Berufsfachschule für Technische Assistenten für Informatik
Abschlussprüfung 2010

Prüfungsfach: Betriebssystem- und Netzwerktechnik,(Theorie)

Prüfungstag	28.06.2010
Prüfungszeit	8:15 Uhr bis 10:15 Uhr
Hilfsmittel	Befehlsübersicht: Iptables, Windows2003-Konsolenbefehle
Name	
Aufgabenstellung	Theoretische Prüfung

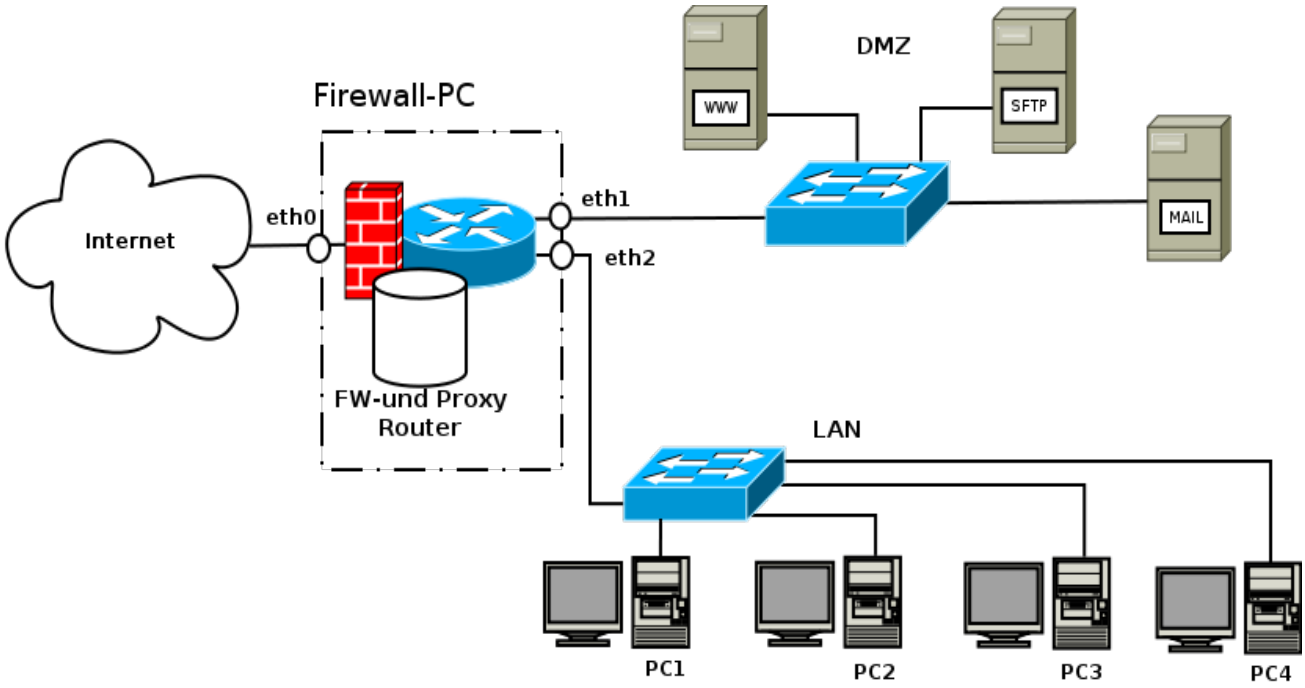
	Punkte
Erstkorrektor	
Zweitkorrektor	
Endergebnis	

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 2010

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 für die beiden internen Netze, die subnetierte IP-Adressen und Subnet-masken, so dass zu einem späteren Zeitpunkt mindestens noch zwei zusätzliche Netze an den Router anschließbar sind (vier Netze ohne Null- und Broadcastnetz)!

Name:	Interface:	IP-Adresse:	Subnetmaske:
WWW	eth0		
SFTP	eth0		
MAIL	eth0		
Firewall	eth0	62.146.202.115	255.255.255.192
	eth1		
	eth2		
PC1	eth0		
PC2	eth0		
PC3	eth0		
PC4	eth0		

(10 Punkte)

1.2 Es dürfen keine IP-Adressen der internen Netze (LAN+DMZ) Richtung Internet übertragen werden. Schreiben sie nur die "Default"- und "Masquerading/Natting"-Regeln des IPTABLES-Skriptes nieder, so dass zunächst alle "Chains" und auch die selbst definierten "Chains" gelöscht werden und das "Natting/Masquerading" Richtung extern aktiviert ist. Hinweis: FORWARD und INPUT sollen gesperrt sein, während alle anderen Chains "frei durchleitend" eingestellt sind! Sie müssen keine Iptables-Module nennen oder aufzählen!
(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)

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-Antwort-Pakete bezogen auf die Aufgabenstellung 1.3) auch wieder an die anfragenden Clients zurück gelangen! (5 Punkte)

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

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

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)

- Ist ein SSH-Sever mit Standard-Einstellungen auf einem Linux-Server aktiv, so kann man mittels WinSCP oder SCP Dateien transferieren.
- Viele veraltete 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.
- 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.

