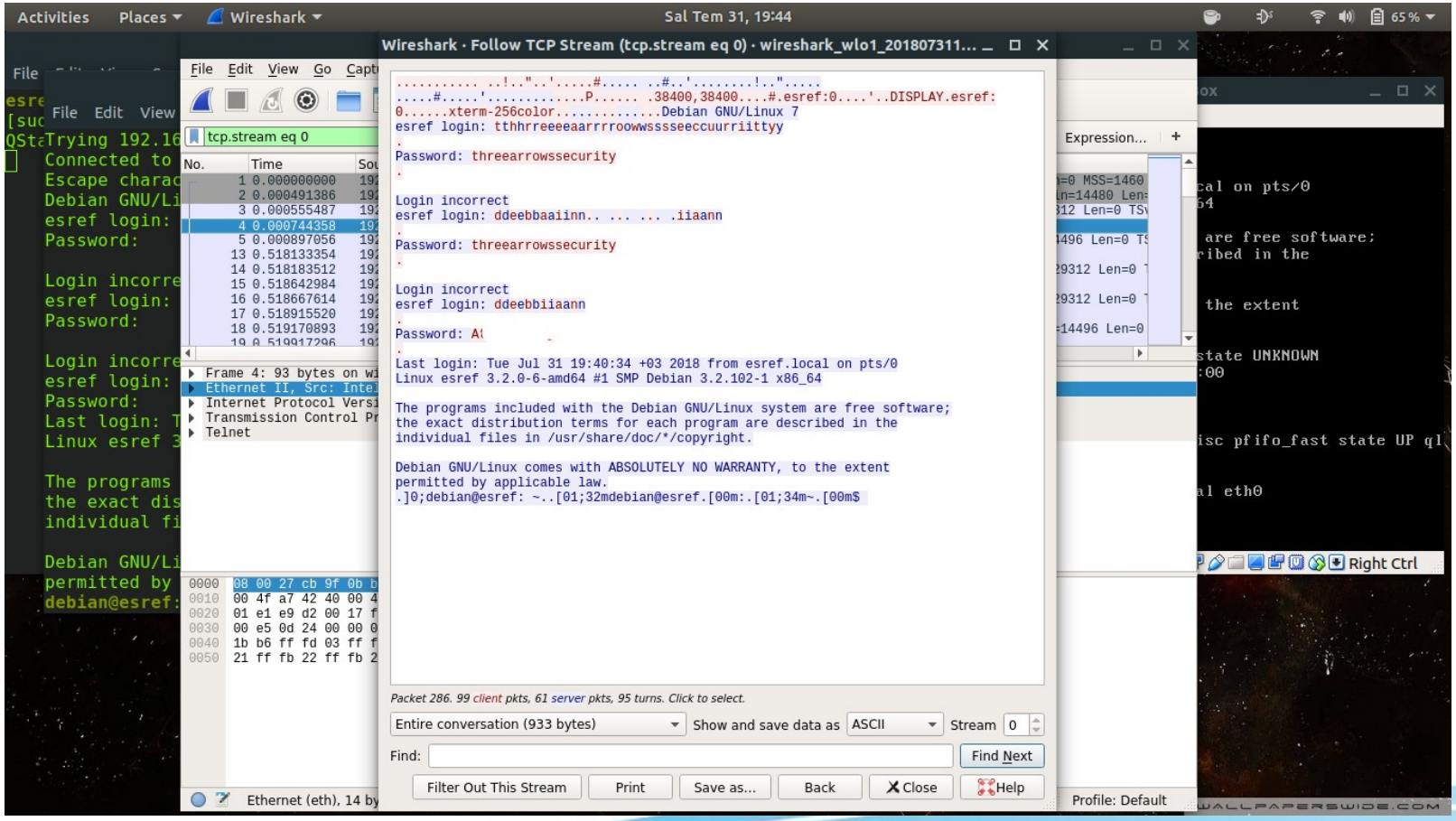
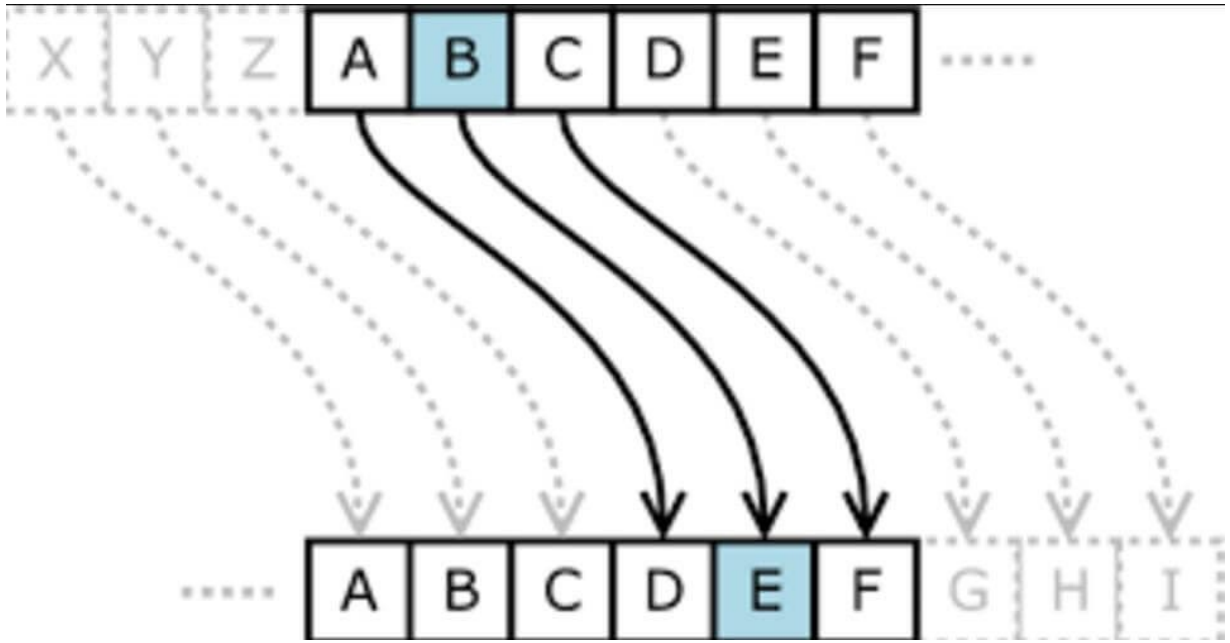
Linux Ağ ve Yönetimi

