Turkish Hacker Anti Fighters

TU HAF

GÜVENLİK

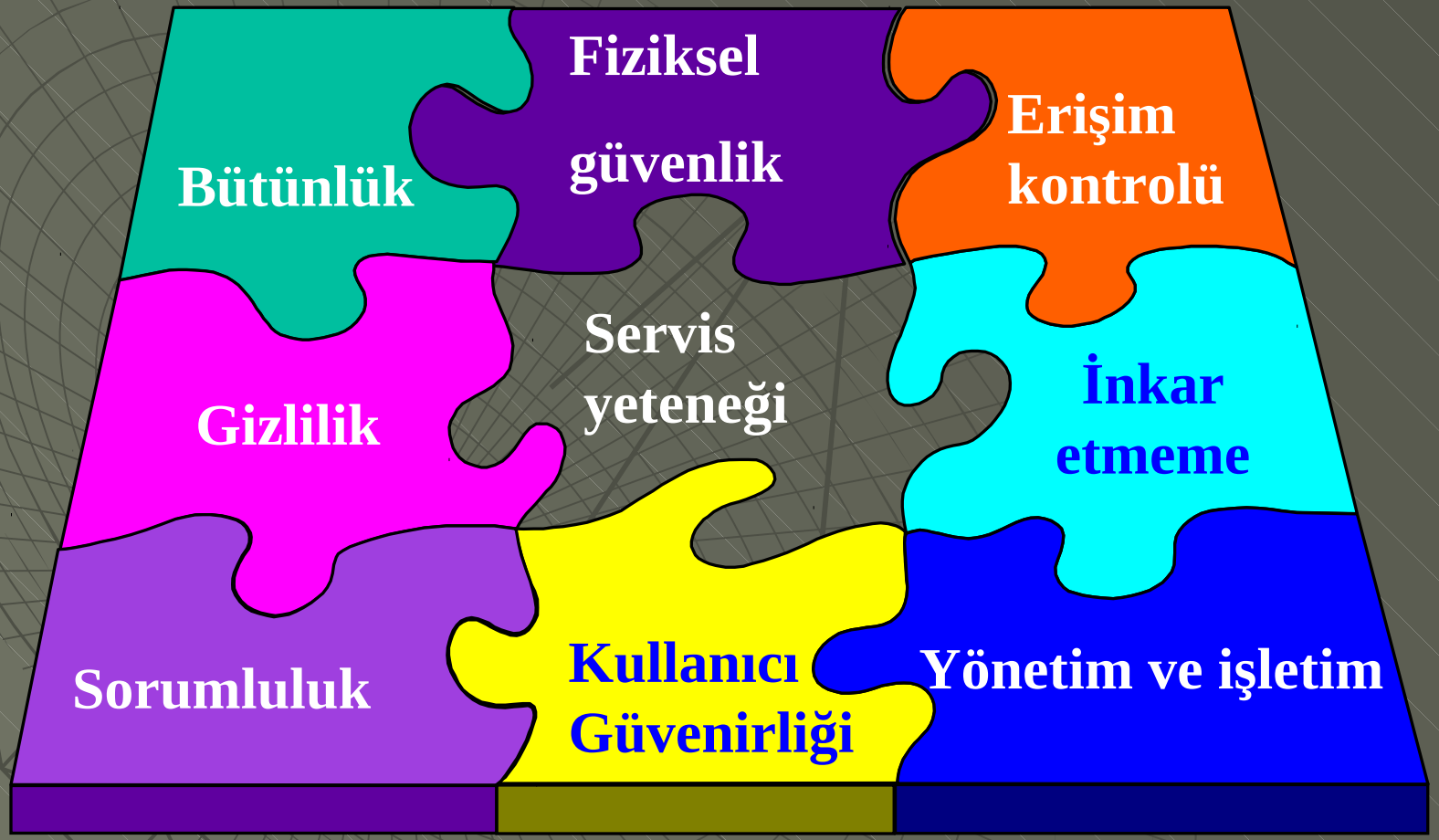
Çağlar ÜLKÜDERNER
caglar@tubitak.gov.tr

TUHAF NEDİR?