Berufsfachschule für Technische Assistenten für Informatik
Abschlussprüfung 2010

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+fZ7VunfP0DIDCwlfTwtMuAYO16FkuuJfoq apoidUa6F7PS+taW/q2HUucel86cV2ntkYUGFRISZZxzUm6Okl q/GMqGWLcs4JFBzW62rV1P3U0JybKbRQVMCZiGZ6RSuBLYP2 XUmJKX05JkPAF5j2VkHwIDAQAB\;"

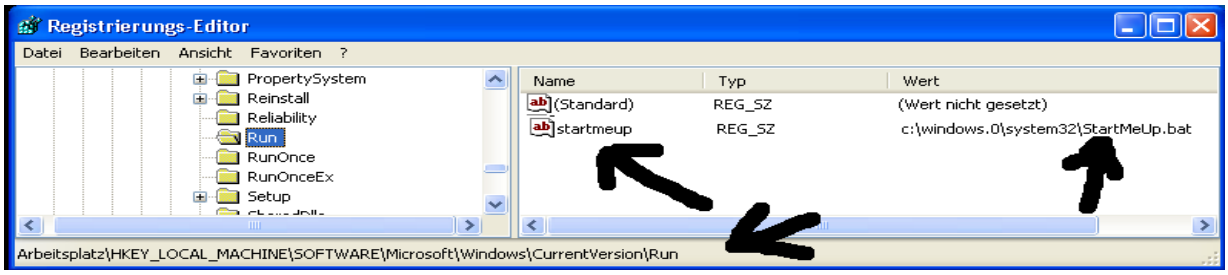
4. Aufgabe (Drucker, Cups, PS)

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

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

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)

5. Aufgabe (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)

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)

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

- 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.*

- *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.*

- *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!

Berufsfachschule für Technische Assistenten für Informatik
Abschlussprüfung 2010

Prüfungsfach: Betriebssystem- und Netzwerktechnik,(Theorie)

– Musterlösung –

Prüfungstag	28.06.2010
Prüfungszeit	8:15 Uhr bis 10:15 Uhr
Hilfsmittel	Befehlsübersicht: Iptables, Windows2003-Konsolenbefehle
Name	
Aufgabenstellung	Theoretische Prüfung

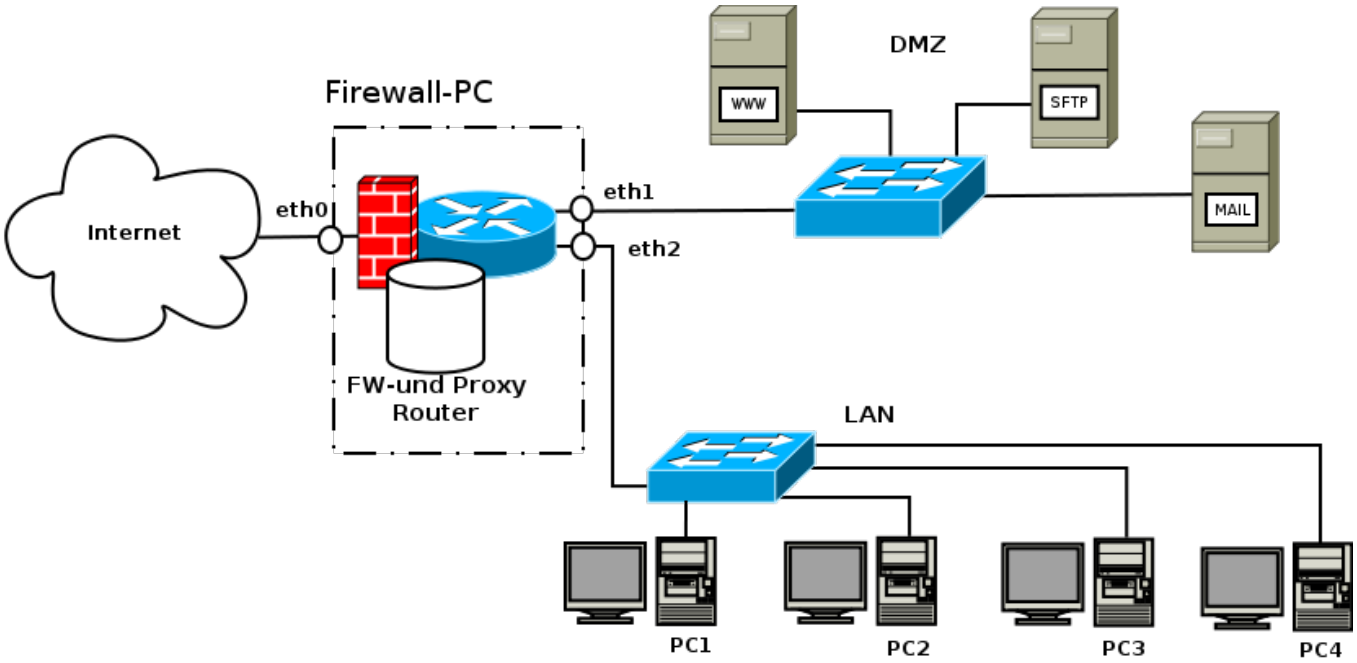
	Punkte
Erstkorrektor	
Zweitkorrektor	
Endergebnis	