Linux Ağ ve Yönetimi



- Şifre ve şifreleme (Encription)
- Peki parola (Password)
- Anahtar (Key)
- Hash



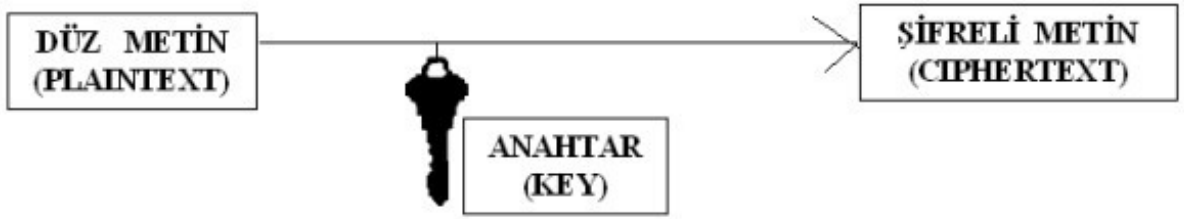
Anahtar kelime(Şifre): ANAHTARANAHTAR
Düz Metin : kekliklergeldi
Şifreli Metin : KRKSBKCEEGLEDZ

Parola : GuvenliParola2022
HASH : 6HnDHFdNpqsen8kD8$Zdcsb2DP0yjLl66xsIAMf jnXcyvFKAoQoJV3epRG6U81ktV5CFJofQdeMLSBhRiuyqh0yYVM.hQpwqZ413 pHh.

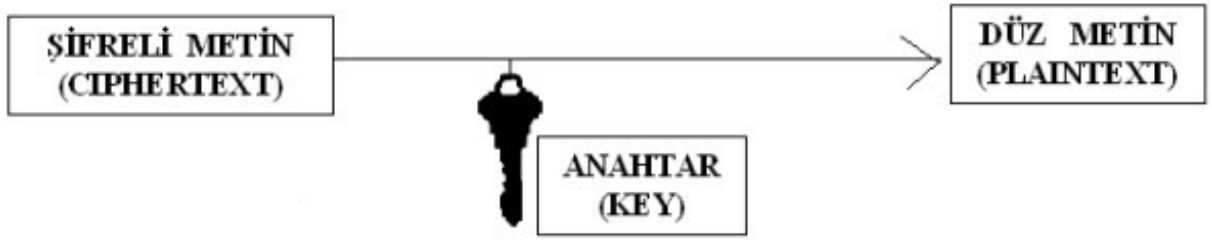
- Gizlilik (Confidentiality)
- Bilgi Bütünlüğü (Data Integrity)
- Kimlik Doğrulama (Authentication)
- Reddedilemezlik (Non-Repudiation)