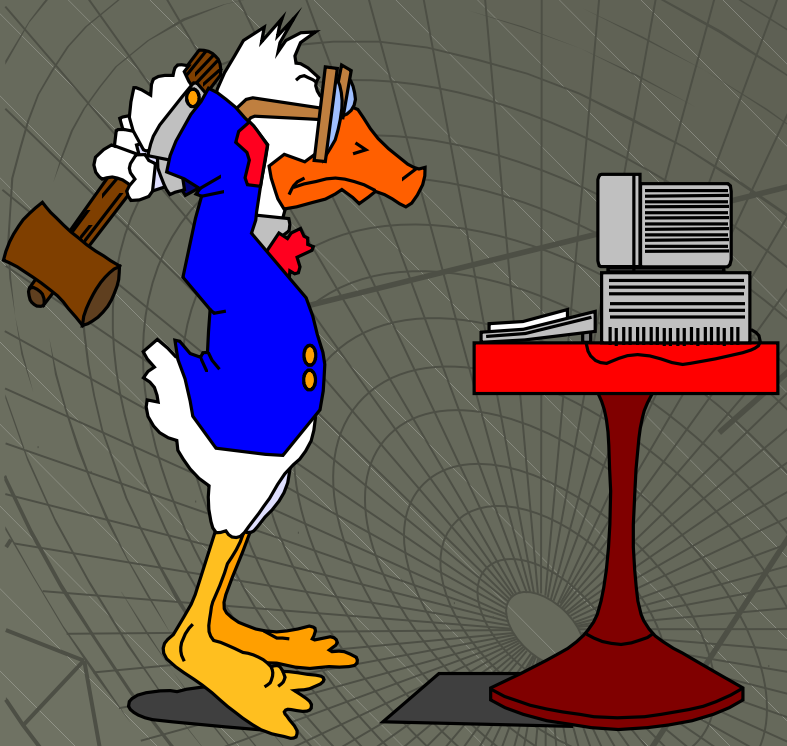
Turkish Hacker AntiFighters:

- **Süleyman Kondakçı'nın fikri.**
- **Bilişim ile iç içe olan kişi, kurum ve kuruluşların bilgi güvenliği açısından bilinçlendirmek.**
- **Bilinçlendirme tek başına yeterli olmayabilir. Bu nedenle gönüllü olarak güvenlik tarama, çözüm ve önerileri sunmak.**

BT Güvenlik Bileşenleri



Dağıtık Sistem Güvenliği



- Merkezi sistemden çok farklı
- Merkezi sistemde güvenlik tek noktada odaklı
- Dağıtık sistem güvenliği geniş coğrafik alan kapsamında
- Dağıtık sistemde güvenliği denetleyen herhangi bir merkezi nokta yok
- Güvenlik sistemi bütün coğrafik alana dağıtılmalı
- Dağıtık sistem güvenliği pahalı ve daha güvensiz
- Her uç kendi kafasına ve kurallarına göre iş yapar

BT Güvenliği Tehditleri

- Kimlik Gizleme
- Yetkisiz Giriş
- Bilgi Açığa çıkarmak
- Değişiklikler, bozulmalar
- Servislerin Engellenmesi
- Servislerin Çalınması
- İnkar etmeme (denial of origin)
- Zaman değişiklikleri

Saldırı Tipleri

- Packet Sniffing (Eavesdropping)
- IP Address Spoofing
- Port Scanning
- Denial-of-Service Attack
- Application Layer Attack
  - Trojan Horse
  - Java and ActiveX applets
  - Virus and Worms

