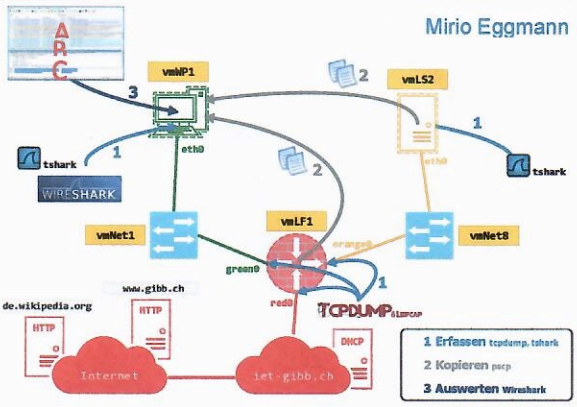
Modul 129

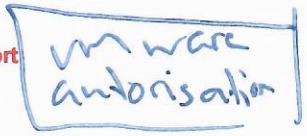
Mirio Eggmann

Praktisch



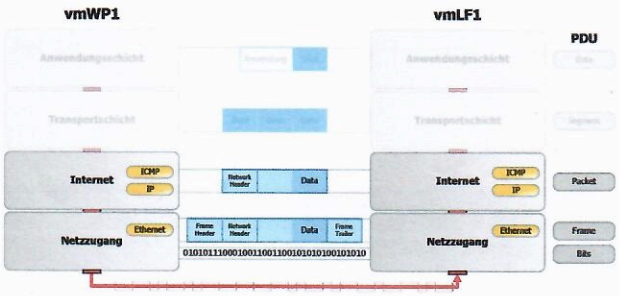
Ablauf: 1 Erfassen (tcpdump,tshark), 2 Kopieren (pscp), 3 Auswerten (Wireshark)
vmLF1: Linux Router, Firewall + tcpdump | User: root, PW: gibbiX12345
vmLS2: Linux Server + tshark | User: vmadmin, PW: gibbiX12345
vmWP1: Windows Rechner + wireshark | User: vmadmin, PW: gibbiX12345
Wireshark: A: Paketliste, B: Paketdetails, C: Hexadezimale Darstellung
Linux zwischen Konsolen wechseln: Alt+F1, Alt+F2

Umgebung in Betrieb nehmen:
vmLF1: root@vmLF1: # *host www.gibb.ch* ENTER .... address 86.118.90.94
// Falls keine Verbindung */etc/init.d/network restart* ENTER
vmLS2: vmadmin@vmLS2: # *nslookup www.gibbix.ch* ENTER Server ... 86.118.65.51
vmLS2: sudo apt-get update ; sudo apt-get upgrade ; sudo apt-get install tshark
vmLS2: sudo chgrp adm /usr/bin/dumpcap ; sudo chmod 750 /usr/bin/dumpcap ;
sudo setcap cap_net_raw, cap_net_admin+eip /usr/bin/dumpcap ; sudo setcap cap_net_raw, cap_net_admin+eip /usr/bin/tshark
tshark –D ENTER 1. Eth 0 \n 2. Nflog \n 3. Nfqueue \n 4. Any
vmWP1: RECHTSKLICK auf Desktop -> neu -> Verknüpfung -> C:\Windows\System32\cmd.exe -> Eingabeaufforderung
RECHTSKLICK auf Verknüpfung -> Eigenschaften -> Verknüpfung -> Ausführen in: C:\ ; Optionen -> QuickEdit-Modus: Aktiviert ;
Schriftart -> Schriftgrad: 20 ; Schriftart -> Schriftart -> Lucida Console ; Layout -> 1. 120*300 ; Layout -> 2. 120*35
vmWP1: *netsh interface ip show config* // Anpassen der Einstellungen ncpa.cpl
vmWP1: C:\> *appwiz.cpl* // Die alte Wireshark Version löschen
vmWP1: C:\> *„Program Files\Wireshark\tshark.exe" –v* // Ausführen nach Installation von neuer Wireshark Version
vmWP1: C:\Windows\system32> *netsh advfirewall set allprofiles state off* // Eingabeaufforderung als **Admin** ausführen \ FW ausschalten
Verbindung vmWP1 – vmLS2 / vmWP1 – vmLF1
vmWP1: C:\>md c:\capdat ; cd c:\capdat ;
vmWP1: C:\>setx path "%path%;%ProgramFiles%\Wireshark;%ProgramFiles(x86)%\Putty" // **Nicht als Admin**
vmWP1: C:\>path // Zuerst schliessen Eingabeaufforderung restart und dann ausgeben ob übernommen | korrigieren: control sysdm.cpl,,3
vmLS2: cat /var/log/syslog > /tmp/syslog_vmls2.txt
vmLF1: cat /var/log/messages > /tmp/messages_vmlf1.txt
vmWP1: C:\> pscp vmadmin@192.168.220.11:/tmp/syslog_vmls2.txt C:\capdat
vmWP1: C:\> pscp –P 222 root@192.168.210.1:/tmp/messages_vmlf1.txt C:\capdat\ // Portangabe, da nicht Standardport
vmWP1: C:\> dir c:\capdat // Die 2 Dateien sollten drin sein