Simetrik Şifreleme

Şekil-3 Simetrik Anahtarlı Şifreleme



Şekil-4 Simetrik Anahtarlı Şifre Çözme



Asimetrik Şifreleme

Şekil-6 Açık Anahtarlı Şifreleme

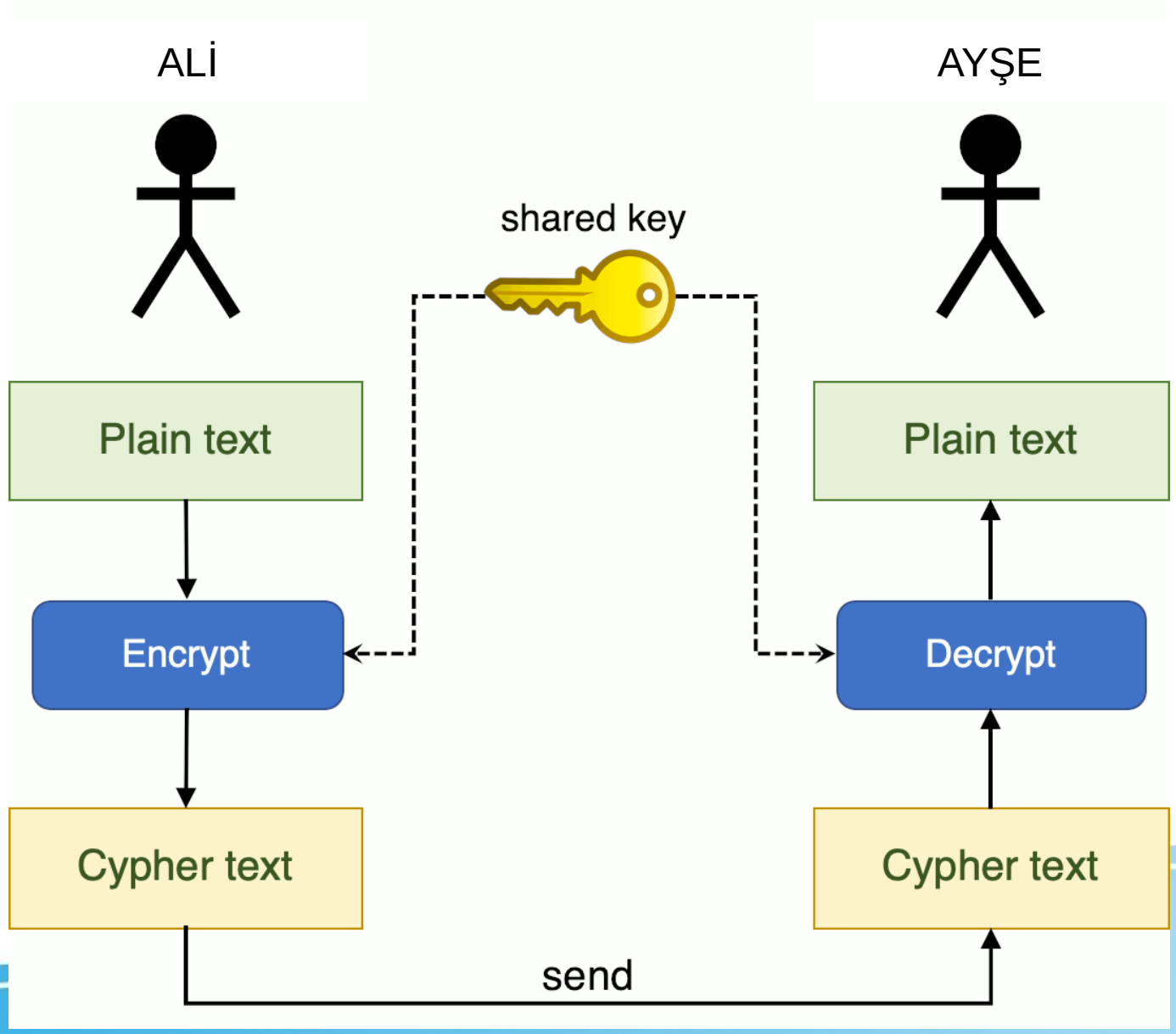
Şekil-7 Açık Anahtarlı Şifre Çözme

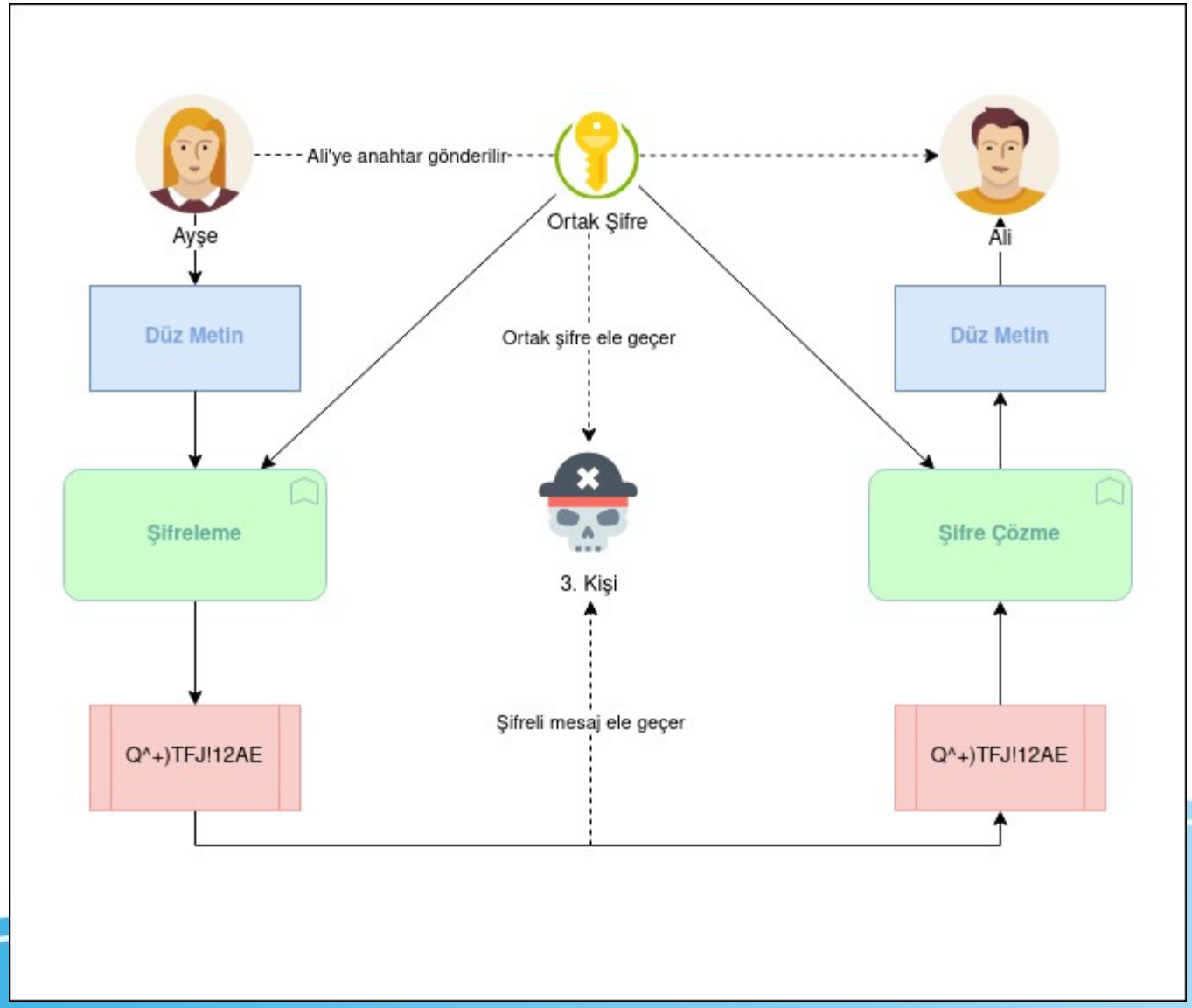