Internet Yolundan

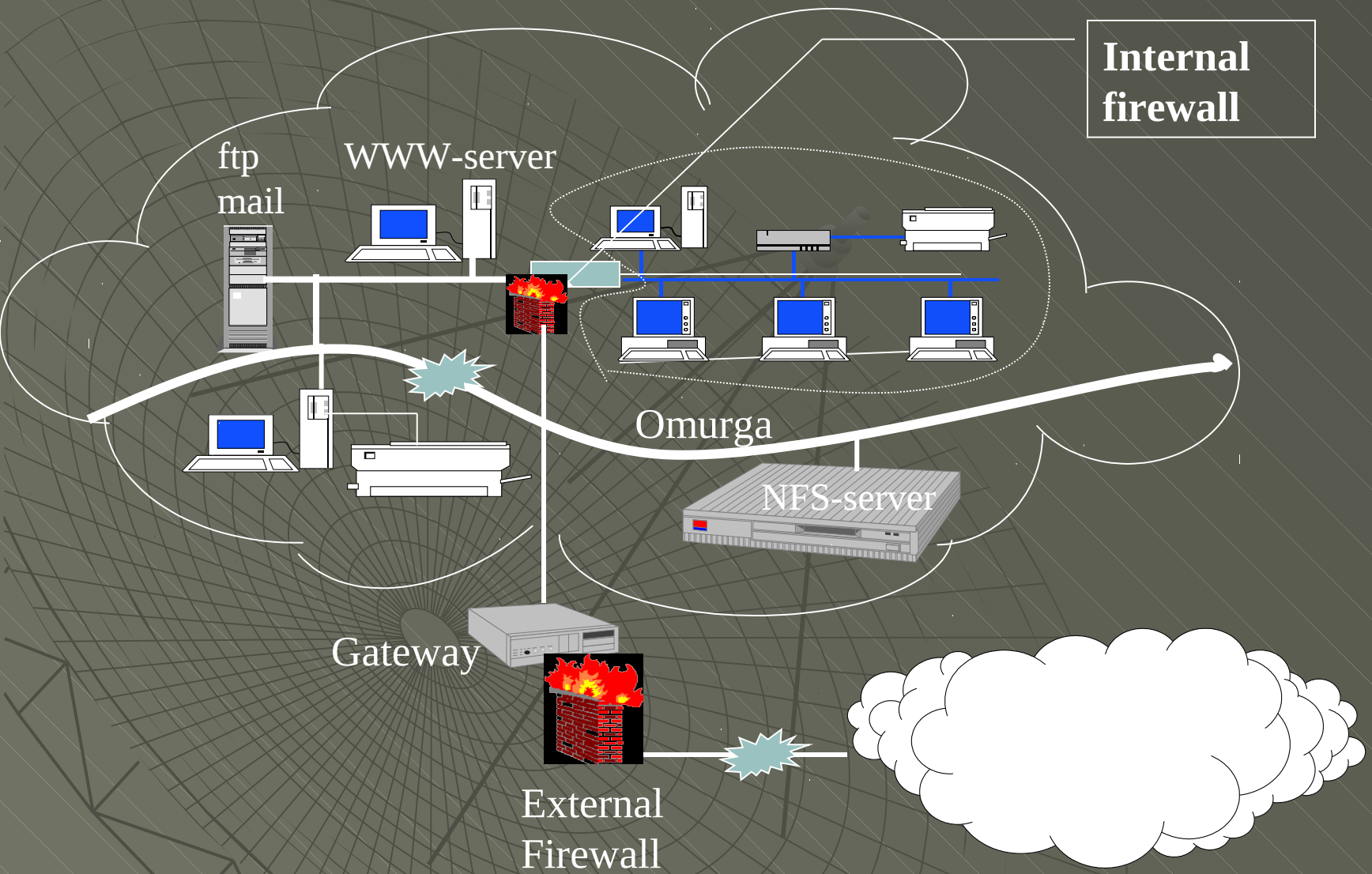
- **Firewall'u araştırın**:
  - Bilinen ***zayıflıkları?***
  - Nelere ***izin veriyor?***
  - Nelere ***izin vermiyor?***
- **Routerı araştırın*:***
  - Bilinen ***zayıflıkları?***
  - Remote login ***izini?***
  - Network ***topoğrafyası ulaşılabilir mi?***

Internet Yoluyla

- ***Gelen istekleri başlatan*** adres ne?
- ***Firewall ününde*** bir sistem var mı?
- Uzaktan bağlantıya izin veriyor ise, Hangi **doğrulama methodu** var?
  - Simple passwords?
  - one-time passwords?
  - single sign-on?