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 2010

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
```

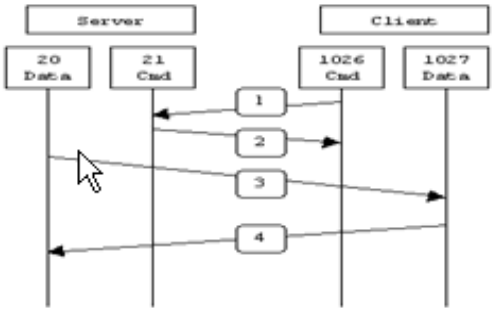
1.4 Erklären sie die Begriffe "source-natting", "destination-natting" und "established"-, und "related-forwarding" und wenden sie die Established-Regel richtig an, so dass die tcp-Antwortpakete zu den Ports bezogen auf Aufgabenstellung 1.3) und 1.4) auch wieder an die anfragenden Clients zurück gelangen.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

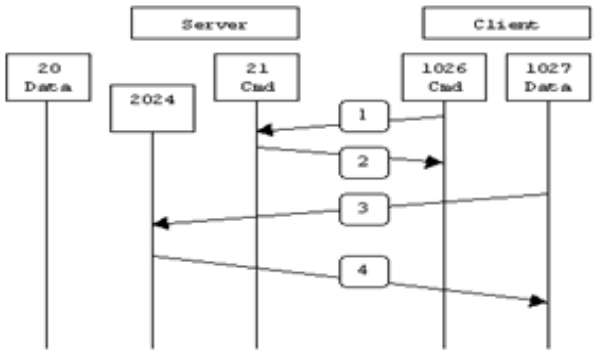
```
iptables -I FORWARD -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT
```

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 Verbindungs-anfrage 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 ausge-liefert 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/q2HUucel86cV2ntkYUGFRISZZxzUm6OkIq/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)

Berufsfachschule für Technische Assistenten für Informatik
Abschlussprüfung 2010

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.

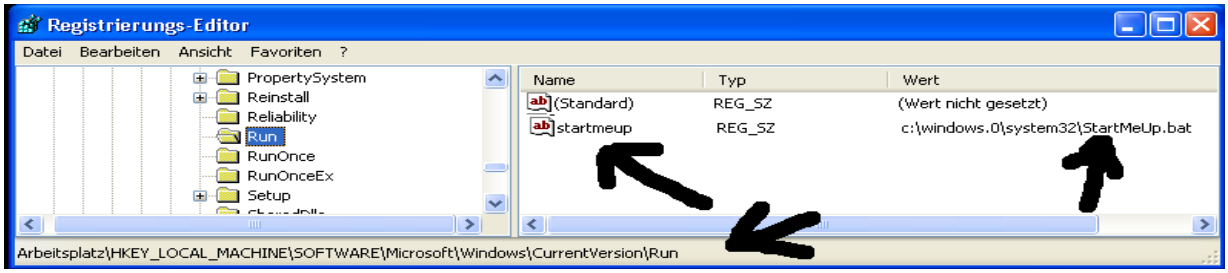
4.2 Wozu benötigt man eine ppd-Datei? (3 Punkte)

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

[x] î 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] î *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.*

[ ] î *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] î *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!