Informationssicherheit Praktikum Nr.1: Reconnaissance, Portscans mit NAMP und Angriffe mit CAIN

Wie jeder *normale* Einbrecher kundschaftet auch ein Cracker sein Ziel zuerst aus. Reconnaissance ist der entsprechende englische Begriff dafür. Es gibt passive Reconnaissance und aktive Reconnaissance. Bei der passiven Reconnaissance werden Daten, die im Internet frei verfügbar sind, gesammelt. Das eigentliche Ziel wird dabei noch nicht kontaktiert. Diese Informationsbeschaffung ist nicht strafbar! Bei der aktiven Reconnaissance werden dann die Ziele direkt nach Informationen untersucht. Prinzipiell ist auch das nicht strafbar, allerdings wird aktive Reconnaissance, wie z.B. ein Portscan, von den betroffen Administratoren als feindlicher Akt betrachtete, da er häufig auch die Vorstufe zu einem Angriff ist. Führen Sie also niemals einen Portscan in einem Netz durch, ohne dem verantwortlichen Admin VORHER zu unterrichten. Dies gilt ins besondere für das Netz der FH Aachen!! (Hinweis: Im Netz der FH Aachen monitoren IDS-Systeme das Netz, die Portscans erkennen und den Benutzer, ob im Ethernet oder im Wireless LAN, ermitteln können. Da ein Portscan den Benutzerrichtlinien wiederspricht, könnte der/diejenige mächtig Ärger bekommen!!)

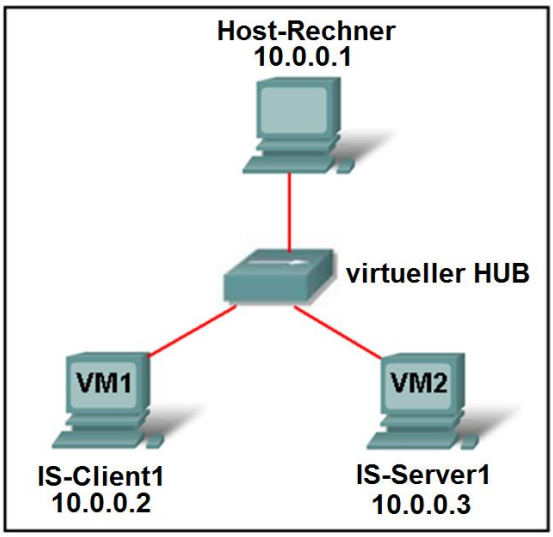
Was im produktiven Netz der FH Aachen verboten ist, können wir aber in einer privaten Umgebung sehr wohl durchführen und testen.

In diesem Praktikum arbeiten Sie mit 2 virtuellen Maschinen, **IS-Client1** und **IS-Server1**. Sie werden den Server vom Client aus mit NMAP scannen.

Anschließend sollen Sie einige Angriffe mit ***CAIN*** auf den Server starten.

Auf den VMs sind alle benötigten Programme schon installiert. Prüfen Sie, dass Sie über die virtuelle Netzwerkkarte Host-only-Ethernet Adapter verbunden sind.

Der gesamte Aufbau sieht folgendermaßen aus, prüfen Sie ob alle IP Adressen richtig eingestellt sind!



Hinweis: Prüfen Sie die IP Adressen aller beteiligten Systeme.

1. Teil: Aktives Reconnaisance - Portscans mit NMAP

1. Starten Sie den VMWare-Server (local Host) unter ***Start/Programme/Informatik/VMWare/ VMWare Server/VMWare Server Console***. Klicken Sie auf die VM VM-Client1, Sie sehen die Konfiguration der VM. Links unten unter **Notes** sehen Sie alle konfigurierten Benutzer und deren Passwörter!
   Hinweis: Falls die VMs nicht im Inventory sichtbar sind, müssen Sie sie erst eintragen. Dazu klicken Sie auf ***File/Open***, dann auf ***Browse***. Sie finden die VMs dann unter C:\Hoefken.