Überprüfen der Vorbereitungsarbeiten
vmLF1: host www.google.ch ; ping 192.168.210.10
vmLS2: nslookup www.gibb.ch ; tshark –D
vmWP1: nslookup www.gibb.ch ; tshark.exe –v ; kopieren pscp vmLS2 auf vmWP1 erfolgreich ; kopieren pscp vmLF1 auf vmWP1 ;
Desktop Verknüpfung „Eingabeaufforderung" ; Desktop Verknüpfung „Wireshark"

Protokollanalyse - Workshop
Ping Auswertungen anzeigen

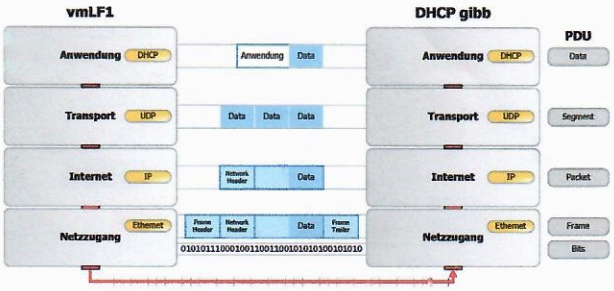


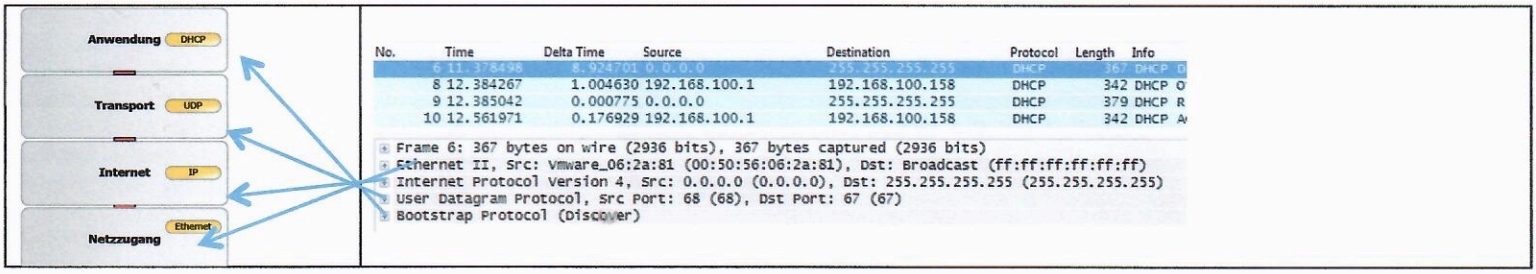
vmLF1: tcpdump –i green0
vmWP1 (CMD-Fenster1): tshark –i 1
vmWP1 (CMD-Fenster2): ping –n 10 192.168.210.1
vmLF1/vmWP1: Aufzeichnung mit CTRL C abbrechen
Ping Auswertung speichern und anzeigen
vmLF1: tcpdump –i green0 –s 65535 –w /tmp/wp1-ping-lf1-r.pcap
vmWP1 (CMD-Fenster1): tshark –i 1 –w \capdat\wp1-ping-lf1-s.pcap
vmWP2 (CMD-Fenster2): ping –n 10 192.168.210.1
vmLF1/vmWP1: CTRL C abbrechen
vmWP1: Aufzeichnung von vmLF1 mit pscp.exe ins Verzeichnis C:\capdat
vmWP1: vmWP1-ping-vmfl1-r.pcap und vmWP1-ping-vmlf1-s.pcap mit Wireshark öffnen und vergleichen
vmWP1: Filter auf icmp stellen
Verschiedene Ping Auswertungs Infos:
Protokolle ping-Befehl: ICMP, IP, Ethernet
ICMP-Request Senderseite: 192.168.210.10 -> 192.168.210.1 ICMP 74 Echo (ping) request
Beteiligte PDU's beim ping: Paket, Frame, Bit
Unterschied tshark / tcpdump: id bei tshark hexadezimal, bei tcpsump dezimal ; - ttl wird nur bei tshark angezeigt
- Länge wird nur bei tcpdump angezeigt ; - tcpdump zeigt Namen an, tshark IP
Unterschied ttl: - ICMP-request hat 128 ; - ICMP-replay hat 64
Unterschied der zwei Auswertungen: keine, es sind die gleichen ICMP Pakete
Konsequenz ersten Punkt: Es spielt keine Rolle an welchem Endpunkt die Aufzeichnung gemacht wird wenn die überwachten Geräte im gleichen Netz sind.
ICMP-Filter: Es werden nur die ICMP-Pakete angezeigt
Display-Filter icmp.type == 0: Es werden nur die ICMP-Replys angezeigt.
Display-Filter für die ICMP-Requests: icmp.type == 8
Bereich für ICMP-Type: Paketdetail, Abschnitt Internet Control Message Protocol (Type 8 request, Type 0 reply).
Filter ip.dst == 192.168.210.1: Nur die Pakete welche für vmLF1 bestimmt sind, in unserem Fall die ICMP-Request.
Nur ausgehende Pakete von vmWP1 sehen: ip.src == 192.168.210.10
Der Ping-Befehl schickt per Default 32 Byte Daten. Daten finden und aussehen: Im Unterabschnitt Data des Internet Control Message Proto-col und zwar wiederholt die Kleinbuchstaben a..w.
Laufzeit zwischen einem ICMP-Request und einem ICMP-Reply herauslesen: Die Time-Differenz zwischen ICMP-Request und ICMP-Reply.

