Labor II

In dieser Laboreinheit werden durch Einsatz eines „angreifenden" Routers gefälschte Routeninformation in ein über OSPF ohne Authentifizierung geroutetes Netz eingeschleust.

Protokollieren Sie für jede Aufgabe alle Schritte (auf sinnvoller Abstraktionsebene) mit, beantworten Sie im Protokoll auch die Fragestellungen am Ende jeder Aufgabe. Einige Fragestellungen sind optional (sie dienen der Verbesserung der Note, siehe Folien). Dieses Protokoll geben Sie bitte auf Moodle bis zum in der Moodle Abgabemaske angegebenen Termin ab.

Diese Einheit wird in Teams durchgeführt. Es ist zulässig, das Protokoll im Team zu verfassen. Der Upload muss trotzdem von jedem Teammitglied einzeln durchgeführt werden. Für jedes Teammitglied besteht die Möglichkeit, das Protokoll individuell zu verbessern (z.B. durch Erarbeitung von Zusatzaufgaben.)

Sollten Sie die Übung in der verfügbaren Zeit nicht abschließen können, ist es möglich die Übung im Packet Tracer durchführen (downloadbar unter `http://cisco.netacad.net/`).

1 Aufbau der Testumgebung

1. Bilden Sie Teams.
2. Jedes Team braucht:
   - 4 Router
   - 3 Switches

Konfigurieren Sie eine Testumgebung, basierend auf dem Netzwerkdiagramm in Abbildung 1 – jedes Teammitglied konfiguriert mindestens einen Router. Die Clockrate für den seriellen Link zwischen `RouterA` und `RouterB` ist 64000, DCE ist bei `RouterA`. `RouterA`, `RouterB`, und `RouterC` sind so zu konfigurieren, dass sie ihre Routinginformationen über OSPF austauschen (Area 0). Für den PC `User1` und den `WebServer` können Sie Laborrechner verwenden. (Es ist nicht notwendig, auf dem Rechner `Webserver` tatsächlich einen Webserver-dienst zu konfigurieren).

Verifizieren Sie den korrekten Aufbau der Testumgebung indem Sie von PC `User1` den Rechner `WebServer` pingen. (Stellen Sie vorher sicher, dass die Windows Firewall auf beiden Geräten Pings zulässt.)

2 Router Spoofing

Fügen Sie nun einen angreifenden Router (`RouterX`) zum Netzwerk hinzu, siehe Abbildung 2.Dieser Router propagiert über OSPF (in der gleichen Area wie `RouterA`, `RouterB` und `RouterC`) eine

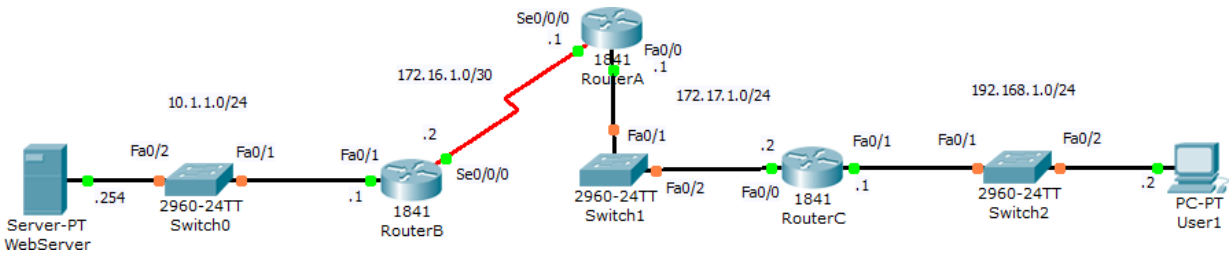

Abbildung 1: Testaufbau

Route zu Netzwerk `10.1.1.0/24`. Dies hat zum Ziel, Zugriffe von PC `User1` auf `10.1.1.254` (die IP Adresse des `Webservers`) auf den an `RouterX` angeschlossenen `FakeServer` umzuleiten.

