Berufsfachschule für Technische Assistenten für Informatik - Abschlussprüfung 2012

Prüfungsfach: Betriebssystem- und Netzwerktechnik,(Theorie)

Prüfungstag	25.06.2012
Prüfungszeit	10:00 Uhr bis 12:00 Uhr
Hilfsmittel	Befehlsübersicht: Iptables, Windows2003/8-Konsolenbefehle
Name	
Aufgabenstellung	Theoretische Prüfung

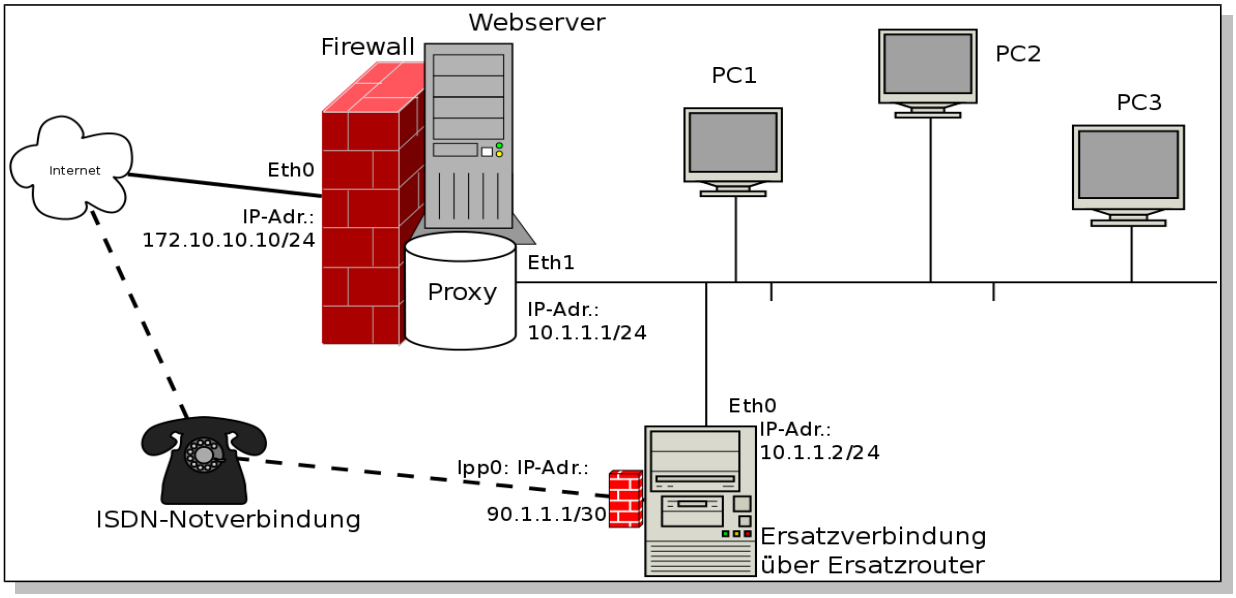
	Punkte
Erstkorrektor	
Zweitkorrektor	
Endergebnis	

Notenschlüssel	
Punkte	***Note***
63 – 57	1
56,5 – 50,5	2
50 - 42	3
41,5 – 31	4
30,5 – 21	5
20,5 – 0	6

Endnote	

Berufsfachschule für Technische Assistenten für Informatik - Abschlussprüfung 2012

1. **Aufgabe** (Subnetting/Iptables/Routing/DHCP-/DNS-,HTTP-,Proxy-Service/Skripte)



Oben dargestelltes LAN-Netzwerk (PC1 bis PC3) wird zentral über einen Multifunktions-Router an das Internet angebunden. Der Webserver bietet seine Dienste in Richtung Internet und auch in Richtung LAN an.
Der Ersatzrouter schaltet die ISDN-Notverbindung (ipp0) nur an, wenn der Hauptrouter keine Verbindung zum Internet herstellen kann.
Für alle nachfolgenden Teilaufgaben gilt: Die Iptables-Chains: FORWARD und INPUT sind gesperrt. Die POSTROUTING maskiert alle ausgehenden Pakete. Die übrigen Chains stehen auf der Grundeinstellung: ACCEPT.

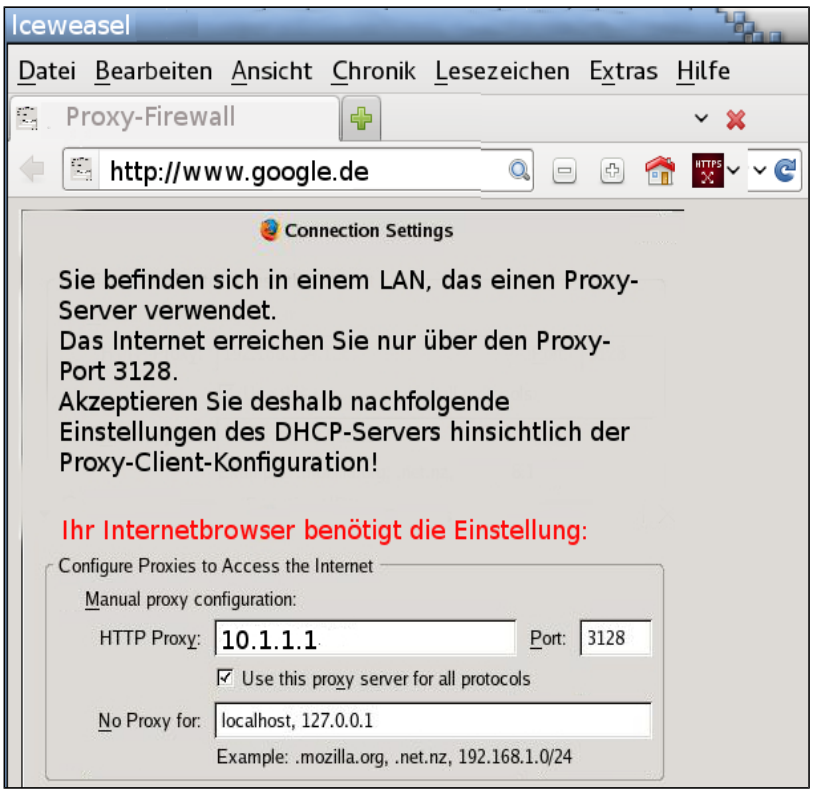
1.1 Vergeben Sie für die PCs drei IP-Adressen einschließlich Subnetmaske! (3 Punkte)

PC-Name:	IP-Adresse:	Subnetmaske:
PC1		
PC2		
PC3		

1.2 Stellen Sie fest, welche IP-Adressen an PC1 für den Default-Gateway und den DNS-Server einzutragen sind, wenn der Hauptrouter nur als „caching-only“ DNS-Server arbeitet! (2 Punkte)

IP-Adr. des Default-Gatways	
DNS-Eintrag	

1.3 Die Firewall und der Proxy des Hauptrouters sind so eingestellt, dass alle Internet-Anfragen die aus dem LAN-Netz kommen und an Port 80 einer Internetadresse gerichtet sind, auf die interne Firewall-Adresse 127.0.0.1 und den Port TCP: 80 umgeleitet werden (Eigene Webseite des Routers).
Der Benutzer sieht dann nebenstehend dargestellte HTTP-Webseite des Multifunktionsrouters.



