateway: 172.16.137.2

1.4

- Ping an 10.1.1.2 aus beiden VMs erfolgreich (0% Package loss)

2 Sniffing mit tcpdump

2.1

- `tcpdump` listet alle Pakete auf, die über die Netzwerkkarte laufen
- Capture-Filter zum Filtern und Sortieren der gefangenen Packages

2.2

- Kommando: `sudo tcpdump -p -i eth1 -s 0 -vvv udp port 53 > log`[1] ([1], [2])

Anmerkung: Output-Prokotolle vgl. Anhang: Sniffing (S. 8)

Anmerkung: tcpdump kennt nur wenige Protokolle und gibt, wenn er ein Protokoll nicht erkennt, IP an.

Bezüglich der Antwort: Die erste Zeile ist jeweils Meta-Information. Die zweite Zeile ist eine Anfrage unserer Domain an unseren Nameserver, welcher dann an Google weiterfragt, wo die Nameserver von Google die Anfrage durch reichen.

[1] -p: weil Aufgabe. -i ethX: Adapter, der gelistened werden woll. -s 0: Größe des Capture in Bytes (0=alle). -vvv: alle Paketinformationen ausgeben. «schnittstelle» port «port». > log: in die Datei 'log' echoen, die ggf. im $(pwd) angelegt wird.

2.3

- Kommando: `sudo tcpdump -p -i eth1 -s 0 -vvv '(tcp port 80) or (tcp port 443)' > log`[2] ([1])

Output: vgl. Output des HTTPS-Sniffing (S. 8)

2.4

Neuer Befehl: `sudo tcpdump -p -i eth1 -s 0 -vvv -A 'tcp port 80'` Output vgl. Anhang Output des HTTP-Sniffing (S. 8)

2.5

- Aufrufen der URL `http://10.1.1.2/verysecure/`
- Eingabe der Login-Daten `alice:sehrgeheim`
- Login-Daten im Package `Authorization: Basic YWxpY2U6c2V0cmdlaGVpbQ==` ⇒ Base-64-verschlüsselt.
- Entschlüsselung ergibt: `alice:sehrgeheim`

3 Sniffing mit dsniff und urlsnarf

3.1 urlsnarf

Befehl:`sudo urlsnarf -i eth1 > log`
Aufbau des Output: IP - Timestamp - Adresse - Protokoll - Browser - Systemdaten
Befehl greift alle HTTP-Pakete vom angegebenen Adapter ab und zeigt ihre Daten an.

3.2 dsniff

Befehl: `sudo dsniff -i eth1 > log`
Aufbau des Output: Timestamp - Senderadresse - Empfängeradresse - Adresse - Protokoll - Host - Paketinhalt (decoded)
Liest den Inhalt von HTTP-Paketen aus und decodiert (zumindest Base-64).

4 Sniffing mit Wireshark

4.1

Wireshark liefert eine graphische Darstellung der gesnifften Pakete in lesbarer Tabellenform und zeigt den Inhalt der Pakete an.

4.2

Display-Filter: Bestimmt, welche der aufgefangenen Pakete angezeigt werden.

Capture-Filter: Bestimmt, welche Pakete aufgefangen werden.

4.4

- `eth1` liegt nahe, da dieses Interface das Gateway für die SurfingVM bereitstellt (Capture-Filter).
- Alternativ zur Interface-Wahl kann ein Display-Filter zur Steuerung des Outputs erstellt werden.

[2] s.o., tcp port 80 für HTTP, tcp port 443 für HTTPS

4.5

Es wird nur ein Ping gesendet. Der Server pingt zurück. Die Pings werden über ICMP[3] übertragen.

Der Klient DARF die Daten so lange behalten, wie er will. Jedes Paket hat einen time-to-live-Eintrag; ist dieser überschritten, wird das Paket erneut angefordert.

Weil Linux den DNS nicht cached, erwarten wir die gleiche Antwort.

Wir bekommen die gleiche Antwort, was bedeutet, Linux cached den DNS nicht.

Der Browser sendet Pings über TCP und anschließend HTTP. Dies wechselt sich stetig ab.

Es würde erwartet, dass in beiden Fällen das Gleiche passiert

4.6

Erstellen des Filters durch Rechtsklick auf einen HTTP-Eintrag und Auswahl des Menüpunktes “Apply as filter”.

4.7

Funktion liegt unter Menüreiter “Analyze”.

Ausgabe eines HTTP-Response öffnet Popup, in welchem der Content des Package angezeigt wird. Es kann zwischen verschiedenen Darstellungen gewählt werden (Raw/ASCII, HexDump, C Arrays)

4.8

- Server starten auf RoutingVM
- Auf SurfingVM mit telnet auf Server einwählen
- Auf RoutingVM Wireshark starten
- Auf SurfingVM Dinge tun
- Auf der RoutingVM kann der gesamte Chat nun als TCP-Packages ausgelesen werden (u.a. auch die Login Daten)

4.9

- Aufrufen von `https://de-de.facebook.com`
- Verwendete Protokolle: TCP, TLSv1
- Es wurden nicht alle Pakete in Wireshark angezeigt (Nummerierung nicht durchgehend). Kein Filter eingestellt. Theorie: HTTPS wird verborgen.

5 ARP-Spoofing

5.1

Ablauf des ARP-Spoofings:

Der ’Angreifer’ klemmt sich zwischen Remote Host und Remote Server und gibt sich in beide Richtungen als der jeweils andere Gesprächsparter aus. Er fängt Pakete aus beiden Richtungen ab, liest sie aus, und schickt sie unter dem Namen des ursprünglichen Absenders weiter. Funktionsweise von `arpspoof`:

- Abzufangender Adapter wird angegeben
- Entity, die gespooft werden soll
- Domain, deren eingehender Datenstream mitgelesen werden soll

[3] Internet Control Message Protocol

5.2

Befehl: `sudo arpspoof 172.16.137.2`. Es wird eine lange Reihe identischer arp-Replys ausgegeben.

5.3

Es wurde der Wireshark-Adapter “any” ausgewählt.

5.4

Nach Setzen des Display-Filters auf `ICMP` wurde durch den Zeitintervall die IP-Adresse 172.16.137.146 ermittelt (vgl. Grafik 1: Anhang: Wireshark-Screenshot).

5.5

- Display-Filter `ip.addr==172.16.137.146 && pop`
- beliebigen Eintrag ausgewählt und per Rechtsklick “Follow TCP Stream”
- Nutzerdaten: `USER bumblebee`, `PASS Optimus Prime`
- hat eine ungelesene Mail von root@labservervm
- Alternativen: EInhalten von Verdecktheit und Verborgenheit (GSS Sicherheitsziele :P)

5.6

- Browser/Version: Mozilla/5.0
- URL: http://10.1.1.2/secure/secret.html
- Login-Daten: Base-64 encoded im Kopf des Paketes; Daten: `admin:geheim`

Keine Widersprüche zwischen Erkenntnissen festgestellt.