Alles an Strom = aktiv sonst Passiv | Endgerät = NAS, Drucker, virtueller Server, virtueller PC, PC | Netzwerkkomponente = Switch, WLAN/Router, Firewall | Netzwerkmedium: Funk, Kupfer, Glaskabel

DHCP-Bezug

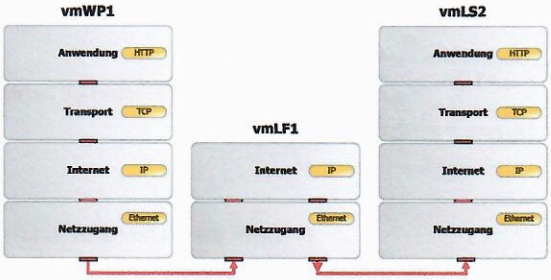
vmLF1 (Konsole 2): dhcpcd –k red0
vmLF1 (Konsole 2): ifconfig red0 up
vmLF1 (Konsole 1): tcpdump –i red0 –s 65535 –w /tmp/lf1-dhcp-iet-r.pcap
vmLF1 (Konsole 2): dhcpcd –n red0
vmLF1 (Konsole 1): Mit CTRL C Aufzeichung abbrechen + Firewall zurücksetzen
/etc/init.d/network restart
vmWP1: Aufzeichung vmLF1 mit pscp.exe ins Verzeichnis C:\capdat
vmWP1: lf1-dhcp-iet-r.pcap mit wireshark öffnen.
Verschiedene DHCP Auswertungs Infos:
Protokoll DHCP Transportschicht: UDP
Zielport vmLF1 DHCP Anfrage: 67
Quellport vmLF1 DHCP Anfrage: 68
Filter Ziel- und Quellport DHCP-Anfrage: udp.port == 68 and udp.port == 67
DHCP-Anfrage anders filtern: bootp