/etc/passwd

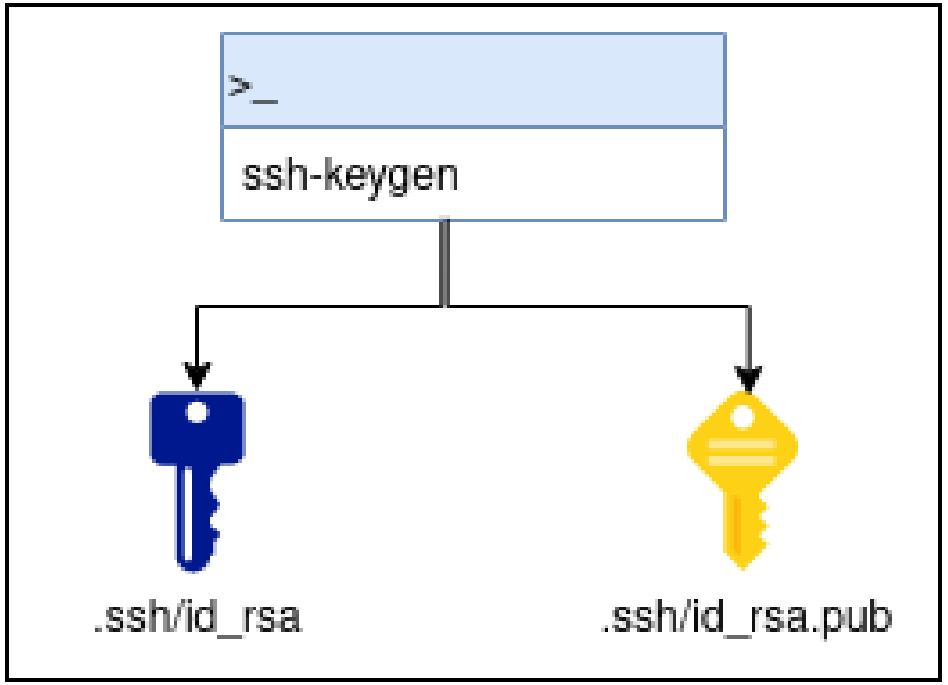
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
...
duygu:x:1000:1000:duygu,,,:/home/duygu:/bin/bash
sshd:x:123:65534::/var/run/sshd:/usr/sbin/nologin
```

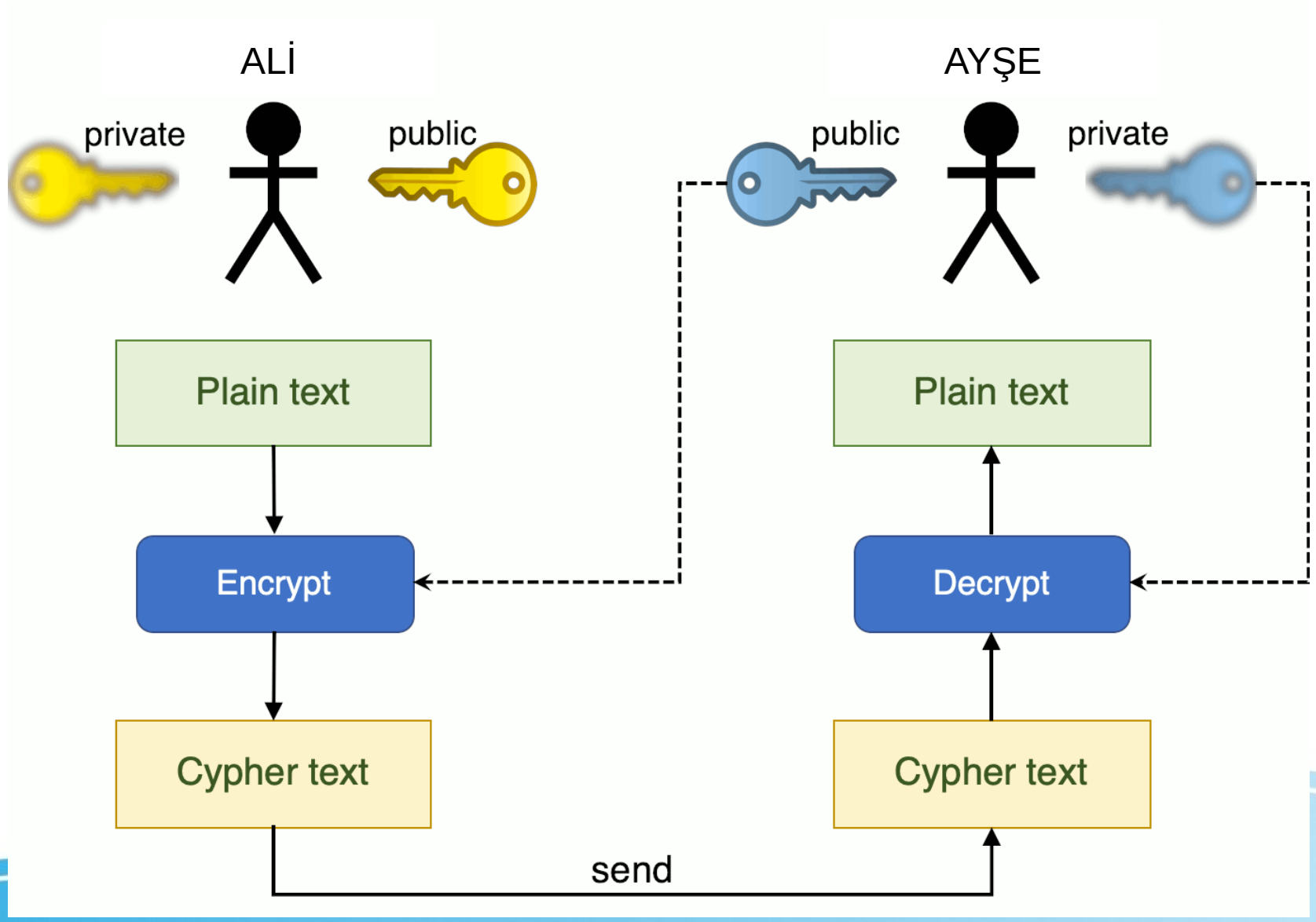
/etc/shadow