6 Scanning mit nmap

6.1

Die 5 coolsten NMAP-Funktionen (nach [4]):

Security Audits	Network Inventory	Monitoring Host Uptime
Managing Service Upgrade Schedules	Monitoring Service Uptime	

6.2

- Skript vgl. Anhang Anhang: Ping-Skript (Aufgabe 6.2) (S. 8); gewählte Sprache: Bash (Output vgl. Anhang: 6.2 (IP-Liste) (S. 9))

6.3

Im Gegensatz zum `ping`, welcher die meisten Adressen als down angezeigt hat, zeigt `nmap` alle als up an.

- Erzeugung von `nmap` bei einem für einen Ping unerreichbaren Host: vgl. nmap bei einem Offline-Host (S. 7)
- Erzeugung von `nmap` bei einem für einen Ping erreichbaren Host: vgl. nmap bei einem Offline-Host (S. 7)
- Ermittlung des Up-Status durch Erhalt der HTTP-Antwort

6.4

- Three-Way-Handshake: SequenceNumber(SYN) (x) von Client and Host, Rücksenden von SequenceNumber (y) und AcknowledgeNumber(ACK) (x+1) von Host an Client, Rücksenden von AcknowledgeNumber (y+1) Client an Host. ([5])
- TCP-Connect-Scan durch `sudo nmap -sT 10.1.1.2` (vollständiger 3-way-handshake, (SYN)->(SYN+ACK)->(ACK))
- TCP-SYN-Scan durch `sudo nmap -sS 10.1.1.2` (nur halber handshake, (SYN)->(SYN+ACK))

6.5

- Scannen aller Ports mit `sudo nmap -p- -sV 172.16.137.146 -oG logs.txt`
- Output enthält `5288/open/tcp//http//Apache httpd 2.2.14 ((Ubuntu))/`
- Apache-Webserver im Browser aufgerufen mit 172.16.137.146:5288 (Secret Site)

7 OpenVAS

7.2

Start des OpenVAS-Servers mit `/etc/init.d/openvas-server start`
Der Server konnte einige Plugins nicht laden, was jedoch scheinbar keine weiteren Auswirkungen hatte.

7.4

Login auf dem Server als user@localhost:user

7.5

Es wurde auf das Fragezeichen geklickt und der Assistent durchgearbeitet. Währenddessen wurde als Name "localhost" und als IP-Adresse die eigene IP-Adresse gewählt. Danach würde auf das Stecker-Symbol gekilckt, die Daten eingegeben und "ok" betätigt.

localhost hat 2 Sicherheitslücken, die sich laut OpenVAS beide durch Updates beheben lassen. Es werden Weblinks für weitere Nachforschungen zu diesen Sicherheitslücken gegeben.

Desweiteren werden 6 Security-Notes angegeben, es gibt 0 Security Warnings (Protokoll: **??** (S. **??**)).

7.6

Eingabe: File -> Scan Assistant -> Task: $name -> Scope: $name -> Targets: IP der MysteryVM (172.16.137.146) -> Execute

MysteryVM hat eine Sicherheitslücke, 3 Sicherheitswarnungen und 4 Security Notes (Protokoll: **??** (S. **??**)).

Sicherheitslücke: Login-Daten: root:password (Daten sind korrekt, wurden überprüft)

7.7

Nach Eingabe der SSH-Login-Daten in sowohl den Global Settings als auch den Host-Settings wurde ein neuer Scope aufgerufen. Das Ergebnis ist gleich (1 Issue, 3 Warnings, 4 Notes) (Protokoll: **??** (S. **??**)). Fazit: OpenVAS erkennt von außen alle Sicherheitsprobleme.

Literatur

[1] `https://wiki.ubuntuusers.de/tcpdump/`

[2] `http://danielmessler.com/study/tcpdump/`

[3] `www.alexonlinux.com/tcpdump-for-dummies#...`

[4] `https://nmap.org/book/man.html`

[5] `https://de.wikipedia.org/wiki/Drei-Wege-Handschlag#/media/File:Three-way-handshake-example.gif`

Anhang: nmap

nmap bei einem Offline-Host

- Ping (ICMP)
- Senden eines HTTPS-Package (TCP)
- Senden eines HTTP-Package (TCP)
- Timestamp anfragen (ICMP)
- Antwort auf HTTP von Remote Host (TCP)

nmap bei einem Online-Host

- Ping (ICMP)
- Ping Response vom Remote Host (ICMP)
- Senden eines HTTPS-Package (TCP)
- Senden eines HTTP-Package (TCP)
- Timestamp anfragen (ICMP)
- Antwort auf HTTP von Remote Host (TCP)

Anhang: 2.2

7.7.1 Anfrage

Output:

```
14:01:53:677232 IP (tos 0x0, ttl 64, id 1258, offset 0, flags [DF], proto
    UDP (17), length 60)
    192.168.254.44.35616 > server.svslab.domain: [udp sum ok] 19679+ A? www
        .google.com. (32)
```

Aufbau ([3]):

```
timestamp protocoll (package-information)
    nameserver > local-domain checksum-check some-number Question? target.
        (num)
```

Antwort

Output:

```
14:01:53.677765 IP (tos 0x0, ttl 127, id 21488, offset 0, flags [none],
    proto UDP (17), length 212)
    server.svslab.domain > 192.168.254.44.35616: [udp sum ok] 19679 q: A?
        www.google.com. 1/4/4 www.google.com. [2m33s] A 216.58.213.228 ns:
        google.com. [1d21h4m48s] NS ns1.google.com., google.com. [1
        d21h4m48s] NS ns3.google.com., google.com. [1d21h4m48s] NS ns2.
        google.com., google.com. [1d21h4m48s] NS ns4.google.com. ar: ns1.
        google.com. [3d21h12m22s] A 216.239.32.10, ns2.google.com. [3
        d21h12m22s] A 216.239.34.10, ns3.google.com. [3d21h12m22s] A
        216.239.36.10, ns4.google.com. [3d21h12m44s] A 216.239.38.10 (184)
```

Anhang: Sniffing

Output des HTTP-Sniffing

```
14:37:51.282324 IP (tos 0x0, ttl 64, id 51836, offset 0, flags [DF], proto
    TCP (6), length 487)
    192.168.254.44.35465 > ham04s01-in-f4.1e100.net.www: Flags [P.], cksum
        0xbb75 (correct), seq 311797790:311798237, ack 398350995, win 9648,
        length 447
E....|@.@......,.:.....P......Z.P.%..u..GET / HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.1) Gecko/20100101
    Firefox/10.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: NID=79=
    WlzebisuVRgORNA05jSpuedXCNNs1eBM8yEMd8n30_OluRdkzWbkChEEQ4YgUvHTWB3a64hs
     LjaseRkBrUN1vGIU56_9YOWlq0yWpZRTS4cdFs9-0wKsmJyANZ1uZ7UPnFbMMSPb
```