2. Starten Sie die beiden VMs nacheinander und loggen Sie sich ein (Benutzername ***infosec)***, Passwort ***P@ssword***). Falls Sie aufgefordert werden einen neuen Identifier zu erzeugen, klicken Sie auf ***Create***.
   Hinweis: Die Tastenkombination **Strg-Alt-Entf** wird in *VirtualBox* durch die Tastenkombination **Strg-Rechts Entf** ersetzt!

3. Öffnen Sie auf **IS-Client1** eine DOS-Box. Geben Sie den Befehl **nmap** ein.
   Mit welcher NMAP-Version arbeiten Sie? **4.53**

4. Prüfen Sie, dass Sie den **IS-Server1** und den **Host-Rechner** (siehe Schaubild auf Seite 1) erreichen können.
   Welche Befehle verwenden Sie?
   ping 10.0.0.1
   ping 10.0.0.3

   Hinweis: Falls Sie den Server nicht erreichen können, führen Sie eine Fehlersuche (wie in GCN erlernt) durch.
   Hinweis: Der Host ist durch eine Firewall geschützt, schalten Sie diese für die VirtualBox-NIC ab.

5. Öffnen Sie **WireShark** und starten Sie ein Capture auf die VM-NIC mit der IP Adresse 10.0.0.2.

6. Führen Sie einen TCP Connect Scan der VM **IS-Server1** durch. (**Hinweis:** Dieser Scan kann 5-10 Minuten dauern, bewahren Sie RUHE! Wenn Sie den Parameter **–v** mit verwenden, erhalten Sie schon Zwischenergebnisse auf dem Bildschirm,)
   Welchen Befehl verwenden Sie?
   nmap –sT 10.0.0.3

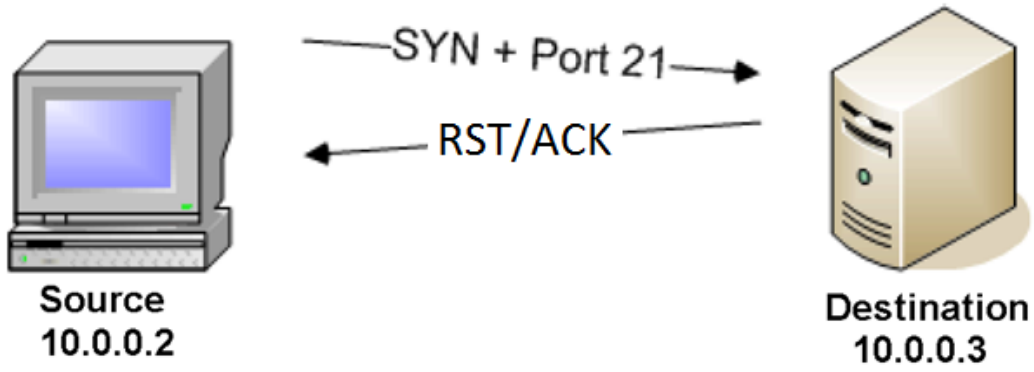
7. Stoppen Sie nach dem Scan den WireShark-Mitschnitt!
   Welche offenen Ports hat NMAP gefunden?
   23,80,135, 139, 445, 1025, 1026,3389

8. Suchen Sie in **WireShark** über den Filter den Scan des TCP-Ports 1111. Zeigen Sie alle Pakete an, in denen der Port 1111 vorkommt. Über den Knopf **Expression…**, oben neben dem Filterfenster, können Sie den benötigten Filterstring zusammen bauen.

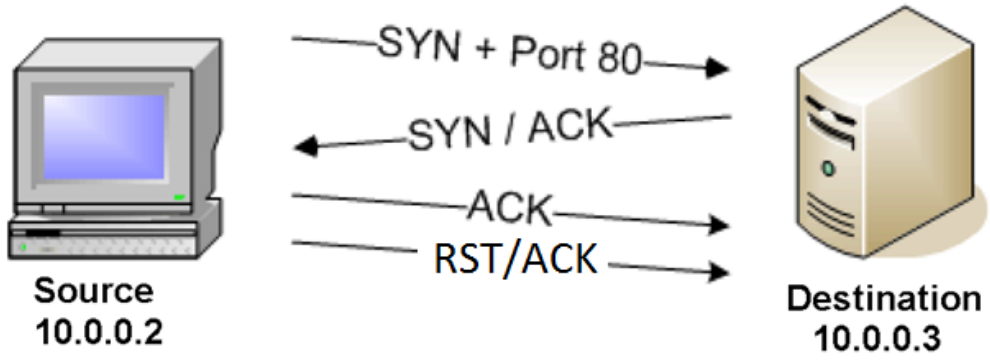
   Wie lautet der benötigte Filterstring? **tcp.port == 1111**

   Drücken Sie anschließend **Apply**.

