Wireshark

Jens Link

jenslink@quux.de

FrOSCon 2012

Wer bin ich?

- Freiberuflicher Consultant
- Schwerpunkt: komplexe Netzwerke, Netzwerksecurity, Netzwerkmonitoring, Troubleshooting

Ich bin käuflich ;-)

Warnungen

- Das ist eine Einführung in Wireshark!
- Wer Wireshark täglich nutzt wird nichts neues lernen
- Wireshark ist mächtig, kann aber keine Wunder vollbringen
- Wenig Theorie! Ihr sollt selbst was machen
- Mit Wireshark seht ihr u.U. Daten, die ihr nicht sehen sollt

Wireshark (I)

- Früher: Ethereal
- Netzwerktraffic aufzeichnen und analysieren
- Mehr als tcpdump in Farbe
- Nutz libpcap (winpcap)
- auf der CLI: **tshark**
- Nur aufzeichen: **dumpcap**
- Für spezielle Aufgaben gibt es teilweise bessere Tools
- Kann nur sehen was die Netzwerkkarte auch weiter gibt

Wireshark (II)

“Kann nur sehen was die Netzwerkkarte auch weiter gibt”

- Netzwerkkarte verwirft Frames, die nicht für sie bestimmt sind – **Promiscous Mode**
- Netzwerkkarte verwirft kaputte Frames – **Spezialhardware**
- Geswitchtes Netz: Netzwerkkarte sieht nur Pakete die für sie bestimmt sind – **Switch konfigurieren** / **Hub** / **TAP**
- Braucht RAM und ggf. Plattenplatz

Wireshark (III)

Zwei Arten von Filtern:

- Capture Filter (wie tcpdump)
- Display Filter
- Was nutzt man? Kommt darauf an ;-)

Switch Konfiguration

Beispiel Cisco

```
SW(config)# monitor session 1 source interface
             g1/0/24 both
SW(config)# monitor session 1 destination interface
             g1/0/23
```

Andere

`http://http://wiki.wireshark.org/SwitchReference`

Sammeln von Daten

- Häufig sehr praktisch: Daten auf einem Host aufzeichnen, später mit Wireshark ansehen
- *NIX: tcpdump
- Cisco Router / ASA können auch pcap Files schreiben
- Andere Hersteller zum Teil auch

tcpdump

```
tcpdump -i eth0 -n -s0 -vv
```

Vorsicht: Gibt Probleme wenn ihr das so z.B. per ssh nutzt

Cheat Sheet:

`http://media.packetlife.net/media/library/12/tcpdump.pdf`

Cisco Router

Warnung: CEF aus aus sein, Router forwarded über die normale CPU. Sehr wahrscheinlich keine gute Idee!

```
Router# monitor capture buffer cap ip cef ipceffa0/1 fastEthernet 0/1 both
Router# monitor capture point associate ipceffa0/1 pktrace1
Router# monitor capture point start ipceffa0/1
```

CheckPoint fwmonitor

- Monitoring des Pakets auf dem Weg durch die Fierwall
- Format: Erweitertes tcpdump, kann mit Wireshark gelesen werden
- 4 “Meßpunkte” können definiert werden
- Anleitung: `http://www.checkpoint.com/techsupport/downloads/html/ethereal/fw_monitor_rev1_01.pdf`
- Kann man mit Wireshark analysieren
- Hätte ich auch gerne für andere Systme
- Geht angeblich nicht für IPv6 :-(

Demo / Praxis

Aufgabe 1

Surft im Internet, ruft ein paar Webseiten auf und schaut euch die Daten an.

Aufgabe 2

macht ein traceroute auf `www.heise.de` und erklärt wie traceroute funktioniert

Aufgabe 3

Auf `http://wiki.wireshark.org/SampleCaptures` gibt es ein VoIP Sample.
Was findet ihr da alles an Daten?

Aufgabe 4

Auf meinem Rechner läuft ein http(s) Webserver. Ruft die Webseite auf und versucht die Daten zu lesen.

Werbung

26.02.-01.03. GUUG FFG in Frankfurt am Main

Kontakt

eMail	jenslink@quux.de
Jabber	jenslink@guug.de
PGP Fingerprint	D9FF E215 6686 6194 FFC8 A135 19CF A676 DB85 EF91
Blog	http://blog.quux.de