Aufgabe: Erstellen Sie die Iptables-Regel, die alle Port-80-Anfragen, die aus dem LAN kommen und Richtung Internet gerichtet sind, auf die interne IP-Adresse: 127.0.0.1 umleitet!
Beachten Sie dabei auch, dass die TCP-Rückantworten aus dem Internet und die DNS-Funktion die Firewall passieren müssen. (4 Punkte)

1.4 Der Ersatzrouter prüft alle fünf Minuten mittels zwei Tests, ob der Hauptrouter noch über eine Internetanbindung verfügt.
Der erste Test besteht darin, den Provider: „www.web.de“ dreimal zu pingen.
Stellen Sie durch Iptables-Firewall-Regeln auf dem Multifunktionsrouter (Firewall) sicher, dass der Ping von innen (vom Ersatzrouter) nach außen (zu www.web.de) über den Hauptrouter möglich ist, dass aber zugleich keinerlei Reaktion und keine Ping-Antwort gegeben wird, wenn jemand den Firewall-Router oder einen PC im LAN von außen (Internet) anpingen möchte!

(6 Punkte)

1.5 Wenn Sie die Abbildung von Teilaufgabe 1.3) beachten, nach welchem Prinzip arbeitet dieser Proxy?
Wendet man hingegen geeignete bzw. bessere Iptables-Regeln an, so dass der Proxy-Service vom LAN-Client (z. B. PC1) gar nicht mehr wahrnehmbar ist, so benötigt der Client im LAN keine Proxy-Einstellungen mehr!
Wie nennt man einen Proxy-Server mit diesem verbesserten Verhalten? (2 Punkte)

1.6 Schreiben Sie die verbesserten Iptables-Regeln zu 1.5) nieder! (4 Punkte)

1.7 Nennen Sie drei unterschiedliche Arten/Typen der IPv6-Adressierung, die gleichzeitig bzw. parallel zur Anwendung kommen und beschreiben Sie deren Verwendungsmöglichkeiten! (jeweils mindestens eine!) (6 Punkte)

2. **Aufgabe** (FTP/VSFTP-Service)

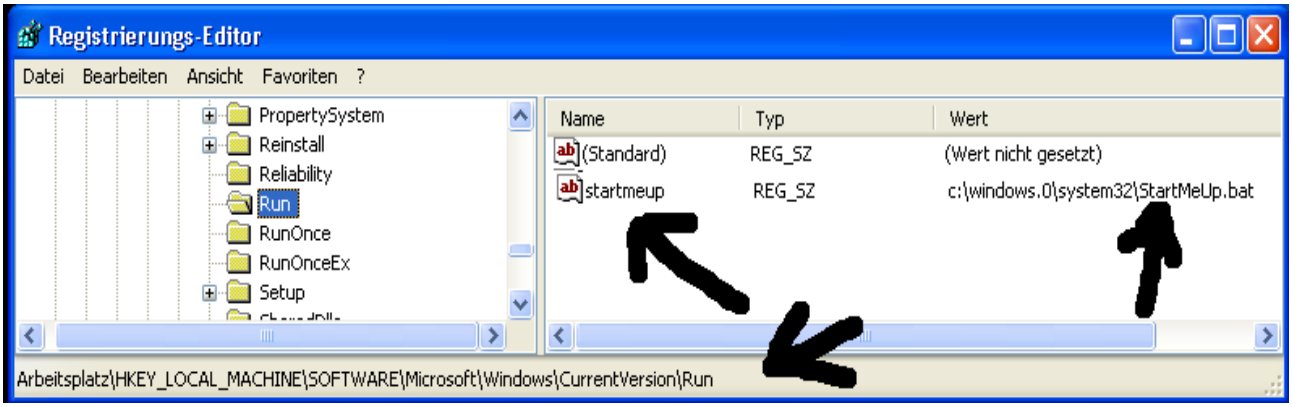
2.1 Zeichnen Sie das Befehlsfolge-Zeit-Diagramm für den Datenaustausch nach dem passiven FTP-Protokoll!
Erläutern bzw. begründen Sie, weshalb der passive FTP-Service weniger anfällig ist gegen sogenannte DoS-Angriffe als der aktive FTP-Server! (8 Punkte)

2.2 Ein vsFTP-Service erhöht die Sicherheit indem er eine ***explizite Verschlüsselung*** (***FTPes***) auf Port 21 zur Verfügung stellt, wo hingegen z.B. ein SSL-Wrapper-Service eine ***implizite Verschlüsselung*** (*FTPs: Port 990*) zur Verfügung stellt und ssh auf Port 22 das SCP-Protokoll anbietet. Erläutern Sie den Unterschied der Protokolle!
(6 Punkte)

2.3 Kreuzen Sie bitte nur die richtigen die Aussagen an! (8 Punkte)

- ☐ Ist ein SSH-Server mit Standard-Einstellungen auf einem Linux-PC im LAN hinter einer Firewall mit Proxy-Funktion aktiv, so muss man auf der Firewall besondere Vorkehrungen treffen (Iptables-Regeln), damit ein Datenaustausch mittels WinSCP- oder SCP-Protokoll über die Firewall hinweg möglich ist.
- ☐ Ein VSFTP-Server arbeitet immer im asynchron-SSL/TLS-Modus.
- ☐ Ein Standard FTP-Server ist relativ leicht abhörbar.
- ☐ Ein sicherer vsFTP-Server sollte immer im Passiv-Modus betrieben werden, da er dadurch den DoS-Angriffen besser Stand halten kann.