(Sie müssen keinen Webserver installieren, der gefälschte Routeneintrag auf `RouterC` und der Output eines `tracert` von PC `User1` auf die IP `10.1.1.254` ist ausreichend. Falls Sie genug Zeit haben, spricht natürlich nichts dagegen, einen Webserverdienst auf `Webserver` und `FakeServer` aufzusetzen.)

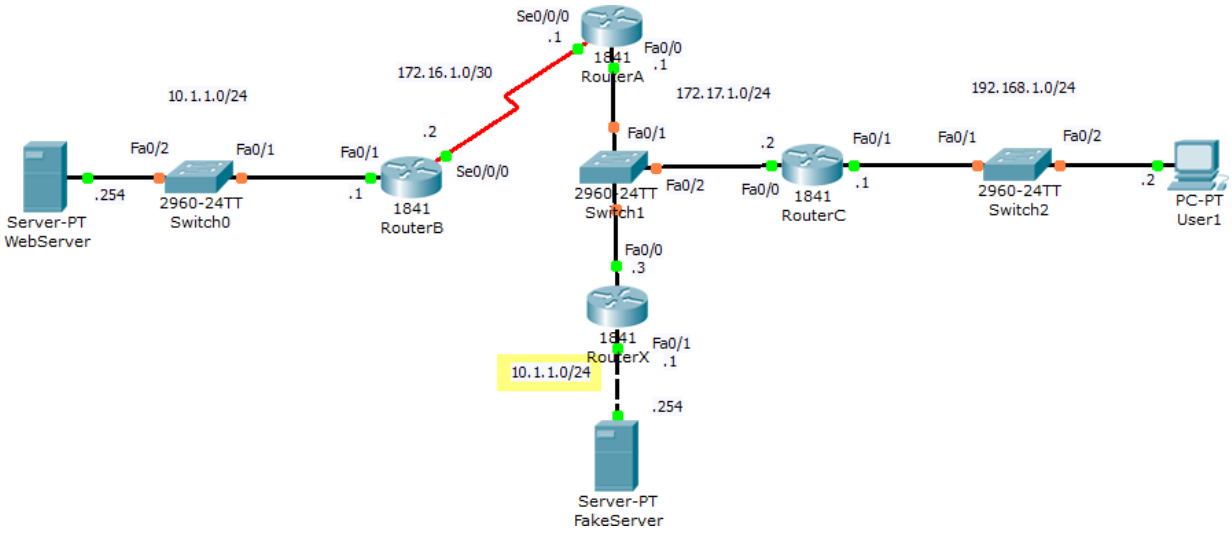

Abbildung 2: Testumgebung mit Router Spoofing

3 Router Authentication

Konfigurieren Sie, als Maßnahme gegen die Spoofing Attacke, Authentifizierungsmechanismen für OSPF auf `RouterA`, `RouterB`, und `RouterC`.

Details dazu finden Sie in den CCNA Online Inhalten (CCNAv5: Semester 3, Kapitel 5.1.5.4, CCNAv4: Semester 4, Kapitel 4.3.2) auf `http://cna.fh-salzburg.ac.at` oder `http://www.netacad.com`.

Beschreiben Sie in Ihrem Protokoll die Einrichtung und Funktionsweise des verwendeten Authentifizierungsverfahren. Gehen Sie auch auf Alternativen ein.

4 Sniffing Attacke auf Clear Text Password Routher Authentication (ADVANCED)

Verbinden Sie einen PC mit `Switch1`, um mittels Wireshark alle Pakete der OSPF Authentifizierung mitzusniffen.

Untersuchen Sie die folgenden beiden Authentifizierungsverfahren:

- Clear Text Password
- MD5-Hash

Beantworten Sie folgende Fragen:

- Welche Informationen kann ein potentieller Angreifer auf diese Weise herausfinden? Welche Probleme ergeben sich bei Authentifizierungsverfahren 1)?
- Welchen Vorteil hat Authentifizierungsverfahren 2) (und welche Nachteile hat andererseits der verwendete Hashing Algorithmus MD5)?