Protokoll - Network Sniffing und Portscanning

Manuel Neufeld, Dennis Tobias Rautenberg

October 19, 2016

Chapter 1

Intro

1.1 Versuchsaufbau

Bei unserem Versuchsaufbau in unserem Labor wurde der bestehende Switch durch einen Hub ersetzt, um so alle Datenpakete aller Teilnehmer mitlesen/sniffen zu können.

1.2 Software

Wir verwenden für die uns bevorstehende Aufgabe das Betriebsystem Ubuntu und die Software Wireshark.

Figure 1.1: Wireshark Logo

Chapter 2

Grundlagen des Network-Sniffing

Chapter 3

Aufgaben

3.1 a.) Analyse von typischem Netzwerkverkehr

3.1.1 Aufbauen einer TCP Verbindung

Bauen Sie eine TCP Verbindung zu einem Dienst (z.B. http(s), ftp, smb, ssh, telnet) ihrer Wahl auf und beschreiben sie den Ablauf des Verbindungsaufbau/Verbindungsabbau (Sequenzdiagramm).

3.1.2 Verbindungsversuch - geschlossener TCP Port

Was passiert bei einem Verbindungsversuch auf einem geschlossenen TCP Port (Sequenzdiagramm), z.B. telnet auf Port 161 (Befehl: telnet $< ip >$ 161).

3.1.3 Beobachtung - DNS Traffic

Sniffen Sie den DNS Traffic aus dem Netzwerkverkehr heraus, was beobachten Sie?

3.1.4 Filtern von nicht IP basiertem Traffic

Filtern Sie den nicht IP basierten Traffic heraus. Was bleibt nun noch übrig?

3.2 b.) Sniffing von Passwörtern

3.2.1 Verbindung zu Telnet und FTP

Verbinden Sie sich mit anderen Telnet und FTP Servern, nutzen Sie den PC Ihres Nachbarn!

3.2.2 Passwort Sniffing

Versuchen Sie Passwörter und Benutzernamen anderer Benutzer, mitzusniffen. Filtern Sie gezielt die entsprechenden Pakete heraus.

3.2.3 Unterschied des übermittelten Passworts

Beschreiben Sie den Unterschied zwischen dem FTP und Telnet Protokoll bezüglich der Passwort Übermittlung.

3.3 c.) Portscanning / Nmap

3.3.1 Scannen vom Labornetz

Scannen Sie das gesamte Labor Netz um aktive Systeme zu erkennen.

3.3.2 Genauere Untersuchung eines Rechners

Nehmen Sie einen Rechner genauer unter die Lupe und führen Sie einen detaillierten Portscan sowohl für TCP als auch für UDP Dienste durch.

3.3.3 Verschiedene Scanverfahren

Beobachten Sie die unterschiedlichen Scan-Varianten (Syn, Fin, Xmas, etc.) in Wireshark und analysieren Sie diese.

Chapter 4

Unterschied - Hub / Switch

4.1 Hub

Ein Hub ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Hub als Verteiler fuer die Datenpakete. Hubs arbeiten auf der Bituebertragungsschicht (Schicht 1) des OSI-Schichtenmodells und sind damit auf die reine Verteilfunktion beschraenkt. Ein Hub nimmt ein Datenpaket entgegen und sendet es an alle anderen Ports weiter. Das bedeutet, er broadcastet. Dadurch sind nicht nur alle Ports belegt, sondern auch alle Hosts. Sie bekommen alle Datenpakete zugeschickt, auch wenn sie nicht die Empfaenger sind. Fuer die Hosts bedeutet das auch, dass sie nur dann senden koennen, wenn der Hub gerade keine Datenpakete sendet. Sonst kommt es zu Kollisionen.[1]

4.2 Switch

Ein Switch ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler fuer die Datenpakete. Die Funktion ist aehnlich einem Hub, mit dem Unterschied, das ein Switch direkte Verbindungen zwischen den angeschlossenen Geraeten schalten kann, sofern ihm die Ports der Datenpaket-Empfaenger bekannt sind. Wenn nicht, dann broadcastet der Switch die Datenpakete an alle Ports. Wenn die Antwortpakete von den Empfaengern zurueck kommen, dann merkt sich der Switch die MAC-Adressen der Datenpakete und den dazugehoerigen Port und sendet die Datenpakete dann nur noch dorthin. Waehrend ein Hub die Bandbreite des Netzwerks limitiert, steht der Verbindung zwischen zwei Hosts, die volle Bandbreite der Ende-zu-Ende-Netzwerk-Verbindung zur Verfuegung.[2]

[1] http://www.elektronik-kompendium.de/sites/net/1405161.htm
[2] http://www.elektronik-kompendium.de/sites/net/0811021.htm