```
root:!:17733:0:99999:7:::
daemon:*:17494:0:99999:7:::
bin:*:17494:0:99999:7:::
sys:*:17494:0:99999:7:::
sync:*:17494:0:99999:7:::
...
Duygu:$6$uez6ZjeR$aoFYcVilpLMM5pCOT10qgfPtf9T5u1..oVdau3lvzvYTnc6FvF/KgAB
iGlMRfipf9Zg7z.HocwlAZTbGnfsKS.:17733:0:99999:7:::
sshd:*:17733:0:99999:7:::
```

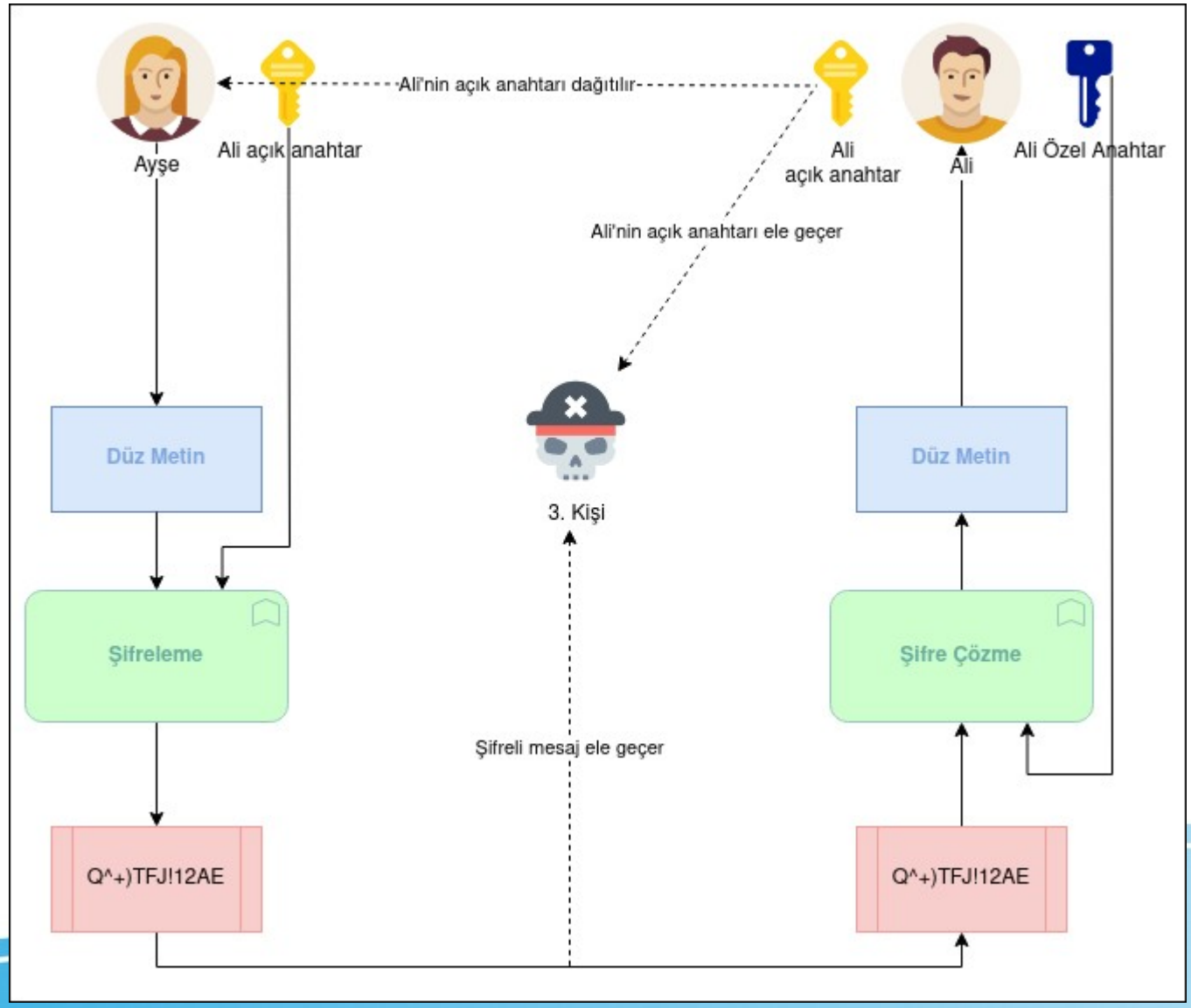

ALİ
AYŞE
shared key
Plain text
Encrypt
Cypher text
Plain text
Decrypt
Cypher text
send


Ali'ye anahtar gönderilir
Ayşe
Ortak Şifre
Ali
Düz Metin
Ortak şifre ele geçer
Düz Metin
Şifreleme
3. Kişi
Şifre Çözme
Şifreli mesaj ele geçer
Q^+)TFJ!12AE
Q^+)TFJ!12AE




ALİ
AYŞE
private
public
public
private
Plain text
Plain text
Encrypt
Decrypt
Cypher text
Cypher text
send

Linux Ağ ve Yönetimi




Bağlanma isteği
Makine + Sunucu Anahtarları
Şifrelenmiş Oturum Anahtarı
Onay
İstemci
Sunucu

Port Değiştirme
Port 22

Root Girişi
root hiçbir şekilde ssh ile bağlanamaz
PermitRootLogin no

root dosyada tanımlanan yöntemlerle bağlanabilir
PermitRootLogin yes

root şifre kullanarak bağlanamaz, anahtar gerekir
PermitRootLogin without-password

StrictModes
StrictModes yes

X11 Forwarding
X11Forwarding yes

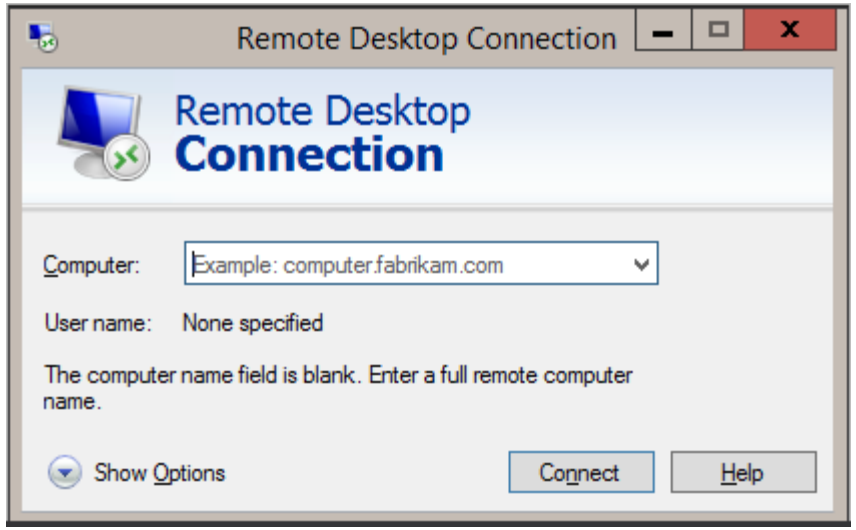
```
Host sunucu
    HostName 192.168.5.106
    User sysadmin
    ForwardX11 yes
    Port 5555