Output des HTTPS-Sniffing

```
14:27:10.394893 IP (tos 0x0, ttl 64, id 18592, offset 0, flags [DF], proto
    TCP (6), length 60)
    192.168.254.44.35453 > ham04s01-in-f4.1e100.net.www: tcp 0
```

Output von urlsnarf

```
192.168.254.44 - - [26/May/2016:15:03:07 +0200] "GET http://10.1.1.2/
    verysecure/ HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv
    :10.0.1) Gecko/20100101 Firefox/10.0.1"
```

Output von dsniff

```
dsniff: listening on eth1
-----------------
05/26/16 15:06:17 tcp 192.168.254.44.56594 -> labservervm.svslab.80 (http)
GET /verysecure/ HTTP/1.1
Host: 10.1.1.2
Authorization: Basic YWxpY2U6c2VocmdlaGVpbQ== [alice:sehrgeheim]
```

Anhang: Ping-Skript (Aufgabe 6.2)

```
#!/bin/bash
COUNTER=0
LIMIT=255
while [ $COUNTER -lt $LIMIT ]; do
    echo "pinging␣10.1.1.$COUNTER"
    ping -c1 10.1.1.$COUNTER
    let COUNTER=COUNTER+1
done
```

Anhang: 6.2 (IP-Liste)

- 10.1.1.1
- 10.1.1.2
- 10.1.1.5
- 10.1.1.11
- 10.1.1.21
- 10.1.1.31
- 10.1.1.41
- 10.1.1.51
- 10.1.1.61
- 10.1.1.71
- 10.1.1.81
- 10.1.1.91
- 10.1.1.101
- 10.1.1.111
- 10.1.1.121
- 10.1.1.131
- 10.1.1.181
- 10.1.1.186
- 10.1.1.218
- 10.1.1.222
- 10.1.1.235
- 10.1.1.238
- 10.1.1.254

Anhang: Security-Protokoll localhost

```
OpenVAS Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 2
 - Number of security warnings found : 0
 - Number of security notes found : 6
 - Number of false positives found : 0
```

```



TESTED HOSTS

 localhost (Security holes found)



DETAILS

+ localhost :
 . List of open ports :
   o ipp (631/tcp) (Security hole found)
   o otp (9390/tcp)
   o general/tcp (Security notes found)
   o general/IT-Grundschutz
   o general/HOST-T
   o general/IT-Grundschutz-T
   o general/CPE-T

 . Vulnerability found on port ipp (631/tcp) :


    Overview:
    CUPS is prone to a NULL-pointer dereference vulnerability.

    Successful exploits may allow attackers to execute arbitrary code with
    the privileges of a user running the application. Failed exploit
    attempts likely cause denial-of-service conditions.

    CUPS versions prior to 1.4.4 are affected.

    Solution:
    Updates are available. Please see the references for more information.

    References:
    https://www.securityfocus.com/bid/40943
    http://cups.org/articles.php?L596
    http://www.cups.org
    http://cups.org/str.php?L3516
    CVE : CVE-2010-0542, CVE-2010-2431, CVE-2010-2432
    BID : 40943

 . Vulnerability found on port ipp (631/tcp) :


    Overview:
    CUPS Web Interface is prone to Multiple Vulnerabilities.

    1.
    A remote information-disclosure vulnerability. This
    issue affects the CUPS web interface component.

    Remote attackers can exploit this issue to obtain sensitive
    information that may lead to further attacks.

    2.
    A cross-site request-forgery vulnerability.

    Attackers can exploit this issue to perform certain administrative
    actions and gain unauthorized access to the affected application.

    Solution:
    Updates are available. Please see the references for more information.

    References:
    https://www.securityfocus.com/bid/40897
    http://cups.org/articles.php?L596
    http://www.apple.com/macosx/
    CVE : CVE-2010-1748, CVE-2010-0540
    BID : 40897, 40889

. Information found on port ipp (631/tcp)


    A web server is running on this port

. Information found on port ipp (631/tcp)


    The remote web server type is :

    CUPS/1.4


. Information found on port ipp (631/tcp)


    The following CGI have been discovered :

    Syntax : cginame (arguments [default value])

    /help/api-cups.html (TOPIC [Programming] QUERY [] )
    /help/ref-page_log.html (QUERY [] TOPIC [References] )
    /help/accounting.html (TOPIC [Getting+Started] QUERY [] )
    /help/api-ppdc.html (QUERY [] TOPIC [Programming] )
    /help/api-raster.html (QUERY [] TOPIC [Programming] )
    /help/options.html (QUERY [] TOPIC [Getting+Started] )
    /help/sharing.html (TOPIC [Getting+Started] QUERY [] )
    /help/api-httpipp.html (QUERY [] TOPIC [Programming] )
    /help/ref-error_log.html (QUERY [] TOPIC [References] )
    /admin/ (org.cups.sid [c5b6d66ae87a624fdd00590f7c27afd8] OP [add-printer] )
    /help/translation.html (TOPIC [Getting+Started] QUERY [] )
    /help/policies.html (TOPIC [Getting+Started] QUERY [] )
    /printers/ (CLEAR [Clear] QUERY [] )
    /help/glossary.html (TOPIC [Getting+Started] QUERY [] )
    /help/api-array.html (TOPIC [Programming] QUERY [] )
    /help/cgi.html (TOPIC [Getting+Started] QUERY [] )
    /help/overview.html (TOPIC [Getting+Started] QUERY [] )
    /help/standard.html (TOPIC [Getting+Started] QUERY [] )
    /help/network.html (TOPIC [Getting+Started] QUERY [] )
    /help/api-filter.html (TOPIC [Programming] QUERY [] )
    /help/api-overview.html (TOPIC [Programming] QUERY [] )
    /jobs (which_jobs [completed] )
    /help/api-filedir.html (QUERY [] TOPIC [Programming] )
    /jobs/ (CLEAR [Clear] ORDER [asc] QUERY [] )
    /help/license.html (TOPIC [Getting+Started] QUERY [] )
    /help/whatsnew.html (QUERY [] TOPIC [Getting+Started] )
    /help/ref-access_log.html (TOPIC [References] QUERY [] )
    /help/ref-client-conf.html (TOPIC [References] QUERY [] )
    /help/ref-cupsd-conf.html (TOPIC [References] QUERY [] )
    /help/ref-snmp-conf.html (TOPIC [References] QUERY [] )
    /help/ (SEARCH [Search] CLEAR [Clear] TOPIC [Getting+Started] QUERY [] )
    /help/security.html (TOPIC [Getting+Started] QUERY [] )
    /help/postscript-driver.html (QUERY [] TOPIC [Programming] )
    /help/raster-driver.html (QUERY [] TOPIC [Programming] )
    /help/ppd-compiler.html (TOPIC [Programming] QUERY [] )
    /help/api-driver.html (TOPIC [Programming] QUERY [] )
    /classes/ (CLEAR [Clear] QUERY [] )
    /admin/log/error_log ()
    /admin/log/access_log ()
    /help/kerberos.html (TOPIC [Getting+Started] QUERY [] )
    /help/ref-ppdcfile.html (TOPIC [References] QUERY [] )
    /help/ref-classes-conf.html (TOPIC [References] QUERY [] )
    /help/api-mime.html (QUERY [] TOPIC [Programming] )
    /help/api-ppd.html (TOPIC [Programming] QUERY [] )
    /help/ref-mailto-conf.html (QUERY [] TOPIC [References] )
    /help/ref-printers-conf.html (QUERY [] TOPIC [References] )
    /help/ref-subscriptions-conf.html (TOPIC [References] QUERY [] )
    /help/api-cgi.html (QUERY [] TOPIC [Programming] )


 . Information found on port general/tcp


    CUPS version 1.4.3 running at location / was detected on the host

 . Information found on port general/tcp


    CUPS version 1.4.3 running at location /admin/ was detected on the host

 . Information found on port general/tcp


    CUPS version 1.4.3 running at location /admin/log was detected on the host




------------------------------------------------------
This file was generated by the OpenVAS Security Scanner [http://www.openvas.org]
```