Internet Yoluyla

- Sistem ***zayıflıklarını araştırma***:
  - Birçok firewall e-mail izni verdiğinden, **`sendmail`** açıklıkları varmı?
  - Eğer ayrıcalıklı giriş yapılırsa, TCP/IP sniffer diğer sistemlerden bilgi almak için yüklenebilinir mi?
    - IP-spoofing
    - Hijacking


Internal firewall
ftp
mail
WWW-server
Omurga
NFS-server
Gateway
External Firewall

Sınır Korumaları & Firewall Kategorileri

- 1) Packet Filters
- 2) Circuit Level Firewalls
- 3) Application Layer Firewalls
- 4) Dynamic Packet Filters

Paket Filitreleri
İzin Verdikleri ve Vermedikleri

- IP katmanında Network Trafik Analizi
- Her pakete belirli kurallar uygulanır:
  - Fiziksel network arabirimi
  - Kaynak IP adresi
  - Hedef IP adresi
  - Taşıyıcı katman tipi (TCP,UDP, ICMP)
  - Taşıyıcı katman kaynak portu
  - Taşıyıcı katman hedef portu

Circuit Level Firewalls

- Uygulanacak kontrol mekanizmaları:
  - Paketin bağlantı isteyip istemediği
  - Paketin bağlantıya ait olup olmadığı
  - Paketin gerçek circuite ait olup olmadığı
- Paket kontrolü nasıl oluyor?
  - TCP tanışmasını izleyen her bağlantı düzenini sınamak
  - Gerçek circuit'ın tüm oturum durumlarını içeren geçerli bağlantı tablosu tablosunu yönetir

Application Layer Firewalls

- Tüm bağlantıları ve ard arda gelen bilgileri inceler
- HTTP veya FTP proxy sunucu
- Bağlantıdan önce paketler uygulama katmanında geçerli içerik analizinden geçirilir
  - Kullanıcı Şifrleri
  - İstenilen servis

Dynamic Packet Filters

- Güvenlik kuralları tabanında anında değişime izin verir.
- Sınırlı UDP transfer protokolünü ve ICMP protokolünü destekler.
- Her UDP paketini gerçek bağlantı hakkıyla sınırlar.
- DNS gibi uygulama katman protokollerine izin verir.

Güvenlik Politikası

- **Politika zorunlu olmalıdır**
- Politika ***saptanmamışsa*** güvenlik ***olanaksız***
- Güvenlik politikası nedir?
  - Ortak kurallar kümesi
  - Yüksek seviyede yönergeleri içerir ve bunlarla ortak davranış ve korunma biçimi sağlar
  - Güvenlik amaç ve hedeflerini belirler
  - Etikleri tanımlar ve sorumluluk yükler
  - Prosüdürleri belirler
  - Personele liderlerin ne düşündüklerini açıklar
  - Personelin neler yapmaları gerektiğini belirler