Host centos
    HostName 192.168.5.66
    User root
```

```
duygu@azaelia:~$ ssh-keyscan -t rsa -H 192.168.5.106
# 192.168.5.106:22 SSH-2.0-OpenSSH_8.4p1 Debian-5
|1|3GGh5h1jIH7bFrPU8PhW8ADHu44=|AHUWwKLrUluBVx4dUIEHjDiu5/Q= ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCiTZT3lheCcMQMekRRQ9XkXlgkZ7aKQ
k7zKMDYTjN5FUOOZHOWf9v1XlzQ65lY8cnGkVATMFNHCdAvG8p8LPBw+o7+N4y
OVqJKm/YlYMput0LJkLyiUZUHiZ5Pg8pEIMRDUXJ56wyxyS97XhFL/
xeW8zI73B+lXyNqcqjt11nt5Jd1yNHsQNX+rgCrEpePS5jF7OiH/
3c0vxtuig6/330tA8VRi53UMU1WrQacgzFO9A4LHYbPjVYG8A17PdY45Omj7A/
875e9aduT2QsflSlhAd7JpgMWvBND+2TQsrc34xPY78KK8h0csC+p6YVnRzNBI+4Pi
h8KvVDyksuDlksHiTcVC2guGNJQGHstoE5yAlaqQKf/V4CxQnHPvklxGVvpD/
QONb/
R4AvlOIDwIIdqjRjLf9N7WHBVkbyMjXNOcIPrXuI5ILOYxjU1LRGL+RwaLa5gkeQ98g
VVmvNH2ypwvusXeGGmt3hgTHCFSLi+tjpu8Iz3J+JhXWz1UAfPVd8=
```

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDtAx1fC1IVo2L+JN6hpFGyUvADx9WuE
C05Ie0XOCu8oOuSBXVVSut9i0p3odfnOkedx49UkDlwkWP9U2llW8xgCwChT/
6351bm/
rrZ4YQnKDbY06+Yge4MChK+c5+gDgeSD50u4tbcWM98GVosAoVEhSQMmteaFPE
9Wb2fxvGJHO5oUoZEFzZzSqr3BUmyrOrhk9q8Z6/2xPhX2lzBagmq6EQ8annzQj5lB
vkmJXGV4uMQwEPtUNPWh5R4UBpwMMCAoJTcVj5k9eVa34xIScfAhlvSTFgNFgBr
eF90mqP2V9BBhTRs3MZ1IWyXHi//
LgSPCorL7id0Dw8c+cDIgO95pM0DnDvnX65AT17mgXJcX4IM1ZkVn27iY6dlP5E8E
PeTwiM39ea+e+0Kbm08C3Y3/2VUTtVOY1483LH8NCrw/
PehZcrzAP06VFVubQkhx8jyZrLLcfY9uPoAgKC25CiGAOqAelB0gFsfOQQMyl8bLW/
owqC0p4OzAoOY9rwpZus= **duygu@azaelia**

Linux Ağ ve Yönetimi



Ağ İnceleme

Ana Problemler

- DNS sorunları
- Güvenlik duvarı sorunları
- Yanlış ağ yapılandırması
  - Gateway
  - Netmask / CIDR
- Erişim dosyaları

Linux Networking – Configuration