HTTP-Anfrage

vmWP1: Chrome starten und CTRL SHIFT DELETE Cache löschen
vmWP1 (CMD mit Adm): C:\> arp –d
vmLF1: ip –s –s neigh flush all
vmLF1: tcpdump –i green0 –s 65535 –w /tmp/wp1-http-ls2-lf1.pcap
vmLS2: tshark –i eth0 –w /tmp/wp1-http-ls2-ls2.pcap
vmWP1: In Chrome http://192.168.220.11 aufrufen
vmLF1 und vmLS2: Aufzeichnung mit CTRL C abbrechen
vmWP1: Aufzeichnungen von vmLF1 und vmLS2 in Verzeichnis C:\capdat
vmWP1: wp1-http-ls2-lf1-pcap und wp1-http-ls2-ls2.pcap mit Wireshark öffnen
vmWP1: In beide Fenster den Display-Filter arp setzen und Apply drücken
1)vmWP1: Setzen Sie den Display Filter je auf ip.dst == 192.168.220.11 && http
Verschiedene DHCP Auswertungs Infos:



Protokolle arp: ethernet und arp
Unterschied arp-Broadcast in beiden Auswertungen: - MAC von vmWP1 frägt MAC von vmLF1 green0 - MAC vmLF1 orange0 frägt MAC von vmLS2
Filter1): es werden nur Pakete mit der Ziel-IP 192.168.220.11 mit http-Anwendungsanfragen angezeigt
Schichtenunterschied der 2 Dateien: Netzzugangsschicht. Die MAC-Adressen sind bei den gleichen Sätzen verschieden. Einmal vmWP1 -> vmLF1, dann vmLF1 -> vmLS2

OSI

Nr.	OSI-Schicht	Aufgabe	TCP/IP-Schicht	Adressierung	Komponente	PDU	Kapselung	Protokolle etc
7 / 4	Application Layer Anwendungsschicht	Stellt Anwendungen Netzwerkdienste zur Verfügung	Application Layer Anwendungs-schicht		PC	Data	ND, AH	HTTP, FTP, DNS, DHCP, RADIUS
6 / 4	Presentation Layer Darstellungsschicht	Stellt Kompatibilität unterschiedlicher Datenformate her					ND, AH, PH	ASCII, ASN.1, SSL
5 / 4	Session Layer Sitzungsschicht	Stellt Verbindungen von Applikation zu Applikation her (Aufbau, Management, Abbau)					ND, AH, PH, SH	NetBIOS, SSL, RADIUS, TCP(SessMa)
4 / 3	Transport Layer Transportschicht	Stellt Verbindung von Endkomponente zu Endkomponente her (Aufbau, Management, Abbau und Anforderung verlorengegangener Daten)	Transport Layer Transportschicht	Portnummern	Firewall	Segment	ND, AH, PH, SH, TH	TCP UDP
3 / 2	Network Layer Vermittlungsschicht	Stellt Dienst zur globalen Adressierung und Wegewahl zur Verfügung	Internet Layer Internetschicht	IP Adresse	Router Switch	Packet	ND, AH, PH, SH, TH, NH	ICMP, DHCP, Broadcast, IP, Standargw, Subnetzmask
2 / 2	Data Link Layer Sicherungsschicht	Stellt Dienst zur physikalischen Adressierung und Übertragung über das Medium zur Verfügung. Regelt den Zugriff auf das Medium	Netzwerk Access Layer Netzzugangs-schicht	Mac Adresse	Hub Switch Bridge Netzwerkkarte	Frame	ND, AH, PH, SH, TH, NH, DLH, DLT	Kollision ARP CSMA/CD
1 / 1	Physical Layer Bitübertragungs-schicht	Definiert die physikalische Darstellung eines Bits sowie Normen und Standards der Übertragungsmedien, Stecker und Schnittstellen			Kupferkabel Glasfaserkabel Hub Netzwerkkarte Repeater	Bits	Bitcode über das Medium	Ethernet RJ45 Kollision

ND: Nutzerdaten | AH: Application Header | PH: Presentation Header | SH: Session Header | TH: Transport Header | NH: Network Header | DLH: Data Link Header
DLT: Data Link Trailer = Übertragungsfehler aufdecken | SAP: Service Access Point = Schnittstelle zwischen Schichten | Kapselung = Bewegung der Daten durch Schichten | PDU: Protocoll Data Unit

Horizontale oder virtuelle Kommunikation: Kommunikation zwischen Peers. Auch das Protokoll der Schicht X/Y…
Vertikale oder reale Kommunikation: Kommunikation zwischen benachbarten Schichten.
Schnittstelle: Befindet sich in diesem Fall zwischen zwei Schichten. Dadurch kann Schicht X auf die darunterliegende Schicht Y zugreifen.