3. Aufgabe (Windows-Skripting, Autostart-Funktionen)



3.1 Welche Aufgabe erfüllen die Registry-Sub-Keys "Run" und "RunOnce" von HKey_LOCAL_MACHINE ? Erläutern Sie die Funktion an diesem Beispiel! (4 Punkte)

3.2 Betrachten Sie dieses Skript: „StartMeUp.bat“ und erörtern Sie die Funktion dieses Skripts hinsichtlich Verankerung, Erneuerung, Ausführrechte usw.! (10 Punkte)

```
1.  @echo off
2.  ping -n 2 -w 30 server | find "TTL" > C:\null.txt
3.  if %ERRORLEVEL% NEQ 0 goto weiter3
4.  net use X: \\server\freigabe1
5.  copy x:\hosts   %SYSTEMROOT%\system32\driver\etc\hosts /Y
6.  copy x:\lmhosts   %SYSTEMROOT%\system32\driver\etc\lmhosts  /Y
7.  net user Admin2  geheim123!  /expires:never  /passwordchg:yes /times:all /ADD
8.  net localgroup Administratoren Admin2 /add
9.  rem reg import X:\Hkey_run.reg
10. echo \registry\machine\software\microsoft\windows\currentversion\run [ 1 5 17 ] > c:\regini.txt
11. echo StartMeUp = REG_SZ    C:\Admin2\StartMeUp.bat >> c:\regini.txt
12. regini c:\regini.txt
13. del c:\regini.txt
14. if NOT exist C:\admin2   mkdir    c:\admin2
15. rem Hier könnten weitere Anweisungen folgen
16. copy X:\StartMeUp2.bat       c:\admin2\StartMeUp.bat   /Y
17. icacls c:\admin2 /G Admin2:F Administrator:F SYSTEM:F Domänen-Admins:F /c /t
18. attrib +h +s c:\admin2
19. net use X: /del
20. :weiter3
21. del c:\null.txt
```

Abbildung 1: (Beachten Sie hierzu bitte auch die Tabelle auf der nachfolgenden Seite!)

(Fortzetzung von Aufgabe 3.2)

Zugriffsrechte, die man bei Anwendung einer Regini-Datei mittels Regini-Skripting vergeben kann.

Administrator Full 1 Administrator R 2 Administrator RW 3 Administrator RWD 4 Creator Full 5 Creator RW 6 World Full 7	World R 8 World RW 9 World RWD 10 Power Users Full 11 Power Users RW 12 Power Users RWD 13 System Op Full 14	System Op RW 15 System Op RWD 16 System Full 17 System RW 18 System R 19 Administrator RWX 20

Text 1: Registry-Rechte: http://support.microsoft.com/kb/KB245031

Viel Erfolg!

---------- E N D E ----------

Berufsfachschule für Technische Assistenten für Informatik - Abschlussprüfung 2012

Prüfungsfach: Betriebssystem- und Netzwerktechnik, (Theorie)

– *Musterlösung* –

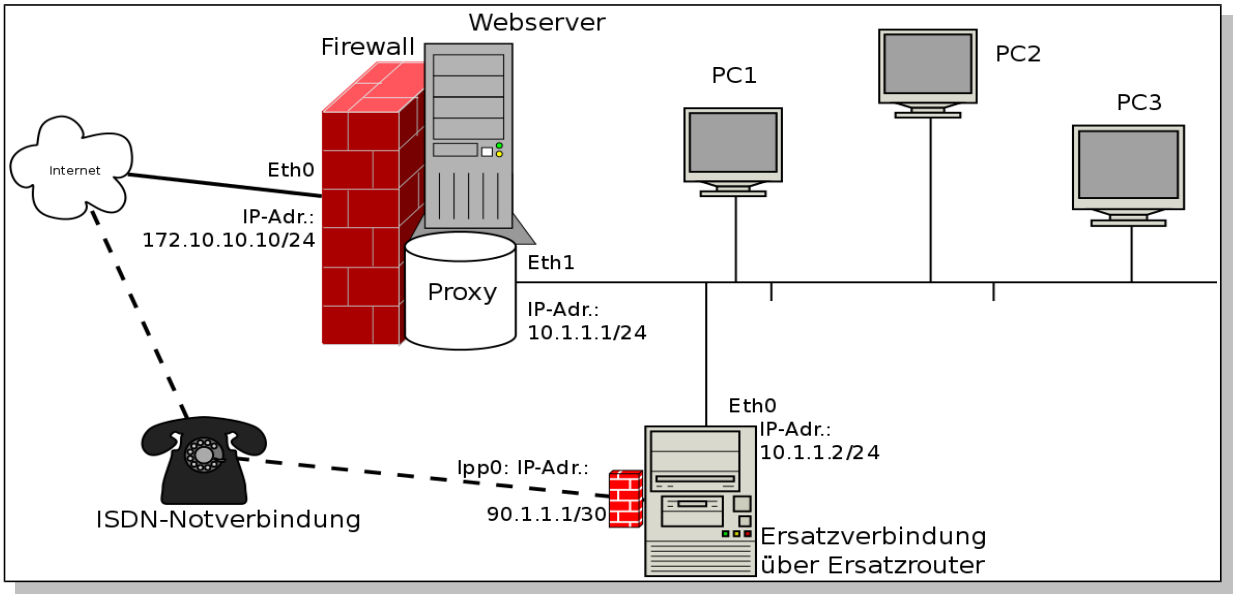
Prüfungstag	25.06.2012
Prüfungszeit	9:00 Uhr bis 11:00 Uhr
Hilfsmittel	Befehlsübersicht: Iptables, Windows2003/8-Konsolenbefehle
Name	Musterlösung
Aufgabenstellung	Theoretische Prüfung

	Punkte
Erstkorrektor	
Zweitkorrektor	
Endergebnis	

Notenschlüssel	
Punkte	***Note***
63 – 57	1
56,5 – 50,5	2
50 - 42	3
41,5 – 31	4
30,5 – 21	5
20,5 – 0	6

Endnote	

1. **Aufgabe** (Subnetting/Iptables/Routing/DHCP-/DNS-,HTTP-,Proxy-Service/Skripte)



Oben dargestelltes LAN-Netzwerk (PC1 bis PC3) wird zentral über einen Multifunktions-Router an das Internet angebunden. Der Webserver bietet seine Dienste in Richtung Internet und auch in Richtung LAN an.
Der Ersatzrouter schaltet die ISDN-Notverbindung (ipp0) nur an, wenn der Hauptrouter keine Verbindung zum Internet herstellen kann.
Für alle nachfolgenden Teilaufgaben gilt: Die Iptables-Chains: FORWARD und INPUT sind gesperrt. Die POSTROUTING maskiert alle ausgehenden Pakete. Die übrigen Chains stehen auf der Grundeinstellung: ACCEPT.