```
deneme6@azaelia:~$ ping google.com
PING google.com (216.58.206.174) 56(84) bytes of data.
64 bytes from sof02s27-in-f14.1e100.net (216.58.206.174): icmp_seq=1 ttl=117 time=50.1 ms
64 bytes from sof02s27-in-f14.1e100.net (216.58.206.174): icmp_seq=2 ttl=117 time=49.5 ms
^C64 bytes from 216.58.206.174: icmp_seq=3 ttl=117 time=50.1 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 49.505/49.895/50.124/0.277 ms
```

Linux Networking – Configuration

```
deneme6@azaelia:~$ host google.com
google.com has address 216.58.206.174
google.com has IPv6 address 2a00:1450:4017:806::200e
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.

deneme6@azaelia:~$ host -t mx google.com
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.

deneme6@azaelia:~$ host 208.67.222.220
220.222.67.208.in-addr.arpa domain name pointer resolver3.opendns.com.
```

Linux Networking – Configuration

```
deneme6@azaelia:~$ nslookup google.com
Server:         208.67.222.222
Address:        208.67.222.222#53

Non-authoritative answer:
Name:google.com
Address: 216.58.206.174
Name:google.com
Address: 2a00:1450:4017:806::200e


deneme6@azaelia:~$ nslookup google.com 208.67.222.220
Server:         208.67.222.220
Address:        208.67.222.220#53

Non-authoritative answer:
Name:google.com
Address: 216.58.206.174
Name:google.com
Address: 2a00:1450:4017:806::200e

nslookup -type=mx google.com 208.67.222.220
Server:         208.67.222.220
Address:        208.67.222.220#53

Non-authoritative answer:
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.

Authoritative answers can be found from:
```

Linux Networking – Configuration

```
deneme6@azaelia:~$ dig google.com

; <<>> DiG 9.16.15-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16617
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             300     IN      A       216.58.206.174

;; Query time: 60 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Tue Mar 22 04:07:21 +03 2022
;; MSG SIZE  rcvd: 55

deneme6@azaelia:~$ dig google.com MX +short
10 aspmx.l.google.com.
20 alt1.aspmx.l.google.com.
30 alt2.aspmx.l.google.com.
40 alt3.aspmx.l.google.com.
50 alt4.aspmx.l.google.com.
```

Linux Networking – Configuration

```
[root@smbdc02 sysadmin]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-03-22 04:14:08 +03; 1s ago
     Docs: man:firewalld(1)
 Main PID: 1676 (firewalld)
    Tasks: 2 (limit: 23676)
   Memory: 29.7M
   CGroup: /system.slice/firewalld.service
           └─1676 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Mar 22 04:14:07 smbdc02.mgrtson.lab systemd[1]: Starting firewalld - dynamic firewall daemon...
Mar 22 04:14:08 smbdc02.mgrtson.lab systemd[1]: Started firewalld - dynamic firewall daemon.
```

[root@smbdc02 sysadmin]# systemctl stop firewalld

Linux Networking – Configuration

```
root@azaelia:/home/sysadmin# systemctl status ufw
● ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
     Active: active (exited) since Tue 2022-03-22 04:18:46 +03; 1s ago
       Docs: man:ufw(8)
    Process: 3273 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
   Main PID: 3273 (code=exited, status=0/SUCCESS)
        CPU: 1ms

Mar 22 04:18:46 azaelia systemd[1]: Starting Uncomplicated firewall...
Mar 22 04:18:46 azaelia systemd[1]: Finished Uncomplicated firewall.
```

root@azaelia:/home/sysadmin# systemctl stop ufw

Linux Networking – Configuration

```
[root@smbdc02 sysadmin]# rpm -qi iptables-services
Name        : iptables-services
Version     : 1.8.4
Release     : 20.el8
Architecture: x86_64
Install Date: Tue Mar 22 04:21:26 2022
Group       : System Environment/Base
Size        : 20214
License     : GPLv2 and Artistic 2.0 and ISC
Signature   : RSA/SHA256, Wed Aug 25 17:25:24 2021, Key ID 05b555b38483c65d
Source RPM  : iptables-1.8.4-20.el8.src.rpm
Build Date  : Wed Aug 25 02:13:58 2021
Build Host  : x86-02.mbox.centos.org
Relocations : (not relocatable)
Packager    : CentOS Buildsys <bugs@centos.org>
Vendor      : CentOS
URL         : http://www.netfilter.org/projects/iptables
Summary     : iptables and ip6tables services for iptables
Description :
iptables services for IPv4 and IPv6
```

```
[root@smbdc02 sysadmin]# systemctl status iptables
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: active (exited) since Tue 2022-03-22 04:22:14 +03; 674ms ago
  Process: 43100 ExecStart=/usr/libexec/iptables/iptables.init start (code=exited, status=0/SUCCESS)
 Main PID: 43100 (code=exited, status=0/SUCCESS)