Anhang: Security-Protokoll MysteryVM

```
OpenVAS Scan Report
------------------



```

```
SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 3
 - Number of security notes found : 4
 - Number of false positives found : 0



TESTED HOSTS

 172.16.137.146 (Security holes found)



DETAILS

+ 172.16.137.146 :
 . List of open ports :
   o commplex-main (5000/tcp)
   o commplex-link (5001/tcp)
   o rfe (5002/tcp)
   o ssh (22/tcp) (Security hole found)
   o fmpro-internal (5003/tcp) (Security notes found)
   o avt-profile-1 (5004/tcp)
   o avt-profile-2 (5005/tcp)
   o wsm-server (5006/tcp)
   o wsm-server-ssl (5007/tcp)
   o synapsis-edge (5008/tcp)
   o ultima-online-game (5009/tcp)
   o telelpathstart (5010/tcp)
   o telelpathattack (5011/tcp)
   o zenginkyo-1 (5020/tcp)
   o zenginkyo-2 (5021/tcp)
   o mice (5022/tcp)
   o htuilsrv (5023/tcp)
   o scpi-telnet (5024/tcp)
   o scpi-raw (5025/tcp)
   o netmetro (5031/tcp)
   o asnaacceler8db (5042/tcp)
   o mmcc (5050/tcp)
   o ita-agent (5051/tcp)
   o ita-manager (5052/tcp)
   o java-service (5053/tcp)
   o java-service (5054/tcp)
   o unot (5055/tcp)
   o intecom-ps1 (5056/tcp)
   o intecom-ps2 (5057/tcp)
   o sip (5060/tcp)
   o sip-tls (5061/tcp)
   o ca-1 (5064/tcp)
   o ca-2 (5065/tcp)
   o stanag-5066 (5066/tcp)
   o i-net-2000-npr (5069/tcp)
   o powerschool (5071/tcp)
   o sdl-ets (5081/tcp)
   o sentinel-lm (5093/tcp)
   o sentlm-srv2srv (5099/tcp)
   o admd (5100/tcp)
   o talarian-tcp (5101/tcp) (Security notes found)
   o admeng (5102/tcp)
   o ctsd (5137/tcp)
   o rmonitor_secure (5145/tcp)
   o atmp (5150/tcp)
   o esri_sde (5151/tcp)
   o sde-discovery (5152/tcp)
   o bzflag (5154/tcp)
   o ife_icorp (5165/tcp)
   o aol (5190/tcp)
   o aol-1 (5191/tcp)
   o aol-2 (5192/tcp)
   o aol-3 (5193/tcp)
   o targus-getdata (5200/tcp)
   o targus-getdata1 (5201/tcp)
   o targus-getdata2 (5202/tcp)
   o targus-getdata3 (5203/tcp)
   o jabber-client (5222/tcp)
   o hp-server (5225/tcp)
   o hp-status (5226/tcp)
   o sgi-dgl (5232/tcp)
   o padl2sim (5236/tcp)
   o igateway (5250/tcp)
   o caevms (5251/tcp)
   o 3com-njack-1 (5264/tcp)
   o 3com-njack-2 (5265/tcp)
   o jabber-server (5269/tcp)
   o pk (5272/tcp)
   o transmit-port (5282/tcp)
   o hacl-hb (5300/tcp)
   o hacl-gs (5301/tcp)
   o hacl-cfg (5302/tcp)
   o hacl-probe (5303/tcp)
   o hacl-local (5304/tcp)
   o hacl-test (5305/tcp)
   o sun-mc-grp (5306/tcp)
   o sco-aip (5307/tcp)
   o cfengine (5308/tcp)
   o jprinter (5309/tcp)
   o outlaws (5310/tcp)
   o tmlogin (5311/tcp)
   o opalis-rbt-ipc (5314/tcp)
   o hacl-poll (5315/tcp)
   o nat-pmp (5351/tcp)
   o dns-llq (5352/tcp)
   o mdns (5353/tcp)
   o mdnsresponder (5354/tcp)
   o llmnr (5355/tcp)
   o excerpt (5400/tcp)
   o excerpts (5401/tcp)
   o mftp (5402/tcp)
   o hpoms-ci-lstn (5403/tcp)
   o hpoms-dps-lstn (5404/tcp)
   o netsupport (5405/tcp)
   o systemics-sox (5406/tcp)
   o foresyte-clear (5407/tcp)
   o foresyte-sec (5408/tcp)
   o salient-dtasrv (5409/tcp)
```

```
    o salient-usrmgr (5410/tcp)
    o actnet (5411/tcp)
    o continuus (5412/tcp)
    o wwiotalk (5413/tcp)
    o statusd (5414/tcp)
    o ns-server (5415/tcp)
    o sns-gateway (5416/tcp)
    o sns-agent (5417/tcp)
    o mcntp (5418/tcp)
    o dj-ice (5419/tcp)
    o cylink-c (5420/tcp)
    o netsupport2 (5421/tcp)
    o salient-mux (5422/tcp)
    o virtualuser (5423/tcp)
    o beyond-remote (5424/tcp)
    o br-channel (5425/tcp)
    o devbasic (5426/tcp)
    o sco-peer-tta (5427/tcp)
    o telaconsole (5428/tcp)
    o base (5429/tcp)
    o radec-corp (5430/tcp)
    o park-agent (5431/tcp)
    o postgresql (5432/tcp)
    o dttl (5435/tcp)
    o apc-5454 (5454/tcp)
    o apc-5455 (5455/tcp)
    o apc-5456 (5456/tcp)
    o silkmeter (5461/tcp)
    o ttl-publisher (5462/tcp)
    o ttlpriceproxy (5463/tcp)
    o netops-broker (5465/tcp)
    o fcp-addr-srvr1 (5500/tcp)
    o fcp-addr-srvr2 (5501/tcp)
    o fcp-srvr-inst1 (5502/tcp)
    o fcp-srvr-inst2 (5503/tcp)
    o fcp-cics-gw1 (5504/tcp)
    o secureidprop (5510/tcp)
    o sdlog (5520/tcp)
    o illusionmailer (5521/tcp)
    o sdserv (5530/tcp)
    o sdreport (5540/tcp)
    o sdadmind (5550/tcp)
    o sgi-eventmond (5553/tcp)
    o sgi-esphttp (5554/tcp)
    o personal-agent (5555/tcp)
    o remotewatch (5556/tcp)
    o udpplus (5566/tcp)
    o robohack (5569/tcp)
    o the-qube (5595/tcp)
    o the-qube (5596/tcp)
    o the-qube (5597/tcp)
    o the-qube (5598/tcp)
    o esinstall (5599/tcp)
    o esmmanager (5600/tcp)
    o esmagent (5601/tcp)
    o a1-msc (5602/tcp)
    o a1-bs (5603/tcp)
    o a3-sdunode (5604/tcp)
    o a4-sdunode (5605/tcp)
    o pcanywheredata (5631/tcp)
    o pcanywherestat (5632/tcp)
    o netsaint (5666/tcp)
    o jms (5673/tcp)
    o hyperscsi-port (5674/tcp)
    o v5ua (5675/tcp)
    o raadmin (5676/tcp)
    o questdb2-lnchr (5677/tcp)
    o rrac (5678/tcp)
    o dccm (5679/tcp)
    o canna (5680/tcp)
    o ggz (5688/tcp)
    o winmx (5690/tcp)
    o proshareaudio (5713/tcp)
    o prosharevideo (5714/tcp)
    o prosharedata (5715/tcp)
    o prosharerequest (5716/tcp)
    o prosharenotify (5717/tcp)
    o ms-licensing (5720/tcp)
    o openmail (5729/tcp)
    o unieng (5730/tcp)
    o ida-discover1 (5741/tcp)
    o ida-discover2 (5742/tcp)
    o fcopy-server (5745/tcp)
    o fcopys-server (5746/tcp)
    o openmailg (5755/tcp)
    o x500ms (5757/tcp)
    o openmailns (5766/tcp)
    o s-openmail (5767/tcp)
    o openmailpxy (5768/tcp)
    o netagent (5771/tcp)
    o vnc-http (5800/tcp)
    o vnc-http-1 (5801/tcp)