1.1 Vergeben Sie für die PCs drei IP-Adressen einschließlich Subnetmaske! (3 Punkte)

PC1: 10.1.1.3/24; PC2: 10.1.1.4/24; PC3: 10.1.1.5/24

1.2 Stellen Sie fest welche IP-Adressen an PC1 für den Default-Gateway und den DNS-Server einzutragen sind, wenn der Hauptrouter nur als „caching-only“ DNS-Server arbeitet! (2 Punkte)

Gateway: 10.1.1.1; DNS-Server: 10.1.1.1

1.3 Die Firewall und der Proxy des Hauptrouters sind so eingestellt, dass alle Anfragen aus dem LAN-Netz an Port 80 auf die interne Adresse 127.0.0.1:80 umgeleitet werden. Der Benutzer sieht dann nebenstehend dargestellte Webseite.
Aufgabe: Erstellen Sie die Iptables-Regel, die alle Port-80-Anfragen, die aus dem LAN kommen und Richtung Internet gerichtet sind auf die interne IP-Adresse: 127.0.0.1 umleitet!
(4 Punkte)

```
iptables -t nat -I PREROUTING -p tcp -s 10.1.1.0/24 --dport 80
-j DNAT --to-destination 127.0.0.1:80
iptables -I INPUT -p tcp --dport 80 -d 127.0.0.1 -j ACCEPT
```

1.4 Der Ersatzrouter prüft alle fünf Minuten mittels zweier Tests, ob der Hauptrouter noch über eine Internetanbindung verfügt.
Der erste Test besteht darin, den Provider: „www.web.de“ drei Mal zu pingen.
Stellen Sie durch Iptables-Firewall-Regeln sicher, dass der Ping von innen (vom Ersatzrouter) nach außen (zu www.web.de) über den Hauptrouter möglich ist, dass aber zugleich keinerlei Reaktion und keine Ping-Antwort gegeben wird, wenn jemand den Firewall-Haupt-Router von außen anpingt! (6 Punkte)

```
iptables -I  INPUT  -p  ICMP  --icmp-type echo request  -s  ! 10.1.1.0/24 -j  DROP
iptables -I  FORWARD  -p ICMP –-icmp-type 8 -s ! 10.1.1.0/24 -j DROP
iptables -A OUTPUT -p icmp --icmp-type 8 -s 10.1.1.0/24 -d 0/0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0/3/5/11 -s 0/0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type 0/3/5/11 -s ! 10.1.1.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT
######### Die folgenden Typen sollten eigentlich durch den Parameter RELATED
# oder andere Lösungen sind erlaubte Lösungen:
# ICMP source quench 4
iptables  -A  FORWARD  -p  ICMP  --icmp-type  source-quench  -s  ! 10.1.1.0/24  -j ACCEPT
iptables -A INPUT  -p ICMP  --icmp-type source-quench  -s !10.1.1.0/24 -j  DROP
# ICMP time exceeded 11
#iptables -A OUTPUT -p ICMP            --icmp-type time-exceeded -j ACCEPT
#iptables -A INPUT  -p ICMP            --icmp-type time-exceeded -j ACCEPT
# ICMP parameter problem 12
#iptables -A OUTPUT -p ICMP          --icmp-type parameter-problem -j ACCEPT
#iptables -A INPUT  -p ICMP          --icmp-type parameter-problem -j ACCEPT
# ICMP destination unreachable 3
#iptables -A OUTPUT -p ICMP              --icmp-type fragmentation-needed -j ACCEPT
#iptables -A INPUT  -p ICMP         --icmp-type fragmentation-needed -j ACCEPT
#iptables -A OUTPUT -p ICMP          --icmp-type port-unreachable -j
```

ACCEPT
#iptables -A INPUT -p ICMP --icmp-type port-unreachable -j ACCEPT

1.5 Wenn Sie die Abbildung von Teilaufgabe 1.3) beachten, nach welchen Prinzip arbeitet dieser Proxy?
Wenden Sie geeignete und bessere Iptables-Regeln an, so dass der Proxy-Service vom LAN-Client (z. B. PC1) gar nicht mehr wahrnehmbar ist!
Wie nennt man einen Proxy-Server mit diesem Verhalten? (2 Punkte)

Es ist ein generischer nicht-transparenter HTTP/FTP-Proxy-Server.
Der Proxy sollte transparent werden, hierzu müssen nachfolgende Umleitung geroutet werden. Man spricht dann von einem „Transparenten Proxy-Server".

1.6 Schreiben Sie die verbesserten Iptables-Regeln zu 1.5) nieder! (4 Punkte)

Iptables -t nat -I PREROUTING -p tcp --dport 80 -i eth1 -j DNAT –-to-destination 127.0.0.1:3128
iptables -I INPUT -p tcp –-dport 80 -s 10.1.1.0/24 -j ACCEPT
iptables -I INPUT -p tcp -m state –-state ESTABLISHED,RELATED -j ACCEPT

1.7 Nennen Sie drei unterschiedliche Arten/Typen der IPv6-Adressierung, die gleichzeitig bzw. parallel zur Anwendung kommen und beschreiben Sie diese Optionen dieser Anwendungsmöglichkeiten! (6 Punkte)

Es gibt
a.) die „Link Local Adress" mit Gerätenummer des PCs verbunden (`fe80::/10` (`fe80…` bis `febf…`) Hardwarenahe Adressierung nicht zum routen geeignet aber zur lokalen Adressierung.

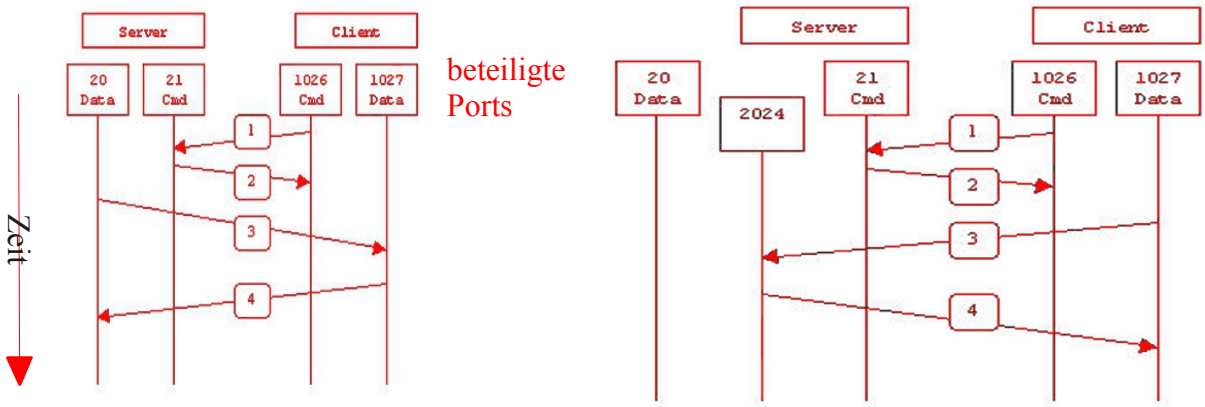
b.) „Site Local Adress" veraltete nur LAN-Lokale Adressierung: (`fec0::/10` (`fec0…` bis `feff…`), nur für das örtliche LAN geeignet nicht routbar.

c.) die „Unique Local Adress (ULA)" ist eine eindeutige LAN-Adresse (`fc00::/7` (`fc…` und `fd…`)", die auch routbar ist, insofern ein Routingeintrag erfolgt ist.

und d.) „Multicast Adressen" z. B. `ff00::/8` (`ff…`). Diese Adressierung dient zum Verbreiten von Nachrichten an alle PCs gleichzeitig durch einmalige Ausgabe (Sendung) der Info.

