Inhalt

[NVS AUSARBEITUNG FRAGEN 1](#_Toc532916059)

[1. Mit welchen Befehlen bekomme ich Infos über das lokale Netz (DNS Server, Gateways, DHCP Server…)? 1](#_Toc532916060)

[2. Wie heißt die Linux Distribution, die speziell für security Analysen (und hacking) zusammengestellt wurde? 1](#_Toc532916061)

[3. Was sind jeweils wireshark, cain&abel, shodan, mitmproxy, certificate spoofing. 1](#_Toc532916062)

[4. Was ist eine „man in the middle“ Attacke. Welches Protokoll wird dabei verwendet (OSISchicht?) 1](#_Toc532916063)

[5. Welche Infos benötigt man, um einen LDAP Authentifizierungsversuch durchzuführen? Wie sieht der connect string ungefähr aus? Was kann man als Administrator dagegen tun? 2](#_Toc532916064)

[6. Bedeutung von /etc/hosts.allow und /etc/hosts.deny? 2](#_Toc532916065)

[7. Wann wird nfs und wann samba verwendet? 2](#_Toc532916066)

[8. Mit welcher Datei wird nfs konfiguriert? Welche gravierende Sicherheitseinschränkung hat nfs? 2](#_Toc532916067)

[9. Was sind die wichtigsten Schritte beim Installieren eines samba Servers mit Zugriffsrechten auf Benutzerebene? 2](#_Toc532916068)

[10. Was bedeuten die folgenden Zeilen 3](#_Toc532916069)

[browseable = yes …Share ersichtlich in Liste der verfügbaren Shares create mask = 0775 …bei erstellen der Datei hat user rwx(7), group rwx(7) & other rx(5) Rechte force directory mode = 0775 …neuer Ordner mit gezwungenen Rechten user rwx, group rwx, other rx force user = schueler …Nachdem eine Verbindung hergestellt wurde, werden alle Operationen als schueler durchgeführt force group = www-data …alle user werden der group „www-data“ zugeordnet 3](#_Toc532916070)

[11. Wer ist www-data? 3](#_Toc532916071)

[12. Mit welchem Typ wird ein Windows Verzeichnis gemountet? 3](#_Toc532916072)

[13. Unterschied beim mount-Befehl von nfs und samba? 3](#_Toc532916073)

[14. writeable = yes und Zugriffsrecht ist 554. Was gilt? Wie ist die allgemeine Regelung in diesem Fall? 3](#_Toc532916074)

[15. Wie erfolgt die Arbitrierung von CSMA/CR beim CAN Bus? 3](#_Toc532916075)

[16. Wie funktioniert das Summentelegramm beim Interbus? 3](#_Toc532916076)

[17. Wie läuft ein Master-Slave Verfahren ab? Was ist in diesem Zusammenhang Token passing wie es beim Profibus verwendet wird? 3](#_Toc532916077)

[18. Was ist polling? 3](#_Toc532916078)

[19. Was bedeutet Echtzeitfähigkeit? 3](#_Toc532916079)

[20. Welche Vorteile hat WLAN im 2.4 GHz gegenüber dem 5GHz Netz, welche Nachteile hat es? 4](#_Toc532916080)

[21. Was 802.11ac? 4](#_Toc532916081)

[22. Was bedeutet roaming und welche Rolle spielen dabei das beacon Intervall und DTIM? 4](#_Toc532916082)

[23. Wozu dienen base-rates? 4](#_Toc532916083)

[24. Was ist eine LDAP- oder eine Radius Authentifizierung und wozu ist die gut? 4](#_Toc532916084)

[25. Für welche Komponenten steht LAMPP? 4](#_Toc532916085)

[26. Wie erreiche ich unter Linux den sql-prompt? 4](#_Toc532916086)

[27. Wie kann ich in mysql ein Reihe von sql-Statements ausführen, die in einer Datei gespeichert sind? 4](#_Toc532916087)

[28. Wie lautet die Syntax einer Schleife in der bash? 4](#_Toc532916088)

[29. Was ist die übliche Art der Datenbankverwaltung über eine GUI im LAMPP? 5](#_Toc532916089)

[30. Wie kann man am einfachsten https zur Verfügung stellen? 5](#_Toc532916090)

[31. Welche Schritte sind üblicherweise durchzuführen, um ein CMS zu einem anderen Provider zu transferieren? 5](#_Toc532916091)

[32. Was bedeutet die Notation MM1∞ ? 5](#_Toc532916092)