    o vnc-http-2 (5802/tcp)
    o vnc-http-3 (5803/tcp)
    o icmpd (5813/tcp)
    o otadmin (5858/tcp)
    o wherehoo (5859/tcp)
    o y3k (5882/tcp)
    o y3k (5888/tcp)
    o y3k (5889/tcp)
    o vnc (5900/tcp)
    o vnc-1 (5901/tcp)
    o vnc-2 (5902/tcp)
    o vnc-3 (5903/tcp)
    o mppolicy-v5 (5968/tcp)
    o mppolicy-mgr (5969/tcp)
    o ncd-pref-tcp (5977/tcp)
    o ncd-diag-tcp (5978/tcp)
    o ncd-conf-tcp (5979/tcp)
    o wbem-rmi (5987/tcp)
    o wbem-http (5988/tcp)
    o wbem-https (5989/tcp)
    o wbem-local (5990/tcp)
    o nuxsl (5991/tcp)
    o ncd-pref (5997/tcp)
    o ncd-diag (5998/tcp)
    o cvsup (5999/tcp)
    o x11 (6000/tcp)
```

```
  o general/tcp (Security warnings found)
  o general/IT-Grundschutz
  o general/icmp (Security notes found)
  o general/HOST-T
  o general/IT-Grundschutz-T
  o general/CPE-T

. Vulnerability found on port ssh (22/tcp) :


   Overview:
   It was possible to login into the remote host using default credentials.

   Solution:
   Change the password as soon as possible.

   It was possible to login with the following credentials <User>:<Password>

   root:password


. Warning found on port ssh (22/tcp)


   According to its banner, the version of OpenSSH installed on the remote
   host is older than 5.7:
    ssh-2.0-openssh_5.3p1 debian-3ubuntu7

   Overview:
   The auth_parse_options function in auth-options.c in sshd in OpenSSH before
    5.7
   provides debug messages containing authorized_keys command options, which
    allows
   remote authenticated users to obtain potentially sensitive information by
   reading these messages, as demonstrated by the shared user account required
    by
   Gitolite. NOTE: this can cross privilege boundaries because a user account
    may
   intentionally have no shell or filesystem access, and therefore may have no
   supported way to read an authorized_keys file in its own home directory.

   OpenSSH before 5.7 is affected;

   Solution:
   Updates are available. Please see the references for more information.

   References:
   http://www.securityfocus.com/bid/51702
   http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
   http://packages.debian.org/squeeze/openssh-server
```

```
    https://downloads.avaya.com/css/P8/documents/100161262
    CVE : CVE-2012-0814
    BID : 51702

 . Information found on port ssh (22/tcp)


    An ssh server is running on this port

 . Information found on port fmpro-internal (5003/tcp)



    The remote host is running the Filemaker database server.
    FileMaker Pro is a cross-platform relational database application from
     FileMaker Inc.,
    a subsidiary of Apple Inc., has compatible versions for both the Mac OS X
     and Microsoft Windows operating systems


    Solution :
    You should Allow connection to this host only from trusted host or
     networks,
    or disable the service if not used.

    Risk factor : None

 . Information found on port talarian-tcp (5101/tcp)



    Yahoo Messenger is running on this machine and this port. It can
    be used to share files and chat with other users.

     Tested with Yahoo Messenger versions 7 and 8.

     References:
     http://libyahoo2.sourceforge.net/ymsg-9.txt
     http://www.astahost.com/info.php/yahoo-protocol-part-10-peer-peer-transfers_t11490.html
 http://libyahoo2.sourceforge.net/README
 http://www.ycoderscookbook.com/
 http://www.venkydude.com/articles/yahoo.htm

Risk factor :None




 . Warning found on port general/tcp



    Synopsis :

    The remote service implements TCP timestamps.

    Description :
```

```

   The remote host implements TCP timestamps, as defined by RFC1323.
   A side effect of this feature is that the uptime of the remote
   host can sometimes be computed.

   See also :

   http://www.ietf.org/rfc/rfc1323.txt

   Risk factor :

   None

. Warning found on port general/tcp



     Overview: The host is running TCP services and is prone to denial of
    service
     vulnerability.

     Vulnerability Insight:
     The flaw is triggered when spoofed TCP Reset packets are received by the
     targeted TCP stack and will result in loss of availability for the
    attacked
     TCP services.

     Impact:
     Successful exploitation will allow remote attackers to guess sequence
    numbers
     and cause a denial of service to persistent TCP connections by repeatedly
     injecting a TCP RST packet.

     Impact Level: System

     Affected Software/OS:
     TCP

     Fix: Please see the referenced advisories for more information on
    obtaining
     and applying fixes.

     References:
     http://www.osvdb.org/4030
     http://xforce.iss.net/xforce/xfdb/15886
     http://www.us-cert.gov/cas/techalerts/TA04-111A.html
     http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
     http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
     http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
     http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
     http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
     http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
     http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
   CVE : CVE-2004-0230
   BID : 10183
```

```

 . Information found on port general/icmp


    Here is the route recorded between 172.16.137.222 and 172.16.137.146 :
    172.16.137.146.
    172.16.137.146.






------------------------------------------------------
This file was generated by the OpenVAS Security Scanner [http://www.openvas.org]
```