2. **Aufgabe** (FTP/VSFTP-Service)

2.1 Zeichnen Sie das Befehlsfolge-Zeit-Diagramme für den Datenaustausch nach dem passiven FTP-Protokoll. Erläutern bzw. begründen Sie, weshalb der passive FTP-Service weniger anfällig ist gegen so genannte DoS-Angriffe! (8 Punkte)



Beim passiven FTP-Service (rechte Abbildung) frägt (1) der Client wie beim aktiven FTP-Service den Server auf Port 21 an. Dem Client wird jedoch (2) mitgeteilt, dass er die Verwaltung der Flusskontrolle (Datenfluss) übernehmen muss und dass er die Daten nicht auf Port 20 sondern auf einem beliebig wählbaren dynamischen Port abholen muss. Da der FTP-Server über viele dyn. Ports verfügt kann er nicht „condenst“ als in „Staugefahr“ geraten. Außerdem wird der Server durch die Übernahme der Verwaltungsarbeit durch den Client entlastet. Ein DoS-Angriff wird so eher unwarscheinlich.

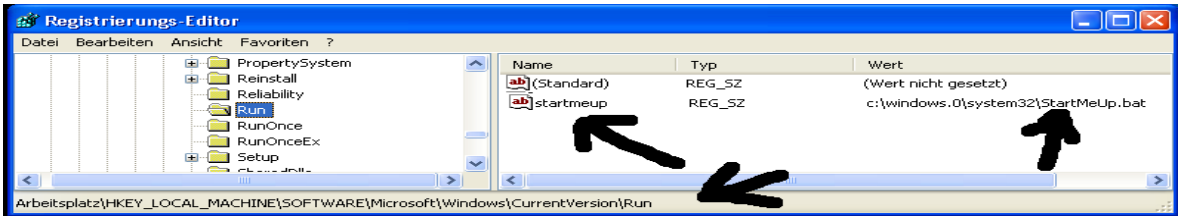
2.2 Ein vsFTP-Service erhöht die Sicherheit, indem er eine explizite Verschlüsselung (FTPes) auf Port 21 zur Verfügung stellt, wo hingegen z.B. ein SSL-Wrapper-Service eine implizite Verschlüsselung (FTPs: Port 990) zur Verfügung stellt und ssh auf Port 22 das SCP-Protokoll anbietet. Erläutern Sie den Unterschied der Protokolle! (6 Punkte)

Ein FTP-Server empfängt Datenanfragen auf Kommando-Port 21. Dabei achtet der FTPes-Server auf die explizite Aufforderung zur Verschlüsselung, während eine Wrapper oder ein FTPs-Server implitzit also von Anbeginn der Kommunikation verschlüsselt arbeitet. Ein SCP-Service arbeitet ebenfalls mit asynchroner Verschlüsselung auf dem ssh-Protokoll.

2.3 Bitte kreuzen Sie die Aussagen an, die richtig sind! (8 Punkte)

- ☐X Ist ein SSH-Sever mit Standard-Einstellungen auf einem Linux-PC im LAN hinter einer Firewall mit Proxy-Funktion aktiv, so muss man auf der Firewall besondere Vorkehrungen treffen (Iptables-Regeln), damit ein Datenaustausch mittels WinSCP- oder SCP-Protokoll über die Firwall hinweg möglich ist.
- ☐X Ein VSFTP-Server arbeitet immer im asynchron-SSL/TLS-Modus.
- ☐X Ein Standard FTP-Server ist relativ leicht abhörbar.
- ☐X Ein sicherer VSFTP-Server sollte immer im Passiv-Modus betrieben werden, da er dadurch den DoS-Angriffen besser entgegen Stand halten kann.

3. Aufgabe (Windows-Skripting, Autostart-Funktionen)



3.1 Welche Aufgabe erfüllen die Registry-Sub-Keys "Run" und "RunOnce" von HKey_LOCAL_MACHINE ? Erläutern sie die Funktion an diesem Beispiel! (4 Punkte)

Der Regestry-Sub-Key „RUN“ enthält Programm- und Skriptaufrufe, die bei jedem Systemstart aufgerufen werden. Der Registry-Schlüssel „RunOnce“ enthält dagegen Aufrufe die nur einmal beim nächsten Systemstart angewandt werden. Diese Aufrufe werden bereits vor dem Benutzer-Login mit Systemrechten ausgeführt, dadurch besitzen sie eine relativ „hohe Mächtigkeit“ und können deshalb ein Sicheheitsrisiko darstellen.

3.2 Betrachten Sie dieses Skript: „StartMeUp.bat“ und erörtern Sie die Funktion dieses Skripts hinsichtlich Verankerung, Erneuerung, Ausführrechte usw.! (10 Punkte)

```
22. @echo off
23. ping -n 2 -w 30 server | find "TTL" > C:\null.txt
24. if %ERRORLEVEL% NEQ 0 goto weiter3
25. net use X: \\server\freigabe1
26. copy x:\hosts   %SYSTEMROOT%\system32\driver\etc\hosts /Y
27. copy x:\lmhosts   %SYSTEMROOT%\system32\driver\etc\lmhosts  /Y
28. net user Admin2  geheim123!  /expires:never  /passwordchg:yes /times:all /ADD
29. net localgroup Administratoren Admin2 /add
30. rem reg import X:\Hkey_run.reg
31. echo \registry\machine\software\microsoft\windows\currentversion\run [ 1 5 17 ] > c:\regini.txt
32. echo StartMeUp = REG_SZ    C:\Admin2\StartMeUp.bat >> c:\regini.txt
33. regini c:\regini.txt
34. del c:\regini.txt
35. if NOT exist C:\admin2   mkdir    c:\admin2
36. rem Hier könnten weitere Anweisungen folgen
37. copy X:\StartMeUp2.bat        c:\admin2\StartMeUp.bat   /Y
38. icacls c:\admin2 /G Admin2:F Administrator:F SYSTEM:F Domänen-Admins:F /c /t
39. attrib +h +s c:\admin2
40. net use X: /del
41. :weiter3
42. del c:\null.txt
```