[33. Wie erhält man aus gleichverteilten Zufallszahlen exponentiell verteilte Zufallszahlen? 5](#_Toc532916093)

[34. Was bedeuten die Zeichen in folgenden Formeln? 5](#_Toc532916094)

[35. Wie hoch ist die Auslastung eines Servers, der 30 Anfragen pro Minute bekommt und für die Bearbeitung einer Anfrage 1 Sekunde benötigt? 5](#_Toc532916095)

[36. Wie kann man eine einfache Warteschlange (MM1∞) simulieren? Was ist dabei zu beachten? 5](#_Toc532916096)

NVS AUSARBEITUNG FRAGEN

1. Mit welchen Befehlen bekomme ich Infos über das lokale Netz (DNS Server, Gateways, DHCP Server…)?

ipconfig /all

1. IP Adresse
2. Gateway (da geht der gesamte Datenverkehr drüber)
3. DHCP (weist Clients ohne manuelle Konfiguration einem bestehenden Netzwerk zu), DNS (Adresse wir in die IP-Adresse umgewandelt) … Server (sind vielleicht für andere Aufgaben zuständig)

tracert URL

1. Hops zum Internet
2. Adresse zur Firewall

Netscan (Tool nicht in der cmd)

1. IP Adresse + Rechnername (ping -a auf alle Adressen im System) + Freigaben
2. 255.255.0.0 = 65534 Adressen müssen durchsucht werden (0 und höchste Broadcast-Adresse fällt weg)
3. Wie heißt die Linux Distribution, die speziell für security Analysen (und hacking) zusammengestellt wurde?

Kali Linux 🡪 bringt Netzwerk Testing-Tools für jeden Zweck mit, etwa um Netzwerkverbindungen zu analysieren oder Systeme auf Schwachstellen zu prüfen. Für Nutzer von ARM-Rechner, wie dem Raspberry Pi, gibt es abgespeckte Version.

1. Was sind jeweils wireshark, cain&abel, shodan, mitmproxy, certificate spoofing.

**Wire Shark** (🡪 Sniffer) 🡪 Besser in Analyse – Logger und Filter um spezielle Sachen zu verfolgen

**Cain & Abel** (🡪 Sniffer++) 🡪 „Man in the Middel” ausprobieren, 2 [oder mehr] Adressen eingeben 🡪 Poisonig auswählen

1

MITM

2

Sniffer zeigt Daten, die übertragen werden

**Website Shodan** 🡪 liefert Infos zu Rechnern, die ungeschützt im Netzt hängen, wenn der eigene dabei ist, ists nicht gut

**Mitmproxy** 🡪 fängt http und https Verkehr ab und protokolliert ihn mit, geht auch für Handys (MITM Attacke)

**Certificate spoofing** 🡪 Es könnte sich jemand als Empfänger ausgeben und einen falschen public key veröffentlichen (MITM Attacke) 🡪 zB bei einer http Website täuscht man dem User vor das diese ein https Zertifikat besitzt und kann sich somit Daten holen (Browser wird nichts melden)

1. Was ist eine „man in the middle“ Attacke. Welches Protokoll wird dabei verwendet (OSISchicht?)

In seiner einfachsten Form braucht sich der Angreifer nur zwischen zwei Parteien zu schalten, die miteinander kommunizieren, und muss dann nur die gesendeten Nachrichten abhören und sich zumindest als eine der beiden Parteien ausgeben. In der realen Welt kann so ein Angreifer zum Beispiel gefälschte Rechnungen an ein Opfer senden und dann einfach die von ihm zurückgeschickten Schecks abfangen.

**Cain & Abel MITM**

* Configuration für http (Schicht 5)… Schlüsselwörter im HTML Stream z.B.: User, Password
  + 🡪 Gefundene Passwörter werden geloggt (zusätzlich ftp, pop, imap, ldap)
  + Besonders interessant ist ldap weil dort alle active directory Anfragen durchlaufen

1. Welche Infos benötigt man, um einen LDAP Authentifizierungsversuch durchzuführen? Wie sieht der connect string ungefähr aus? Was kann man als Administrator dagegen tun?

Öffnungsversuch 🡪 Server, Username, Kennwort und Authentifizierungsmethode (secure oder nicht) mitgeben

strPath = "LDAP://" & strServer & "/" & strDomain & ":636"

'der gesamte string in einem: LDAP://gandalf.htl-vil.local/ou=Users,dc=htl-vil,dc=local[:Port] wobei der optionale Port 636 (SSL) oder 389 ist

Als Administrator Anmeldeversuche verzögern zB 1 Sekunde – für den Benutzer nicht so schlimm, brute force dauert dann aber ewig. Nützt natürlich nichts, wenn das Passwort asdf ist.