Mar 22 04:22:14 smbdc02.mgrtson.lab systemd[1]: Starting IPv4 firewall with iptables...
Mar 22 04:22:14 smbdc02.mgrtson.lab iptables.init[43100]: iptables: Applying firewall rules: [  OK  ]
Mar 22 04:22:14 smbdc02.mgrtson.lab systemd[1]: Started IPv4 firewall with iptables.
```

[root@smbdc02 sysadmin]# systemctl stop iptables

Yanlış Network Yapılandırma

- Yanlış Netmask ve CIDR

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:22:de:8e brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.106/32 brd 192.168.5.106 scope global enp0s3
       valid_lft forever preferred_lft forever
```

```
root@liman21:/home/sysadmin# ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=0.367 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=64 time=0.423 ms
^C
--- 192.168.5.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.367/0.395/0.423/0.028 ms
```

```
duygu@azaelia:/opt/ansible-mico$ ssh sysadmin@192.168.5.106
```

Yanlış Network Yapılandırma

- Yanlış Gateway

```
duygu@azaelia:/opt/ansible-mico$ ssh sysadmin@192.168.5.106
Linux liman21 5.10.0-8-amd64 x86_64

The programs included with the Pardus GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Pardus GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar 22 04:31:09 2022
sysadmin@liman21:~$
```

```
root@liman21:/home/sysadmin# apt update
0% [Working]
```

```
root@liman21:/home/sysadmin# ping google.com
```

```
root@liman21:/home/sysadmin# telnet 8.8.8.8 53
Trying 8.8.8.8...
```

```
root@liman21:/home/sysadmin# ip route
default via 192.168.5.5 dev enp0s3 onlink
192.168.5.0/24 dev enp0s3 proto kernel scope link src 192.168.5.106
```

/etc/hosts.deny ve /etc/hosts.access

```
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the
system.
#                See the manual pages hosts_access(5) and
hosts_options(5).
#
# Example:    ALL: some.host.name, .some.domain
#             ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "rpcbind" for
the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further
information.
#
# The PARANOID wildcard matches any host whose name does not
match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
ALL: 192.168.5.5
```

man 5 hosts_access

Detaylı Hata Ayıklama

Daha detaylı, mevcut ağ ayarlarını görmek istenirse /proc dizininden faydalanılabilir.

Örneğin, Mevcut arp tablosu için

root@liman21:/home/sysadmin# cat /proc/net/arp

IP address	HW type	Flags	HW address	Mask	Device
192.168.5.5	0x1	0x2	e0:d5:5e:80:13:96	*	enp0s3
192.168.5.1	0x1	0x2	90:9a:4a:22:12:a8	*	enp0s3

Örneğin, Mevcut ip yönlendirmenin olup olmadupu

root@liman21:/home/sysadmin# cat /proc/sys/net/ipv4/ip_forward

0

İstemci Gözünden Ağ İnceleme

Ping, nslookup, host, dig, telnet,traceroute, nmap, openssl

Sunucu Gözünden Ağ İnceleme

ss, systemctl, tcpdump

Openssl

SSL ya da TLS protokollerinde hizmet alınan portta gerçekten bir sertifika alınıp alınmadığı kontrol edilebilir

openssl s_client -connect www.google.com:443

openssl s_client -connect domain.lab:636

Nmap

nmap -sP x.x.x.0/24	Ping ile tarama
nmap -PS x.x.x.0/24	TCP-Syn ile tarama
nmap -PA x.x.x.0/24	TCP-ACK ile tarama
nmap -PE x.x.x.0/24	ICMP Echo Reguest ile tarama
nmap -PU x.x.x.0/24	UDP ping ile tarama
nmap -PR x.x.x.0/24	ARP ping ile tarama
nmap -traceroute x.x.x.0/24	Paketin yol analizini yapar
nmap -R x.x.x.0/24	IP adreslerinden hostname keşfi gerçekleştirir
nmap -system-dns x.x.x.0/24	İşletim sisteminde ki DNS serverleri kullanır

nmap -sS x.x.x.x	SYN port analizi
nmap -sU x.x.x.x	UDP port analizi
nmap -sT x.x.x.x	TCP Connect port analizi
nmap -sS x.x.x.x	Servis versiyon taraması
nmap -sS -O x.x.x.x	İşletim sistemi analizi
nmap -sS -A x.x.x.x	İşletim sistemi versiyon taraması

nmap -sS -p50 x.x.x.x	50 portunu tarar
nmap -sS -p1-80 x.x.x.x	1 ve 80 arasında ki tüm portları tarar
nmap -sS -p2,44,65 x.x.x.x	2,44 ve 65 portlarını tarar
nmap -sS -p- x.x.x.x	Ağdaki tüm IP'leri tarar

Linux Networking – Configuration

Qucik Scan (TCP) : En çok kullanılan 100 port üzerinde tarama yaparak hedef sistemdeki portlar, durumları, MAC adresleri gibi genel bilgiler elde edilir.

nmap -T4 -F 192.168.1.39

nmap --reason 192.168.5.106 komutuyla TCP paketleri içindeki SYN-ACK flag’leri kullanılarak en bilinen 1000 port üzerinde tarama yapılır. Açık olan port numaraları ve servis tipleri listelenir.

ss

Parametreler

-a: To display all sockets
-l: To display only listening sockets
-t: To display only TCP sockets
-u: To display only UDP sockets
-x: To display only UNIX domain sockets
-m: To display socket memory usage
-s: To display summary statistics
-p: To show process IDs (PID)
-e: To show detailed socket information
-n: don't resolve service names
-4/6: Filter results further by listing IPv4/IPv6 connections

Filtre

state
dst : 22, src :https