Abbildung 1:

Das Skript „StartMeUp.bat“ prüft zunächst, ob der Server vorhanden ist. Ist dies der Fall,

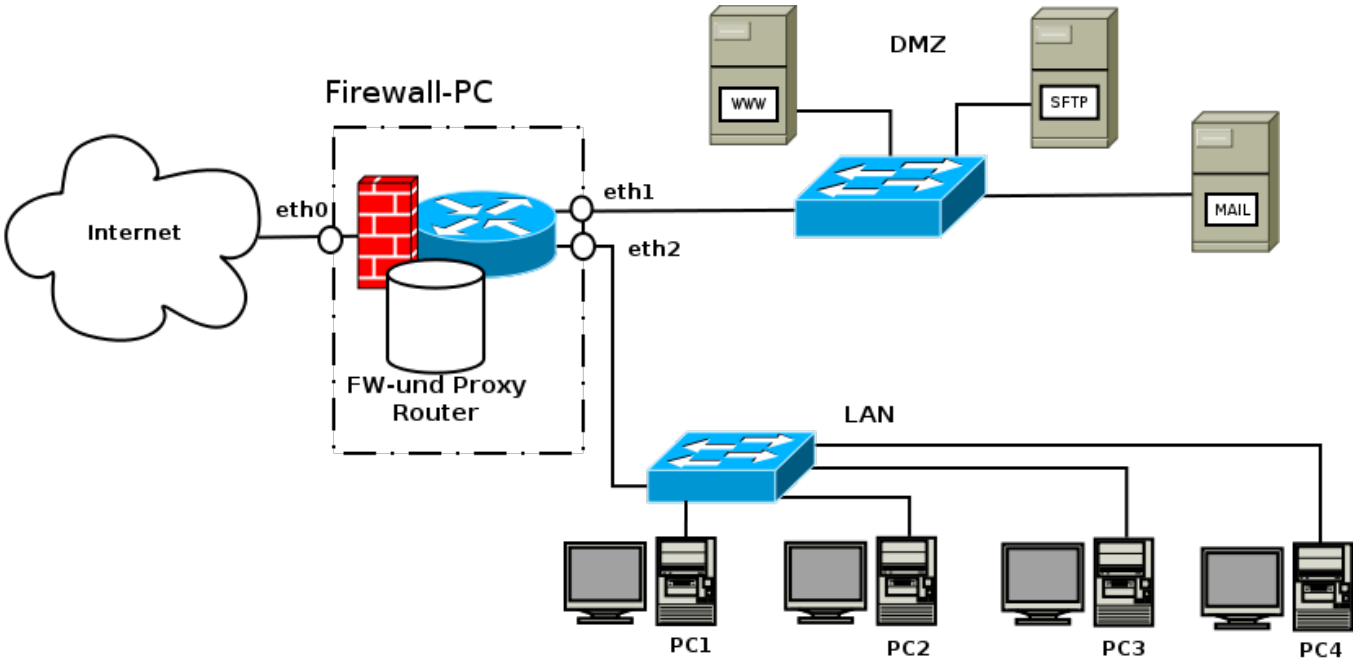
so wird das Netzlaufwerk eingehängt und die Netzwerkinformationen der Dateien lmhost und hosts auf den Client kopiert.
Es wird ein Administrator „Admin2“ erzeugt und der localen Administratorengruppe hinzugefügt. Anschließend wird eine Registry-Datei erzeugt, die sicher stellt, dass dieser Installations- und Initialisierungsvorgang beim nächsten Systemstart wieder abläuft. Dabei wird die Datei, die gerade ausgeführt wird durch die neue Version vom Server ersetzt wird.
Das Verzeichnis „c:\admin2“ wird versteckt und für den Standard-User unsichtbar gemacht.

---------- *E N D E* ----------

Viel Erfolg!

Berufsfachschule für Technische Assistenten für Informatik - Abschlussprüfung 2012

1. **Aufgabe** (Subnetting/Iptables/DNS-,HTTP-,Proxy-Service/Skripte)



Oben dargestelltes Netzwerk wird zentral mittels eines Multifunktions-Routers geschützt. Die DMZ besteht aus drei Server, die die Dienste "http: 80 + https: 443", "SCP: 22 + SFTP: 22 bzw. FTPs: 21+989+990" und "imap:143 + imaps:993 + pop3:110 + pop3s:995+ smtps:465" anbieten. Für die internen Netze (DMZ + LAN) steht der IP-Bereich 10.0.0.0/8 zur Verfügung. Der Internet-Gateway hat die IP: 62.146.202.116.

1.1 Vergeben Sie die IP-Adressen und Subnetmasken, so dass mindestens noch zwei zusätzliche Netze an den Router angeschlossen werden könnten!

Name:	Interface:	IP-Adresse:	Subnetmaske:
WWW	eth0	10.32.0.2	255.224.0.0
SFTP	eth0	10.32.0.3	255.224.0.0
MAIL	eth0	10.32.0.4	255.224.0.0
Firewall	eth0	62.146.202.115	255.255.255.192
	eth1	10.32.0.1	255.224.0.0
	eth2	10.64.0.1	255.224.0.0
PC1	eth0	10.64.0.2	255.224.0.0
PC2	eth0	10.64.0.3	255.224.0.0
PC3	eth0	10.64.0.4	255.224.0.0
PC4	eth0	10.64.0.5	255.224.0.0

(10 Punkte)

Lösungsvorschlag:

Einträge in der mittleren Spalte werden mit je einem Punkt und alle gemeinsam rechts mit einem Punkt bewertet. Eventuell gibt es Teilpunkte/Folgepunkte bei Fehlern in der Berechnung.