1. Bedeutung von /etc/hosts.allow und /etc/hosts.deny?

Wichtig sind bei allen Serverdiensten die Dateien

/etc/hosts.allow und /etc/hosts.deny in denen jeweils steht welche Dienste für wen erlaubt oder veweigert werden (zuerst wird allow ausgewertet dann deny)

zB in hosts.deny ALL:ALL dh es wird grundsätzlich alles verboten und dann in der allow die Dienste einzeln einschalten zB smbd:ALL oder smbd:192.168..

1. Wann wird nfs und wann samba verwendet?

**NFS:**

geht nur zwischen Linux Clients, sehr schnell (wesentlich performanter als samba)

nur in zentral verwalteten Umgebungen, wo der user nicht root ist (usermod nicht verwendbar) und der Admin auch die Netzwerkadressen vergibt.

**Samba:**

Wenn man von Linux auf Windows will 🡪 täuscht Windows Freigaben vor (-> Bei Win ist nichts zu tun außer Freigaben zu machen, Berechtigungen (jeder alles) und Sicherheit (konkret für Benutzer einschränken) setzen)

allgemein unter Linux Zugriffsrechte festlegen zB ALL:ALL oder smbd:ALL:

hosts.allow und hosts.deny

1. Mit welcher Datei wird nfs konfiguriert? Welche gravierende Sicherheitseinschränkung hat nfs?

/etc/exports 🡪 welche user (UID) bzw. welche Netzwerkbereiche dürfen zugreifen

Rechtevergabe sehr eingeschränkt (geht nur über die USERID) und lässt sich nicht auf IP Adressen beschränken

1. Was sind die wichtigsten Schritte beim Installieren eines samba Servers mit Zugriffsrechten auf Benutzerebene?

apt-get install samba

smbpasswd -a pupil //Hinzufügen von Samba Usern mit eigenem Password 🡪 muss auf linux  
 bereits als User existieren

pdbedit -w -L //Auflisten der User, ist nicht notwendig

/etc/samba/smb.conf bearbeiten //alle Einstellungen für Samba

Um z.B.: den Ordner, den apache veröffentlicht, zugänglich zu machen, kann man folgendes an das Ende von smb.conf anhängen

security = user //jeden Benutzer mit smbpasswd -a anlegen ODER = domain (holt sich info vom Active Direktory

[webprojects]  
path = /var/www/userspace  
browseable = yes  
writeable = yes  
force create mask = 0775

…

Dies würde den Zugriff auf den Folder /www/var/userspace für alle angelegten Benutzer freigeben

1. Was bedeuten die folgenden Zeilen

browseable = yes …Share ersichtlich in Liste der verfügbaren Shares  
create mask = 0775 …bei erstellen der Datei hat user rwx(7), group rwx(7) & other rx(5) Rechte  
force directory mode = 0775 …neuer Ordner mit gezwungenen Rechten user rwx, group rwx, other rx  
force user = schueler …Nachdem eine Verbindung hergestellt wurde, werden alle Operationen als  
 schueler durchgeführt  
force group = www-data …alle user werden der group „www-data“ zugeordnet

1. Wer ist www-data?

(externer) Benutzer, der über das Netzwerk einsteigt 🡪 hat nur Leserechte  
wird automatisch zugewiesen

1. Mit welchem Typ wird ein Windows Verzeichnis gemountet?

Cifs 🡪 common internet file system

1. Unterschied beim mount-Befehl von nfs und samba?

**NFS:**

Entferntes Verzeichnis als Lokales darstellen

sudo mount Server:Freigabe lokalerPfad

**Samba:**

mount -t cifs [//gandalf.htl-villach.at/Public](file:///\\gandalf.htl-villach.at\Public) /mnt/gandalfp -o user=nnnnnnnv

wobei /mnt/gandalfp bereits bestehen muss (also evtl. vorher mit mkdir erzeugen)

1. writeable = yes und Zugriffsrecht ist 554. Was gilt? Wie ist die allgemeine Regelung in diesem Fall?