9. Erstellen Sie eine Grafik, in der der Kommunikationsablauf bezüglich eines geschlossenen TCP Ports eingetragen ist.



10. Führen Sie das Gleiche noch einmal mit einem geöffneten Port durch und erstellen Sie noch eine Grafik.



11. Entfernen Sie den Filter und beantworten Sie die folgenden Fragen.

12. Wie viele Verbindungen baut NMAP (etwa) pro Sekunde zum Server auf?

    Hinweis: Wenn Sie ein Paket mit der rechten Maustaste anklicken, können Sie einen Zeitreferenzpunkt setzten.

    Ca. 20-40

13. Diese Art des Scannens fällt in jeder Logdatei sofort auf. Um die Anzahl der Scans zu beschränken können Sie den –T Parameter verwenden. In welchem Abstand werden die Scans bei dem Parameter **–T1** gestartet?

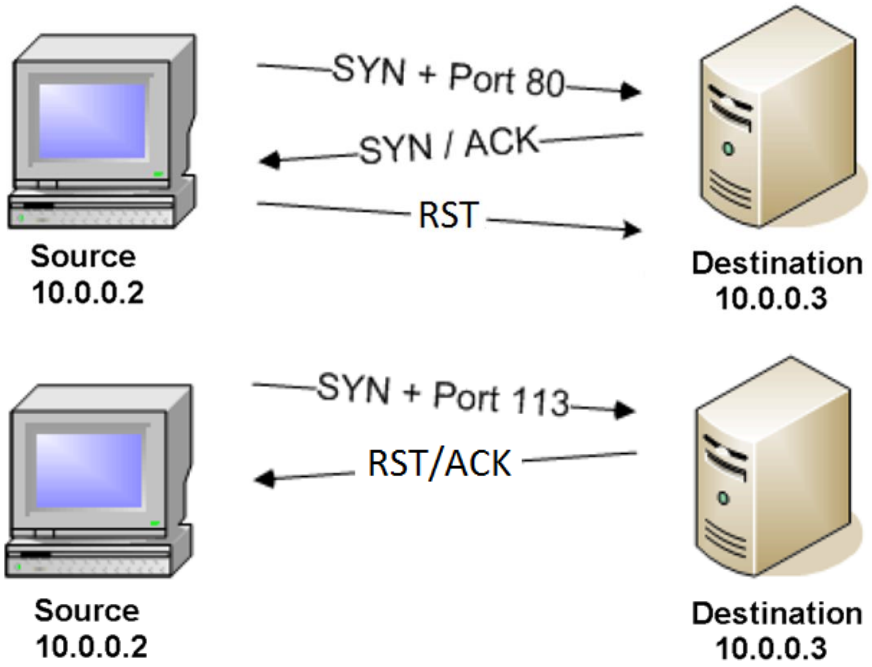
    ca. 5 Scans in 15 Sekunden

14. Ein kompletter TCP Verbindungsaufbau wird auch von vielen Logging-Programmen aufgezeichnet. Um das zu verhindern wird der *SYN-Stealth* Scan verwendet.

15. Starten Sie einen neuen Capture und scannen Sie den **IS-Server1** mit dieser Art des Scans. Welchen Befehl müssen Sie verwenden?