Anhang: Security-Protokoll MysteryVM-SSH

```
OpenVAS Scan Report
------------------




SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 1
 - Number of security warnings found : 3
 - Number of security notes found : 4
 - Number of false positives found : 0



TESTED HOSTS

 172.16.137.146 (Security holes found)



DETAILS

+ 172.16.137.146 :
 . List of open ports :
   o ssh (22/tcp) (Security hole found)
   o commplex-main (5000/tcp)
   o commplex-link (5001/tcp)
   o rfe (5002/tcp)
   o fmpro-internal (5003/tcp) (Security notes found)
   o avt-profile-1 (5004/tcp)
   o avt-profile-2 (5005/tcp)
   o wsm-server (5006/tcp)
   o wsm-server-ssl (5007/tcp)
   o synapsis-edge (5008/tcp)
   o ultima-online-game (5009/tcp)
   o telelpathstart (5010/tcp)
   o telelpathattack (5011/tcp)
   o zenginkyo-1 (5020/tcp)
   o zenginkyo-2 (5021/tcp)
   o mice (5022/tcp)
   o htuilsrv (5023/tcp)
   o scpi-telnet (5024/tcp)
   o scpi-raw (5025/tcp)
   o netmetro (5031/tcp)
   o asnaacceler8db (5042/tcp)
   o mmcc (5050/tcp)
   o ita-agent (5051/tcp)
   o ita-manager (5052/tcp)
   o java-service (5053/tcp)
   o java-service (5054/tcp)
   o unot (5055/tcp)
   o intecom-ps1 (5056/tcp)
   o intecom-ps2 (5057/tcp)
   o sip (5060/tcp)
   o sip-tls (5061/tcp)
   o ca-1 (5064/tcp)
   o ca-2 (5065/tcp)
   o stanag-5066 (5066/tcp)
   o i-net-2000-npr (5069/tcp)
   o powerschool (5071/tcp)
   o sdl-ets (5081/tcp)
   o sentinel-lm (5093/tcp)
   o sentlm-srv2srv (5099/tcp)
   o admd (5100/tcp)
   o talarian-tcp (5101/tcp) (Security notes found)
   o admeng (5102/tcp)
   o ctsd (5137/tcp)
   o rmonitor_secure (5145/tcp)
   o atmp (5150/tcp)
   o esri_sde (5151/tcp)
   o sde-discovery (5152/tcp)
   o bzflag (5154/tcp)
   o ife_icorp (5165/tcp)
   o aol (5190/tcp)
   o aol-1 (5191/tcp)
   o aol-2 (5192/tcp)
   o aol-3 (5193/tcp)
   o targus-getdata (5200/tcp)
   o targus-getdata1 (5201/tcp)
   o targus-getdata2 (5202/tcp)
   o targus-getdata3 (5203/tcp)
   o jabber-client (5222/tcp)
   o hp-server (5225/tcp)
   o hp-status (5226/tcp)
   o sgi-dgl (5232/tcp)
   o padl2sim (5236/tcp)
   o igateway (5250/tcp)
   o caevms (5251/tcp)
   o 3com-njack-1 (5264/tcp)
   o 3com-njack-2 (5265/tcp)
   o jabber-server (5269/tcp)
   o pk (5272/tcp)
   o transmit-port (5282/tcp)
   o hacl-hb (5300/tcp)
   o hacl-gs (5301/tcp)
   o hacl-cfg (5302/tcp)
   o hacl-probe (5303/tcp)
```