Writeable = yes 🡪 schreiben erlaubt (Gegenteil von Read only)  
user r-x (5), group r-x (5), other r-- (4)

Stärkere Einschränkung gilt

1. Wie erfolgt die Arbitrierung von CSMA/CR beim CAN Bus?

Jedes Steuergerät ist ein Master und alle Nachrichten haben eigenes Bitmuster für die Kennung. Je mehr 1en am Anfang stehen, desto höher ist die Priorität. Alle senden evtl gleichzeitig, schicken aber am Anfang ihre Kennung mit. Wenn eine 0 gesendet wird aber 1 am Bus liegt, hat ein Teilnehmer mit höherer Priorität gesendet und der Teilnehmer mit niedriger Priorität hört auf.

1. Wie funktioniert das Summentelegramm beim Interbus?

Alle für die Teilnehmer bestimmten Ausgangsdaten sind darin enthalten. Die für den Master bestimmten Daten werden an der entsprechenden Stelle durch den Slave in das Telegramm eingefügt.  
Kurz: Der Master sendet einen Datenrahmen, in den die Teilnehmer nacheinander reinschreiben.

1. Wie läuft ein Master-Slave Verfahren ab? Was ist in diesem Zusammenhang Token passing wie es beim Profibus verwendet wird?

Master verwaltet alles, Slaves dürfen nur auf Anfrage Informationen senden oder werden in regelmäßigen Abständen gefragt.

Wenn mehrere Master vorhanden sind wird die Sendeberechtigung mit Hilfe eines Telegrams (Tokens) weitergereicht.

1. Was ist polling?

Zyklische Abfrage einzelner Komponenten durch eine zentrale Komponente 🡪 Master-Slave Verfahren

1. Was bedeutet Echtzeitfähigkeit?

Unter Echtzeitfähigkeit versteht man, dass auf ein Ereignis innerhalb einer genau definierten maximalen Zeitspanne reagiert wird - diese Zeitspanne wird Latenzzeit genannt.

1. Welche Vorteile hat WLAN im 2.4 GHz gegenüber dem 5GHz Netz, welche Nachteile hat es?

Je höher die Frequenz, desto geringer ist die Reichweite (skin Effekt). Das 5 GHz-Band bietet höhere Bandbreiten, hat aber eine kürzere Reichweite im Vergleich zu einem 2,4-GHz-Band. Bei Radiofrequenzen gilt, je höher die Frequenz, desto kürzer ist seine Reichweite. Netze mit 5 GHz sind nicht so anfällig für Störungen. Gerade im privaten Gebrauch finden sich in der näheren Umgebung schnell zahlreiche weitere WLANs, die meist mit 2,4 GHz funken.

1. Was 802.11ac?

802.11 ac ist ein Standard für drahtlose Netzwerke.

1. Was bedeutet roaming und welche Rolle spielen dabei das beacon Intervall und DTIM?

Roaming bezeichnet die Fähigkeit eines Mobilefunknetz-Teilnehmer, in einem anderen Netzwerk als sein Heimnetzwerk Anrufe zu empfangen. Clients wechseln zum besten Access Point, wenn sie den Standort wechseln

Beacon Intervall: Zeit zwischen Signalen von AP, in dem die Verschlüsselungsmethode usw. steht, damit sich die Clients damit verbinden können. Bei viel Bewegung (z.B TdoT) geringes Intervall (verbraucht Bandbreite), bei wenig Bewegung größeres Intervall

DTIM: Informiert Clients, dass gebroadcastet wird. Wird im Beacon-Intervall mitgesendet  
Zusatzinformation, welche sagt dass ein Beacon-Intervall kommt 🡪 gewisse Geräte schlafen und reagieren nur auf DTIM 🡪 Energiesparmaßnahme  
je niedriger Beacon und DTIM desto schneller Verbinden weniger Bandbreite

Beides zum Verbinden

1. Wozu dienen base-rates?

Base-rates stellen die Geschwindigkeit ein mit wie viel kommuniziert werden kann.

1. Was ist eine LDAP- oder eine Radius Authentifizierung und wozu ist die gut?

Eine LDAP Authentifizierung ist eine Validierung des Usernames und Passworts mithilfe des Active Directory (Verzeichnisdienst) 🡪 stärker 🡪 kann mehr Informationen speichern

Radius Authentifizierung: weniger Informationen werden gespeichert = nur Username, PWD, eventuell Gruppe 🡪 kann mit AD synchronisiert sein 🡪 nur für Login

