**Netzwerkanalyse mit WIRESHARK**

Ein Bild, das Text, Screenshot, Wolke, Berg enthält.

Automatisch generierte Beschreibung1. "ping" eines Hosts (z.B. olat.bbw.ch): Wie sieht der Paketverkehr aus?

Man sieht sofort das sich ein kleiner Hügel erhebt. Nach dem der Ping aufhört wird es wieder gerade, da kein Datenverkehr mehr ist. Wenn ich wieder Pinge dann kommt wieder ein Hügel.

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

Automatisch generierte Beschreibung2. Zeigen Sie die dazu nötigen ARP und DNS-Pakete auf und notieren Sie sich, was diese bezwecken.

DNS löst den Domainnamen in die entsprechende IP-Adresse auf, während ARP die physische Adresse (MAC-Adresse) für die IP-Adresse auflöst. Beide Protokolle werden benötigt für die Netzwerkkommunikation

3. Welches Transportprotokoll verwendet DNS?

DNS (Domain Name System) verwendet in der Regel das User Datagram Protocol (UDP) als Transportprotokoll. DNS-Anfragen und -Antworten werden normalerweise über UDP-Port 53 übertragen. UDP ist ein verbindungsloses, leichtgewichtiges Protokoll, das für DNS geeignet ist, da DNS-Anfragen oft klein sind und eine geringe Latenz erfordern. UDP wird bevorzugt, da es weniger Overhead hat im Vergleich zu TCP (Transmission Control Protocol).

4. Was ist charakteristisch daran und welches typische Transportprotokoll wird sonst noch verwendet?

UDP (User Datagram Protocol) wird im Domain Name System (DNS)

DNS kann jedoch in bestimmten Szenarien auf das Transmission Control Protocol (TCP) zurückgreifen.

Wo zuverlässige Übertragung erforderlich ist, wird auch oft beispielsweise DNSSEC benutzt.

Welches Protokoll wird verwendet für den "ping"?

Für den "ping"-Befehl wird das Internet Control Message Protocol (ICMP) als Transportprotokoll verwendet. ICMP ist ein Netzwerkprotokoll, das speziell für die Übertragung von Nachrichten verwendet wird, um die Erreichbarkeit eines Hosts im Netzwerk zu überprüfen

Wozu dient der Ping?

Der "ping"-Befehl dient dazu, die Erreichbarkeit eines Netzwerkhosts zu überprüfen und die Latenzzeit für die Datenübertragung zu messen. Es wird häufig für Netzwerkdiagnosen verwendet, um Probleme zu identifizieren.

Machen Sie eine Google-Anfrage mit dem Begriff „Sniffing“.

=> Was bedeutet der Begriff?

Mit Sniffing bezeichnet man die Echtzeitüberwachung des Internetdatenverkehrs. Es handelt sich dabei um ein Programm oder ein Hardware-Gerät, mit welchem man Interaktivitäten ausspionieren kann.

Was fällt im aufgezeichneten Netzwerkverkehr auf?

Der Netzwerkverkehr ruht nicht es kommen oder gehen immer wieder Dinge raus oder rein. Manchmal kommt auch ganz viel auf einmal.

Finden Sie den Begriff „Sniffing“ im Datenverkehr? Begründen Sie.

Nein bei mir habe ich diesen Begriff nicht gefunden, daher denke ich das das schon recht gut ist, ausserdem denke ich das man bei einer VM nicht Sniffen kann.

Könnten Sie ein Passwort sniffen? Begründen Sie

Ja könnte man den wenn man Passwörter über eine http Seite schickt dann könnten diese Abgefangen werden. Dies kann auch mit anderen Datenpackete passieren.