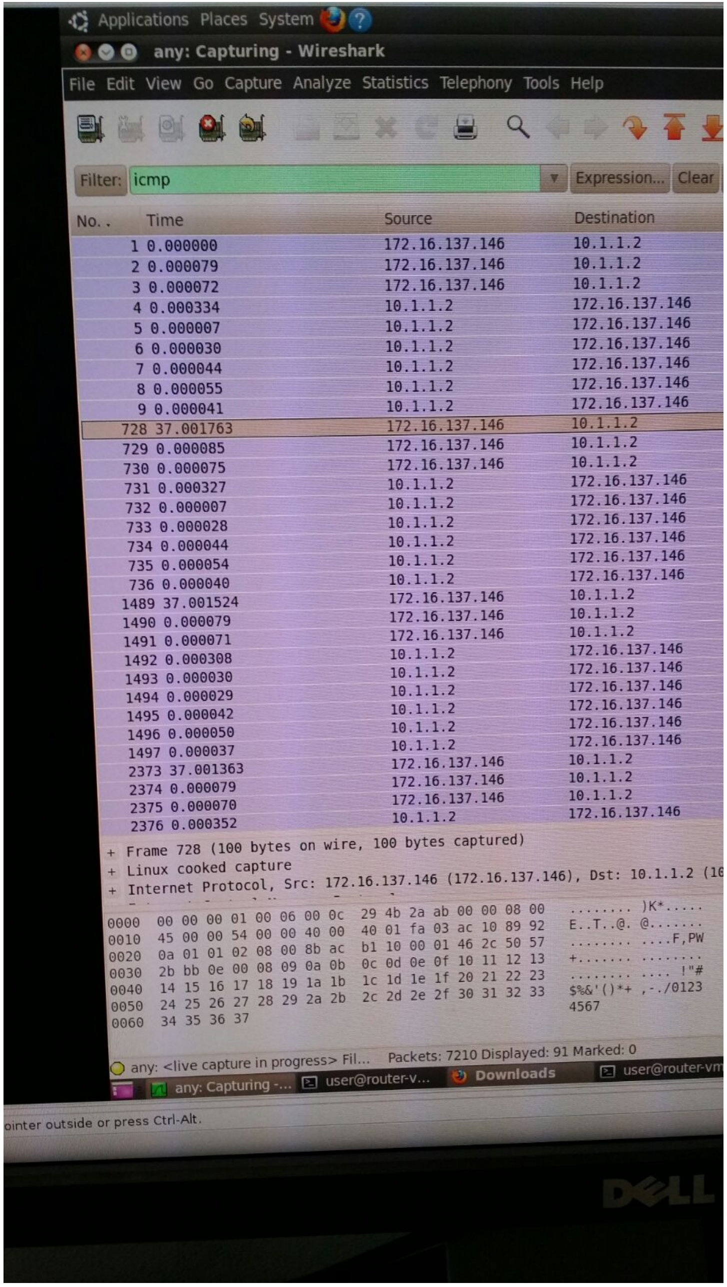
```
    o hacl-local (5304/tcp)
    o hacl-test (5305/tcp)
    o sun-mc-grp (5306/tcp)
    o sco-aip (5307/tcp)
    o cfengine (5308/tcp)
    o jprinter (5309/tcp)
    o outlaws (5310/tcp)
    o tmlogin (5311/tcp)
    o opalis-rbt-ipc (5314/tcp)
    o hacl-poll (5315/tcp)
    o nat-pmp (5351/tcp)
    o dns-llq (5352/tcp)
    o mdns (5353/tcp)
    o mdnsresponder (5354/tcp)
    o llmnr (5355/tcp)
    o excerpt (5400/tcp)
    o excerpts (5401/tcp)
    o mftp (5402/tcp)
    o hpoms-ci-lstn (5403/tcp)
    o hpoms-dps-lstn (5404/tcp)
    o netsupport (5405/tcp)
    o systemics-sox (5406/tcp)
    o foresyte-clear (5407/tcp)
    o foresyte-sec (5408/tcp)
    o salient-dtasrv (5409/tcp)
    o salient-usrmgr (5410/tcp)
    o actnet (5411/tcp)
    o continuus (5412/tcp)
    o wwiotalk (5413/tcp)
    o statusd (5414/tcp)
    o ns-server (5415/tcp)
    o sns-gateway (5416/tcp)
    o sns-agent (5417/tcp)
    o mcntp (5418/tcp)
    o dj-ice (5419/tcp)
    o cylink-c (5420/tcp)
    o netsupport2 (5421/tcp)
    o salient-mux (5422/tcp)
    o virtualuser (5423/tcp)
    o beyond-remote (5424/tcp)
    o br-channel (5425/tcp)
    o devbasic (5426/tcp)
    o sco-peer-tta (5427/tcp)
    o telaconsole (5428/tcp)
    o base (5429/tcp)
    o radec-corp (5430/tcp)
    o park-agent (5431/tcp)
    o postgresql (5432/tcp)
    o dttl (5435/tcp)
    o apc-5454 (5454/tcp)
    o apc-5455 (5455/tcp)
    o apc-5456 (5456/tcp)
    o silkmeter (5461/tcp)
    o ttl-publisher (5462/tcp)
    o ttlpriceproxy (5463/tcp)
    o netops-broker (5465/tcp)
    o fcp-addr-srvr1 (5500/tcp)
    o fcp-addr-srvr2 (5501/tcp)
    o fcp-srvr-inst1 (5502/tcp)
    o fcp-srvr-inst2 (5503/tcp)
    o fcp-cics-gw1 (5504/tcp)
    o secureidprop (5510/tcp)
    o sdlog (5520/tcp)
    o illusionmailer (5521/tcp)
    o sdserv (5530/tcp)
    o sdreport (5540/tcp)
    o sdadmind (5550/tcp)
    o sgi-eventmond (5553/tcp)
    o sgi-esphttp (5554/tcp)
    o personal-agent (5555/tcp)
    o remotewatch (5556/tcp)
    o udpplus (5566/tcp)
    o robohack (5569/tcp)
    o the-qube (5595/tcp)
    o the-qube (5596/tcp)
    o the-qube (5597/tcp)
    o the-qube (5598/tcp)
    o esinstall (5599/tcp)
    o esmmanager (5600/tcp)
    o esmagent (5601/tcp)
    o a1-msc (5602/tcp)
    o a1-bs (5603/tcp)
    o a3-sdunode (5604/tcp)
    o a4-sdunode (5605/tcp)
    o pcanywheredata (5631/tcp)
    o pcanywherestat (5632/tcp)
    o netsaint (5666/tcp)
    o jms (5673/tcp)
    o hyperscsi-port (5674/tcp)
    o v5ua (5675/tcp)
    o raadmin (5676/tcp)
    o questdb2-lnchr (5677/tcp)
    o rrac (5678/tcp)
    o dccm (5679/tcp)
    o canna (5680/tcp)
    o ggz (5688/tcp)
    o winmx (5690/tcp)
    o proshareaudio (5713/tcp)
    o prosharevideo (5714/tcp)
    o prosharedata (5715/tcp)
    o prosharerequest (5716/tcp)
    o prosharenotify (5717/tcp)
    o ms-licensing (5720/tcp)
    o openmail (5729/tcp)
    o unieng (5730/tcp)
    o ida-discover1 (5741/tcp)
    o ida-discover2 (5742/tcp)
    o fcopy-server (5745/tcp)
    o fcopys-server (5746/tcp)
    o openmailg (5755/tcp)
    o x500ms (5757/tcp)
    o openmailns (5766/tcp)
    o s-openmail (5767/tcp)
    o openmailpxy (5768/tcp)
    o netagent (5771/tcp)
    o vnc-http (5800/tcp)
    o vnc-http-1 (5801/tcp)
    o vnc-http-2 (5802/tcp)
```

```
   o vnc-http-3 (5803/tcp)
   o icmpd (5813/tcp)
   o otadmin (5858/tcp)
   o wherehoo (5859/tcp)
   o y3k (5882/tcp)
   o y3k (5888/tcp)
   o y3k (5889/tcp)
   o vnc (5900/tcp)
   o vnc-1 (5901/tcp)
   o vnc-2 (5902/tcp)
   o vnc-3 (5903/tcp)
   o mppolicy-v5 (5968/tcp)
   o mppolicy-mgr (5969/tcp)
   o ncd-pref-tcp (5977/tcp)
   o ncd-diag-tcp (5978/tcp)
   o ncd-conf-tcp (5979/tcp)
   o wbem-rmi (5987/tcp)
   o wbem-http (5988/tcp)
   o wbem-https (5989/tcp)
   o wbem-local (5990/tcp)
   o nuxsl (5991/tcp)
   o ncd-pref (5997/tcp)
   o ncd-diag (5998/tcp)
   o cvsup (5999/tcp)
   o x11 (6000/tcp)
   o general/tcp (Security warnings found)
   o general/IT-Grundschutz
   o general/icmp (Security notes found)
   o general/HOST-T
   o general/IT-Grundschutz-T
   o general/CPE-T

 . Vulnerability found on port ssh (22/tcp) :


    Overview:
    It was possible to login into the remote host using default credentials.

    Solution:
    Change the password as soon as possible.

    It was possible to login with the following credentials <User>:<Password>

    root:password


 . Warning found on port ssh (22/tcp)


    According to its banner, the version of OpenSSH installed on the remote
    host is older than 5.7:
     ssh-2.0-openssh_5.3p1 debian-3ubuntu7

    Overview:
    The auth_parse_options function in auth-options.c in sshd in OpenSSH before
     5.7
    provides debug messages containing authorized_keys command options, which
     allows
    remote authenticated users to obtain potentially sensitive information by
    reading these messages, as demonstrated by the shared user account required
     by
    Gitolite. NOTE: this can cross privilege boundaries because a user account
     may
    intentionally have no shell or filesystem access, and therefore may have no
    supported way to read an authorized_keys file in its own home directory.

    OpenSSH before 5.7 is affected;

    Solution:
    Updates are available. Please see the references for more information.

    References:
    http://www.securityfocus.com/bid/51702
    http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=657445
    http://packages.debian.org/squeeze/openssh-server
    https://downloads.avaya.com/css/P8/documents/100161262
    CVE : CVE-2012-0814
    BID : 51702

 . Information found on port ssh (22/tcp)


    An ssh server is running on this port

 . Information found on port fmpro-internal (5003/tcp)



    The remote host is running the Filemaker database server.
    FileMaker Pro is a cross-platform relational database application from
     FileMaker Inc.,
    a subsidiary of Apple Inc., has compatible versions for both the Mac OS X
     and Microsoft Windows operating systems


    Solution :
    You should Allow connection to this host only from trusted host or
     networks,
    or disable the service if not used.

    Risk factor : None

 . Information found on port talarian-tcp (5101/tcp)



    Yahoo Messenger is running on this machine and this port. It can
    be used to share files and chat with other users.
```

```

     Tested with Yahoo Messenger versions 7 and 8.

     References:
     http://libyahoo2.sourceforge.net/ymsg-9.txt
     http://www.astahost.com/info.php/yahoo-protocol-part-10-peer-peer-transfers_t11490.html
 http://libyahoo2.sourceforge.net/README
 http://www.ycoderscookbook.com/
 http://www.venkydude.com/articles/yahoo.htm

Risk factor :None




 . Warning found on port general/tcp



    Synopsis :

    The remote service implements TCP timestamps.

    Description :

    The remote host implements TCP timestamps, as defined by RFC1323.
    A side effect of this feature is that the uptime of the remote
    host can sometimes be computed.

    See also :

    http://www.ietf.org/rfc/rfc1323.txt

    Risk factor :

    None

 . Warning found on port general/tcp



      Overview: The host is running TCP services and is prone to denial of
     service
      vulnerability.

      Vulnerability Insight:
      The flaw is triggered when spoofed TCP Reset packets are received by the
      targeted TCP stack and will result in loss of availability for the
     attacked
      TCP services.

      Impact:
      Successful exploitation will allow remote attackers to guess sequence
     numbers
      and cause a denial of service to persistent TCP connections by repeatedly
      injecting a TCP RST packet.

      Impact Level: System

      Affected Software/OS:
      TCP

      Fix: Please see the referenced advisories for more information on
     obtaining
      and applying fixes.

      References:
      http://www.osvdb.org/4030
      http://xforce.iss.net/xforce/xfdb/15886
      http://www.us-cert.gov/cas/techalerts/TA04-111A.html
      http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949
      http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950
      http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006
      http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx
      http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx
      http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
      http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html
    CVE : CVE-2004-0230
    BID : 10183

 . Information found on port general/icmp


    Here is the route recorded between 172.16.137.222 and 172.16.137.146 :
    172.16.137.146.
    172.16.137.146.






------------------------------------------------------
This file was generated by the OpenVAS Security Scanner [http://www.openvas.org]
```