    nmap –sS 10.0.0.3

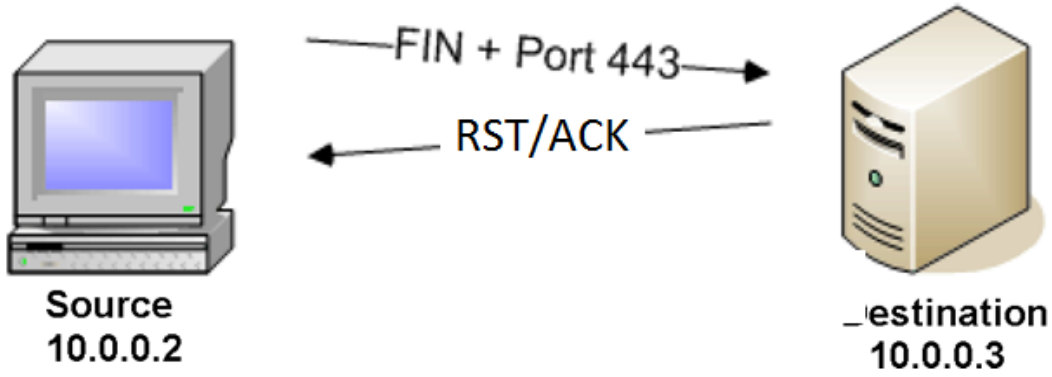
16. Erstellen Sie wieder eine Grafik des Verbindungsverlaufs für einen offenen und für einen geschlossenen Port.



17. Führen Sie nun noch einen *FIN*-Scan durch und zeichnen Sie ihn mit WireShark auf. Wie lautet der entsprechende Befehl?

    nmap –sF 10.0.0.3

18. Wie sieht der Kommunikationsablauf aus (Grafik).



19. Finden Sie offene Ports? **Nein! Bei Windows werden keine offenen Ports gefunden!**

20. Was ist der Vorteil eines FIN-Scans?

Es werden keine Verbindungen aufgebaut, die von Logserver aufgezeichnet werden können. Es werden weiterhin nur sehr wenige Nachrichten ausgetauscht (Netzbelastung).

21. Was ist der Nachteil eines FIN-Scans?

Funktioniert nicht mit Microsoft Betriebssystemen. Benutzer muss Adminrechte haben, um diese, nicht TCP/IP-konformen Pakete zu erzeugen.

Teil 2: Angriffe mit CAIN – Der ARP-Spoof Angriff

Im Rahmen von GCN haben Sie schon das ARP Protokoll kennen gelernt. Eine Eigenschaft von ARP ist dabei aber nicht zur Sprache gekommen*: Gratuitous ARP*. Diese Eigenschaft wird vom ARP Spoofing Angriff ausgenutzt, daher hier ein kurzer Theorieeinschub.

Gratuitous ARP

Gratuitous ARP (engl. „unaufgefordertes ARP“) bezeichnet eine spezielle Verwendung von ARP. Dabei sendet ein Host ein ARP-Anforderungs-Broadcast, bei dem er seine eigene IP-Adresse als Quell- und Ziel-IP-Adresse einträgt. Damit teilt er seine ggf. neue MAC-Adresse unaufgefordert mit. Das kann mehreren Zwecken dienen:

a. Normalerweise darf keine Antwort kommen, denn eine IP-Adresse muss in einem Netz eindeutig sein. Bekommt er trotzdem eine Antwort, ist das für den Administrator ein Hinweis darauf, dass ein Host nicht richtig konfiguriert ist.
b. Jeder Host aktualisiert seinen ARP-Cache. Das ist beispielsweise dann nützlich, wenn die Netzwerkkarte eines Rechners ausgetauscht wurde und die anderen Hosts über die neue MAC-Adresse informiert werden sollen. Gratuitous ARP geschieht deshalb normalerweise beim Booten eines Computers.
c. Wenn zwei Server aus Gründen der Ausfallsicherheit als Server und Ersatzserver aufgebaut sind und sich eine IP-Adresse teilen und der aktive Verkehr vom einen auf den anderen geschwenkt werden soll, ist die IP-Adresse jetzt über eine andere MAC-Adresse zu erreichen. Diese neue MAC-/IP-Adress-Zuordnung muss bekannt gemacht werden. Sonst bekommt niemand den Wechsel mit.
d. In einem *Mobile IP*-Szenario sendet der *Home Agent* einen *Gratuitous ARP*, wenn sich der *Mobile Host* aus dem Heimatnetz entfernt, um die Pakete stellvertretend für diesen zu empfangen. Analog sendet der *Mobile Host* einen *Gratuitous ARP*, sobald er sich wieder im Netz befindet.