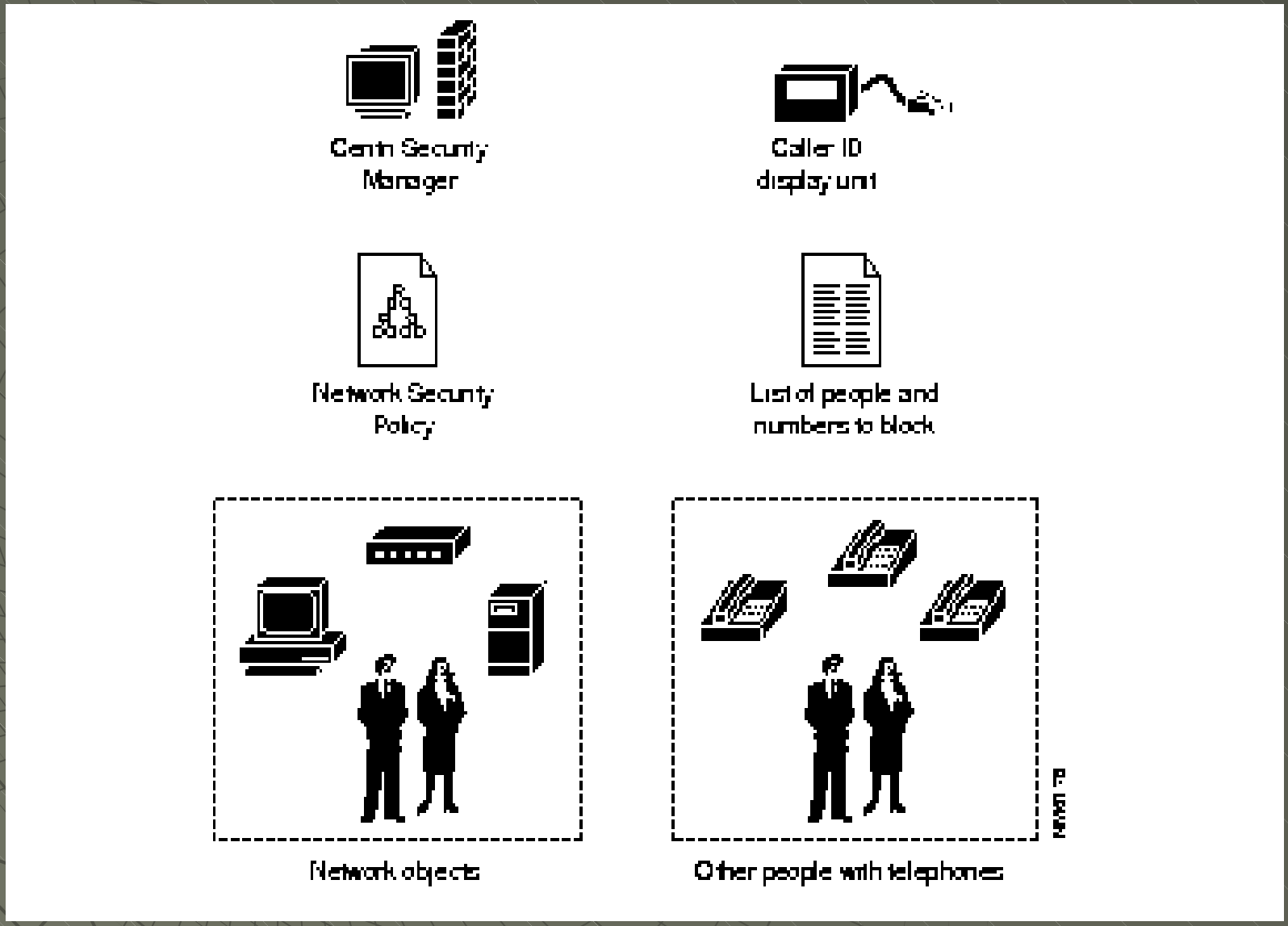
Güvenlik Politikası Yaklaşımı

- **Hangi kaynaklar korunmalı?**
  - Kaynaklar ne derece önemli
- **Kimlerden korunmalı?**
  - Bunlar ne derece tehdit edici
- **Nasıl korunmalı?**
- Güvenlik politikanı sürekli gözden geçir
  - Ağda ve kullanıcılardaki değişmelerin etkisini gözden geçir

Güvenlik Politikası Prensipleri

- **User Awareness (Bilinçli kullanıcı)**
  - Kullanıcılar güvenliğin önemli olduğunu anlamak zorundadır: eğitim, güvenlik onlar için
- **Disaster Recovery Plan (Felaketten arınma Planı)**
  - Bir felaket olduğunda bundan kurtulabilmelisiniz.
- **Security Administration**
  - Güvenlik çalışanlarına otoriteyi şart koşun.

Başka Bir Bakışla Güvenlik Politikası

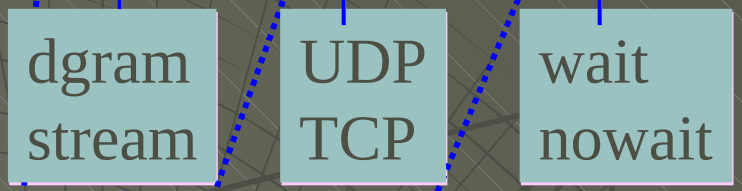


Bazı Ağ Kütük, Program Ve Daemon'ları

- **`/etc/hosts`**:
  - Makina ad ve IP-adreslerini içerir.
- **`/etc/ifconfig`**:
  - Ağ bağlantısını çalıştırmak ve konfigürlemek için kullanılan programdır.
- **`/etc/inetd`**:
  - Ana ağ daemonu, ağı dinler ve ondan istenen hizmetler için gereken programı sürer. Hizmetler **`/etc/inetd.conf`** kütüğünde belirlenmiştir.