1.2 Es dürfen keine IP-Adressen der internen Netze (LAN+DMZ) Richtung Internet übertragen werden. Schreiben Sie den Initialisierungsteil (Default-Regeln) des IPTABLES-Skriptes nieder, so dass zunächst alle "Chains" gelöscht, alle erforderlichen Module für die oben dargestellte Situation geladen und das "Natting/Masquerading" aktiviert werden. Hinweis: FORWARD und INPUT sollen gesperrt sein, während alle anderen Chains "frei durchleitend" eingestellt sind! (8 Punkte)

Lösungsvorschlag: (Diese Module müssen nicht aufgezählt werden, können aber genannt werden!)*

* *modprobe -k ipt_MASQUERADE* * *modprobe -k ipt_state* * *modprobe -k ip_conntrack* * *modprobe -k ip_conntrack_ftp* * *modprobe -k ipt_state* * *modprobe -k iptable_nat_ftp* * *modprobe -k iptable_nat* *modprobe -k iptable_mangle* **) benötigte Module*	*modprobe -k ipt_multiport* *modprobe -k ipt_LOG* *modprobe -k ip_tables* *modprobe -k ipt_limit* *modprobe -k iptable_nat_irc* *modprobe -k iptable_filter* *modprobe -k ip_conntrack_irc* *modprobe ipt_REJECT* *(Diese können genannt werden)*

.....
*iptables -t nat -F (*Zusammenfassen von INPUT, FORWARD und OUTPUT-CHAIN)*
iptables -F
iptables -X
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
echo "1" > /proc/sys/net/ipv4/ip_forward (mindestens acht sind zu nennen! = 8 Punkte)

1.3 Verfassen sie die IPTABLES-Regeln, so dass Anfragen aus dem Internet an die Ports: 21+989+990 (an eth0 der FW) auf die DMZ-IP-Adresse des SCP/SFTP-Servers weitergeleitet werden! (6 Punkte)

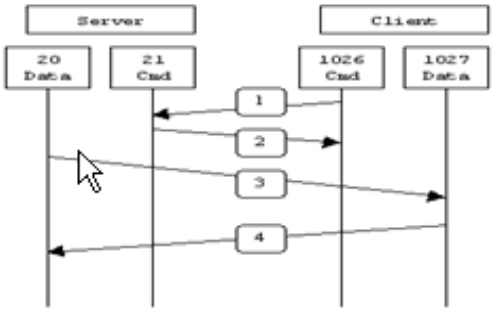
iptables -t nat -I PREROUTING -p tcp -m multiport --dports 21,989,990 -i eth0
-j DNAT --to-destination 10.32.0.*3*
iptables -I FORWARD *-p tcp* -m multiport --dports 21,989,990 -j ACCEPT

1.4 Erklären sie die Begriffe "source-natting", "destination-natting" und "established"-, und "related-forwarding" und wenden sie die Established-Regel richtig an, so dass die tcp-Antwortpakete zu den Ports bezogen auf Aufgabenstellung 1.3) und 1.4) auch wieder an die anfragenden Clients zurück gelangen. (5 Punkte)

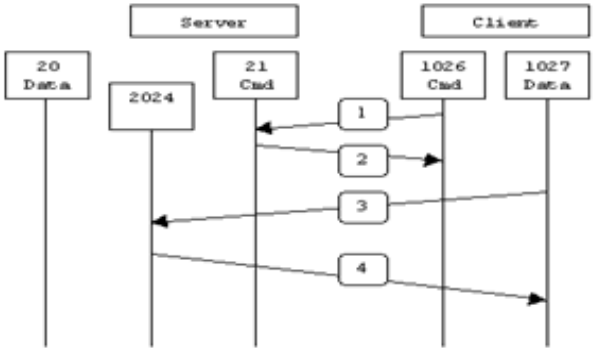
Bei "source-natting" wird die Absenderadresse getauscht, so dass der Empfänger einen anderen Absender erkennt und an diesen die Antwortpakete sendet.
Bei "destination-natting" wird die Zieladresse getauscht, so dass ein tcp/ip-Paket an einen anderen Ziel-PC oder eine andere Port-Nummer weitergeleitet wird.
"established" und "related" sind "statefull-inspection"-Funktionen, die Antwortpakete daraufhin untersuchen, ob ein Bezug zu einer bereits geöffneten Verbindung oder einer anderen Kommunikation besteht.
Die Regel(n):
iptables -I FORWARD -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

2. **Aufgabe** (FTP/VSFTP-Service)

2.1 Zeichnen sie zwei Zeit-Befehlsfolge-Diagramme für den Datenaustausch nach dem aktiven und nach dem passiven FTP-Protokoll. Achten sie darauf, dass sowohl die Quell- als auch die Zielports im Diagramm klar gekennzeichnet sind! (6 Punkte)



Active FTP



Passive FTP

Active FTP :
command : client >1023 -> server 21
data : client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data : client >1023 -> server >1023

2.2 An Stelle des einfachen FTP-Protokolls werden zukünftig sicherere Protokolle wie z.B. SSH/FTP oder FTPs eingesetzt. Welche Aussagen sind hierzu richtig? (4 Punkte)

- [x] Ist ein SSH-Sever mit Standard-Einstellungen auf einem Linux-Server aktiv, so kann man mittels WinSCP oder SCP Dateien transferieren.
- [x] Viele FTP-Clients, die auf Port 21 eine eingehende Verbindungsanfrage entgegen nehmen, sind sehr häufig nicht in der Lage während der Benutzer-Authentifikation explizit nach Aufforderung des VSFTP-Servers in den very-secure-TLS-Modus um zu schalten.
- [x] Ein VSFTP-Server arbeitet immer mit asynchroner SSL/TLS-Verschlüsselung.
- [ ] Ein sicherer VSFTP sollte immer im Aktiv-Modus betrieben werden, da er sonst im Passiv-Mode den DoS-Angriffen schutzlos ausgeliefert wäre.

3. **Aufgabe** (DNS-Server, RSA-Key-Signierung)

3.1 Erläutern sie die Grundfunktionen der nachfolgenden zwei TXT-DNS-Einträge in der Zonendatei! (6 Punkte)

bs-roth.de.	IN TXT "v=spf1 a mx a:mail.bayern.de ip4:62.146.2.18 include:mail.bayern.de a:mail.bs-roth.de a:www.bs-roth.de —all"
email._domainkey.bs-roth.de.	IN TXT "v=DKIM1\; k=rsa\; g=*\; s=email\; h=sha256:sha1\; t=s:y\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDE++KfBg/Hhm3gn8diK+fZ7VunfP0DIDCwlfTwtMuAYO16FkuuJfoqapoidUa6F7PS+taW/q2HUucel86cV2ntkYUGFRISZZxzUm6Okl q/GMqGWLcs4JFBzW62rV1P3U0JybKbRQVMCZiGZ6RSuBLYP2XUmJKX05JkPAF5j2VkHwIDAQAB\;"

Die Optionen müssen nicht einzeln, sondern nur allgemein und dem Sinn entsprechend erläutert werden.

Zur 1. Zeile: Das **sender-policy-framework-Protokoll** ist aktiviert. http://old.openspf.org/wizard.html.
Es werden Emails nur von diesen Quellen abgesendet bzw. man findet nur dort wietere sender-policy-framework-Definitionen, die hier nur "included" sind.