Quelle: Wikipedia.org

22. Starten Sie CAIN auf dem **IS-Client1**.

Nun wollen wir einen ARP-Spoofing Angriff durchführen. Der Datenverkehr zwischen **IS-Server1** und **Host** soll über **IS-Client1** geleitet werden (Man-in-the-Middle).
Um das zu verifizieren notieren wir noch einmal die IP/MAC-Adresspaare, die aktuell auf den Rechnern bekannt sind.

23. Scannen Sie zuerst das lokale Netzwerk, um herauszufinden, welche Rechner vorhanden sind. Öffnen Sie dazu in **CAIN** den Reiter *Sniffer*.

24. Starten Sie den Sniffer (**2. Icon von links**). Wechseln Sie (falls nötig) auf das Fenster **Hosts** (Reiter unten). Wenn Sie dazu aufgefordert werden, wählen Sie die Netzwerkkarte mit der IP Adresse 10.0.0.3. Klicken Sie auf das **blaue Pluszeichen**.

25. Scannen Sie alle Rechner in Ihrem Subnetz. Wählen Sie unter *Promiscous Mode Scanner* den Punkt *All Tests* aus.
Welche Rechner werden gefunden? Tragen Sie alle Daten (IP/MAC) in die Tabelle unten ein.

IP-Adresse	MAC-Adresse
10.0.0.1	xx:xx:xx:xx:xx:xx
10.0.0.3	xx:xx:xx:xx:xx:xx

26. Wechseln Sie auf den **IS-Server1**. Öffnen Sie eine DOS-Box und pingen Sie den **Host** (10.0.0.1) an. Zeigen Sie den ARP-Cache mit dem Befehl ***arp –a*** in der DOS-Box an.
Welche MAC-Adresse wird angezeigt? **xx:xx:xx:xx:xx:xx**

27. Nun wird das ARP-Poisoning gestartet.

Hinweis: Zeichen Sie den gesamten Vorgang mit WireShark auf dem Server auf! (Vergleichen Sie den Ablauf mit dem in den Dateien ***ARP Spoofing*** und ***ARP Spoofing Ablauf*** auf dem Ilias Server!)

28. Wechseln Sie wieder auf **IS-Client1**.

29. Öffnen Sie den Reiter *ARP* (**unten**) im Fenster *Sniffer* und klicken Sie in das obere rechte Teilfenster. Das Pluszeichen oben in der ICON-Zeile wird blau.

30. Nun können Sie die Teilnehmer der Verbindung auswählen, die Sie über Ihren Rechner leiten wollen, indem Sie auf das Pluszeichen klicken. Wählen Sie einen Teilnehmer im linken Teilfenster aus. Es erscheint dann (der noch verbleibende) Rechner im rechten Teilfenster. Wählen Sie diesen auch aus. Klicken Sie auf *OK*.

31. Die Rechner erscheinen im Fenster. Der Status der Verbindung wird mit ***Idle*** (Leerlauf) angezeigt. Starten Sie den Angriff, indem Sie auf das **gelbe ARP-Icon** in der ICON-Leiste oben klicken.

32. Der Zustand wechselt von ***Idle*** auf ***Poisoning***.

33. Wechseln Sie wieder auf **IS-Server1**, pingen Sie den Host und prüfen Sie erneut dessen MAC-Adresse.

    Wie lautet nun die angezeigte MAC-Adresse? **Es ist die des Angreifers**

34. Welcher VM gehört diese MAC-Adresse? **s.o.**

35. Welchen Weg nehmen Daten vom Server zum Host?

    Über den Angreifer

36. Untersuchen Sie Ihre **WireShark** Aufzeichnung und vollziehen Sie die Aktionen des ARP Spoofing nach, es werden von den Betreuern dazu Fragen gestellt.

Damit ist das Praktikum beendet.

Bevor Sie weiterarbeiten, zeigen Sie das Ergebnis den Betreuern!

Klicken Sie links oben auf ***Maschine***, dann auf Schließen.

Wählen Sie im aufgehenden Fenster den untersten Punkt: Die virtuelle Maschine ausschalten. Setzen Sie einen Haken bei ***Zurückkehren auf den Sicherungspunkt…***

Klicken Sie nun auf **OK**.

Jetzt gibt's das Testat.