Anhang: Wireshark-Screenshot

Abbildung 1: Wireshark-Screenshot zu Aufgabe 5.4


Applications Places System
any: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: icmp
Expression...
Clear
any: Capturing -...
user@router-v...
Downloads
user@router-vm
DELL

```
No. .  Time             Source            Destination
    1 0.000000          172.16.137.146    10.1.1.2
    2 0.000079          172.16.137.146    10.1.1.2
    3 0.000072          172.16.137.146    10.1.1.2
    4 0.000334          10.1.1.2          172.16.137.146
    5 0.000007          10.1.1.2          172.16.137.146
    6 0.000030          10.1.1.2          172.16.137.146
    7 0.000044          10.1.1.2          172.16.137.146
    8 0.000055          10.1.1.2          172.16.137.146
    9 0.000041          10.1.1.2          172.16.137.146
  728 37.001763         172.16.137.146    10.1.1.2
  729 0.000085          172.16.137.146    10.1.1.2
  730 0.000075          172.16.137.146    10.1.1.2
  731 0.000327          10.1.1.2          172.16.137.146
  732 0.000007          10.1.1.2          172.16.137.146
  733 0.000028          10.1.1.2          172.16.137.146
  734 0.000044          10.1.1.2          172.16.137.146
  735 0.000054          10.1.1.2          172.16.137.146
  736 0.000040          10.1.1.2          172.16.137.146
 1489 37.001524         172.16.137.146    10.1.1.2
 1490 0.000079          172.16.137.146    10.1.1.2
 1491 0.000071          172.16.137.146    10.1.1.2
 1492 0.000308          10.1.1.2          172.16.137.146
 1493 0.000030          10.1.1.2          172.16.137.146
 1494 0.000029          10.1.1.2          172.16.137.146
 1495 0.000042          10.1.1.2          172.16.137.146
 1496 0.000050          10.1.1.2          172.16.137.146
 1497 0.000037          10.1.1.2          172.16.137.146
 2373 37.001363         172.16.137.146    10.1.1.2
 2374 0.000079          172.16.137.146    10.1.1.2
 2375 0.000070          172.16.137.146    10.1.1.2
 2376 0.000352          10.1.1.2          172.16.137.146

+ Frame 728 (100 bytes on wire, 100 bytes captured)
+ Linux cooked capture
+ Internet Protocol, Src: 172.16.137.146 (172.16.137.146), Dst: 10.1.1.2 (10

0000  00 00 00 01 00 06 00 0c  29 4b 2a ab 00 00 08 00   ........ )K*.....
0010  45 00 00 54 00 00 40 00  40 01 fa 03 ac 10 89 92   E..T..@. @.......
0020  0a 01 01 02 08 00 8b ac  b1 10 00 01 46 2c 50 57   ........ ....F,PW
0030  2b bb 0e 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   +....... ........
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567

any: <live capture in progress> Fil...   Packets: 7210 Displayed: 91 Marked: 0
```

pointer outside or press Ctrl-Alt.