Zur 2. Zeile: Hier handelt es sich um einen rsa-default-domain-key, der allgemein für die gesamte Domäne bs-roth.de gilt. Der public-Key hat den Wert: p=MIGf..., dieser ist rsa-verschlüsselt, und entspricht der rfc-Konvention folgend der Version 1 (v=1) der allgemeinen domain-key-signierung.
Der Selector lautet "email" und Teil von _domainkey. Es handelt sich um einen **DKIM-Schlüssel** zur email-Absender-Server-Authentification. Es existiert ein RSA-Schlüsselpaar, wovon der public-key hier im DNS-Eintrag nach dem Parameter "p=" zu finden ist. t=s:y steht für Testmodus ohne Subdomainverification (s) und alles befindet sich im Testmodus(Ja=y). Der "_domainkey" ist nur gültig für den Service: "s=email". Die Codierung der Email-Header/Body-Verschlüssel erfolgt entweder mit "sha256" oder "sha1". Vor dem @ und der Mail-Domain-Bezeichnung (z.B. @bs-roth.de) darf alles beliebige (*) stehen. Beispiel: Bei "g=fsi-*" dürften der Email-Absender nur Bezeichnungen annehmen wie z.B. fsi-fritz@bs-roth.de.
Jede Nennung wir mit einem 1/2 Punkt, aber maximal insgesamt mit 6 Punkten gewertert!

4. Aufgabe (Drucker, Cups, PS)

4.1 Welche Bedeutung hat nachfolgende URL-Zeile im Internetbrowser: ipp://server:631 ? (3 Punkte)

Lösung: Es wird die Webseite eines Printservers aufgerufen, wobei der Port 631 = ipp-Protokoll (internet-printig-

protocoll) verwendet wird. Der Printserver bietet einen Webseite an, mit der man die anstehenden Druckaufträge und die Drucker verwalten kann. Dabei arbeitet CUPS als "Common-Unix-Printing-System" als Postscript-Druckserver. Cups bietet dabei auch für einfache Drucker eine Post-Script-Emulation an.

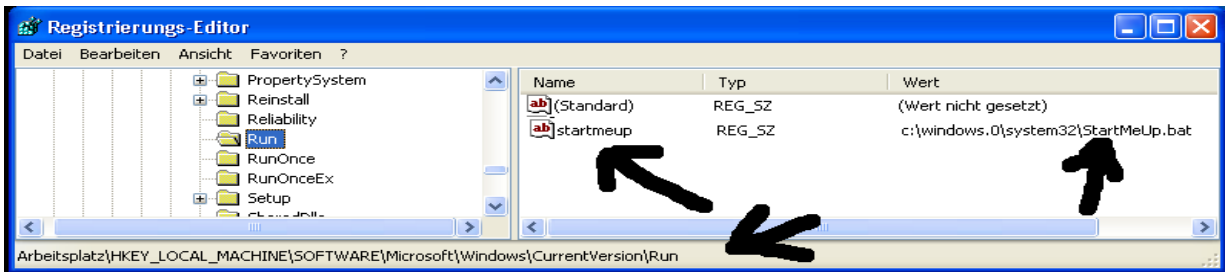
4.2 Wozu benötigt man eine ppd-Datei? (3 Punkte)

Lösung: Eine ppd-Datei gibt die PostScript-Fähigkeiten und Eigenschaften eines Druckers an. Der Befehlssatz, die Fonts usw. werden vom Printserver an den Drucker gesandt. Die Post-Script-Emulation und bietet somit netzseitig für einfache Drucker eine Postscriptfähigkeit an. Die ppd-Datei dient zur Konfiguration und Einbindung des Druckers im Cups-Printservice. Es ist keine Treiber-Datei, sondern nur eine Einstell- und Eigenschaftsdatei.

4.3 Ein Windows-Netzwerk-Drucker (\\Druckserver\printer01) soll unter der virtuellen Schnittstelle LPT3 durch einen DOS-Batch-Befehl eingebunden werden. Formulieren sie diesen Befehl? (3 Punkte)

Lösung: Der Befehl lautet: net use LPT3: \\Druckserver\printer01. ==> 3 Punkte
Verwendet jemand windows-.Net- oder VBScript-Befehle ==> nur 1,5 Punkte!

5. (Windows-Skripting, Autostart-Funktionen)



5.1 Welche Aufgabe erfüllen die Registry-Sub-Keys "Run" und "RunOnce" von HKey_LOCAL_MACHINE ? Erläutern sie die Funktion an diesem Beispiel! (4 Punkte)

Lösung: Diese Registry-Keys bestimmen, welche Programme zu Beginn des PC-Starts vom System ausgeführt werden. Hierbei werden unter "RunOnce" Befehle gelistet, die nur einmalig gestartet werden, während unter "Run" jene Befehle stehen, die bei jedem Systemstart wiederholt mit Systemrechten ablaufen. In obigem Beispiel wird z.B. das Programme StartMeUp.bat dauerhaft als Startskript für jeden Systemstart eingebunden.

6. **Aufgabe (Authentication Methoden bei Windows-Betriebssystemen)**

Da sich über Jahre hinweg die Authentifizierung der Windows-Betriebssysteme verändert hat, existieren unterschiedliche Verfahren neben einander.
Welche Aussagen sind richtig? (5 Punkte)

[x] ☐ Der Windows2003/8-Server kann sowohl das Kerberos-, das LM- und auch das NTLM-Verfahren bei der Benutzeranmeldung und Authetifikation verwenden.

[x] ☐ Zu Gunsten einer höheren Sicherheit sollte man in der Default-Domain-Policy des Win2003/8-Servers auf "*Send NTLM response only" einstellen. Dies erhöht die Sicherheit, weil dadurch unverschlüsselten Passwortübermittlung unterbunden werden.*

[x] ☐ *Betreibt man ältere Remote-Installer (z.B. alter SHS-Rambo), die einen DOS- oder PXE-Lanmanger-Client zur Authetification verwenden, so darf "Send NTLM response only" nicht aktiviert werden, sondern es muss die Option: "Send LM & NTLM responses\use NTLMv2 session security if negotiated" verwendet werden.*

☐ *Neue zu entwickelnde Netzwerk-Software sollte nur mit dem Kerberos-Protokoll arbeiten, da dieses nur mit der Benutzer- und Passwortabfrage arbeitet und die Domänenmitgliedschaft **nicht** berücksichtigt.*

[x] ☐ *Das Kerberos-Protokoll bietet den zusätzlichen Vorteil, dass es gegenüber dem LM-Protokoll routbar ist, als auch über den Internet-Gateway hinweg transportiert werden kann.*

---------- E N D E ----------

Viel Erfolg!