/etc/inetd.conf

Process socket-type protocol processing location daemon




```
# cat /etc/inetd.conf
# Internet server configuration database
ftp    stream tcp    nowait /usr/etc/ftpd       ftpd
telnet stream tcp    nowait /etc/telnetd        telnetd
login  stream tcp    nowait /etc/rlogind        rlogind
finger stream tcp    nowait /usr/etc/fingerd    fingerd
talk   dgram  udp    wait   /etc/talkd          talkd
time   dgram  udp    wait   /etc/miscd          timed
```

Hizmetler Kütüğü

- **`/etc/services`**: Ağ programlarının port numarasını ve adını içerir

```
# cat /etc/services
# Network services, Internet style
echo  7/tcp
netstat     11/tcp
ftp   21/tcp
telnet      23/tcp
route 520/udp
shell 514/tcp
finger      79/tcp
```

Ağ protokol Kütüğü

- **/etc/protocols**:
  - protokol ad ve numaralarını içerir

```
# cat /etc/protocols
ip     0      IP   # Internet Protocol
icmp   1      ICMP # Internet Control Message Prot.
ggp    3      GGP  # Gateway-Gateway Protocol
tcp    6      TCP  # Transmission Control Protocol
pup    12     PUP  # PARC Universal Packet Protocol
udp    17     UDP  # User Datagram Protocol
```

Ağ Sınama Yazılımları

- **`Ifconfig`**: Ağınızı başlatır,durdurur, ayakta olup olmadığını gösterir.
- **`Ping`**: Ağdaki herhangi bir sisteme erişilip erişilmediğini saptar.
- **`Netstat`**: Ağ bağlantısı için istatistik verir:
  - routing table
  - IP packet iletişimi
  - ağınız sağlıklımı?

Ağ Sınama Yazılımları

- **Nslookup**: DNS-name service hakkında bilgi verir. BIND hizmetlerine dahildir.
- **Dig**: **nslookup** gibi,daha basit, detaylı.
- **Arp**:
  - IP ve Ethernet adresi çevirmeleri için bilgi sağlar.
  - Çakışan IP-adreslerini saptar.
- **Tcpdump:** trafik analizi için
- **Traceroute**: Sisteminizden çıkan packetlerin hangi rotada seyrettiğini saptar.
- **Ripquery**: Routing Information Protocol (RIP)'u için bilgi sağlar.

Network Related Files/Directories

/etc/hosts	Local host table
/etc/services	ARPA services
/etc/hosts.equiv	Watch out this, Security prone
/etc/hosts.lpd	Watch out this, Security prone
/.rhosts	Remote accessor, Security prone
/etc/netmasks	Subnetmask in dot notation
/etc/networks	A historical file
/etc/netconfig	Solaris net configuration
/etc/inet/*	Solaris configuration file
/etc/init.d/rootuser	Solaris network startup
/etc/defaultdomain	Default domain name
/etc/defaultrouter	Default router name
/etc/rc.bsdnet	AIX BSD-style net setup
/etc/rc.local	AIX network startup for BSD fans

Network Related Files/Directories

/etc/rc.{net,tcpip,nfs}	AIX network startup files
/etc/inetd.conf	Allows network daemons
/etc/nsswitch.conf	Name service lookup order
/etc/resolv.conf	Name resolver IP-address
/etc/protocols	What protocols should be available
/etc/hostname.*[0-9]	Multi-homed hosts
/etc/ftpusers	Nontrusted ftp users access denier
/etc/dfs/dfstab	Solaris resource distributor
/etc/dfs/fstypes	Solaris filesystem distribution table
/etc/dfs/sharetab	Solaris Exported resource table
/etc/{exports,xtab}	BSD Export and Exported resources
/etc/fstab	BSD filesystem table
/etc/sendmail.cf	Sendmail config file
/etc/init.d/*	IRIX network startup files
/etc/config/*	IRIX network options
/etc/chkconfig	IRIX network configuration tool

Turkish Hacker Anti Fighters

TU HAF

GÜVENLİK

SORULAR?

Çağlar ÜLKÜDERNER
caglar@tubitak.gov.tr