1. Für welche Komponenten steht LAMPP?

LAMPP steht für Linux Apache MYSQL PHP PERL

1. Wie erreiche ich unter Linux den sql-prompt?

In mysql einsteigen mit   
mysql –u root –p

1. Wie kann ich in mysql ein Reihe von sql-Statements ausführen, die in einer Datei gespeichert sind?

Man kommt zur mysql-Eingabeaufforderung, darin werden die die sql Befehle, die in erzeugedb.sql stehen, ausgeführt mit  
mysql>source erzeugedb.sql

1. Wie lautet die Syntax einer Schleife in der bash?

for (( i=1;i<=35;i++ ));

do

//code

done

1. Was ist die übliche Art der Datenbankverwaltung über eine GUI im LAMPP?

Phpmyadmin

1. Wie kann man am einfachsten https zur Verfügung stellen?

Empfehlung letsencrypt (tool) gibt’s für Linux (https, ftps, …) und Windows (zumindest den Webserver) 🡪 regelt alles für einen und erneuert auch die Zertifikate

Sonst sind die Zertifikate selbst signiert und werden evtl. nicht anerkannt bzw. erzeugen eine Warnung

1. Welche Schritte sind üblicherweise durchzuführen, um ein CMS zu einem anderen Provider zu transferieren?

Die Datenbank sichern: in phpmyadmin exportieren – damit wird eine sql Datei erzeugt die alle creates und inserts enthält, um die Datenbank mit den Tabellen neu zu erzeugen. Die sql Datei findet man üblicherweise im download Ordner

Beim neuen Provider die Datenbank (das sql File) importieren und die gesamte Ordnerstruktur kopieren.  
evtl Verweise auf die Datenbanknamen, log File Ordner, Datenbank Credentials,.. anpassen. Dafür gibt es configuration files, in denen die Infos mit einem einfachen Texteditor gändert werden können.

1. Was bedeutet die Notation MM1∞ ?

Exponentialverteilte Ankünfte und Bedienungen und einen unendlich großen Warteraum, in dem keine Kunden abgewiesen werden müssen

1. Wie erhält man aus gleichverteilten Zufallszahlen exponentiell verteilte Zufallszahlen?

Logarithmus von einer gleichverteilten Zufallszahl ist exponentiell verteilt d.h. man nimmt den Logarithmus einer gleichverteilten Zufallszahl um eine exponentiell Verteilte zu bekommen

1. Was bedeuten die Zeichen in folgenden Formeln?

🡪 warum nicht mü gesamt 🡪 kommen verschiedene Verweilzeiten raus und ist komplizierter

Zwischenankunftszeit (die Zeit, die zwischen der Ankunft von 2 Kunden vergeht)  
 Ankunftsrate = 1/Ta (die Anzahl der Kunden, die pro Zeit im System ankommen)  
*Ts* Bedienzeit (die Zeit, die benötigt wird, um einen Kunden zu bedienen)  
 Bedienrate (die Anzahl an Kunden, die pro Zeit bedient werden können)  
 Auslastung des System (muss < 1 damit die Warteschlange nicht unaufhörlich wächst)

= Gesamte Auslastung des Systems, wenn darin mehrere Warteschlangen mit unterschiedlichen Bedienraten bedient werden  
*Tv* Verweilzeit = Tw + Ts (Gesamtzeit, die der Kunde im System verbleibt)

Verweilzeit eines Kunden – dann ergeben sich evtl für jeden Kunden andere Tw

mittlere Wartezeit in der Schlange vor der Bedienung = ca der Mittelwert aller Tw, die man aus der Formel für Tv berechnet hat in dem man Tw=Tv-Ts verwendet

1. Wie hoch ist die Auslastung eines Servers, der 30 Anfragen pro Minute bekommt und für die Bearbeitung einer Anfrage 1 Sekunde benötigt?
2. Wie kann man eine einfache Warteschlange (MM1∞) simulieren? Was ist dabei zu beachten?

Statt die Formeln zu verwenden, wird meist eine Simulation ausgeführt, dh man läßt das Programm mit sleepd warten und simuliert so die Ankünfte und Bedienungen, aber eben viel schneller in der Realität, in dem man den Zeitfaktor ändert. zB statt 1 Minute eine Millisekunde verwendet.

Man benötigt Zahlen, die einer gewissen Verteilung entsprechen.

Problematisch ist dabei das Sleep, weil die Zeitmessung unter Linux und Windows recht ungenau wird, wenn man kleine Intervalle betrachtet, und bei größeren Werte im Sleep dauert die Simualation länger. Mit halbwegs guter Genauigkeit kann man höchstens 20 Kunden pro Sekunde simulieren

Threads oder Sequentiell mit Schleifen