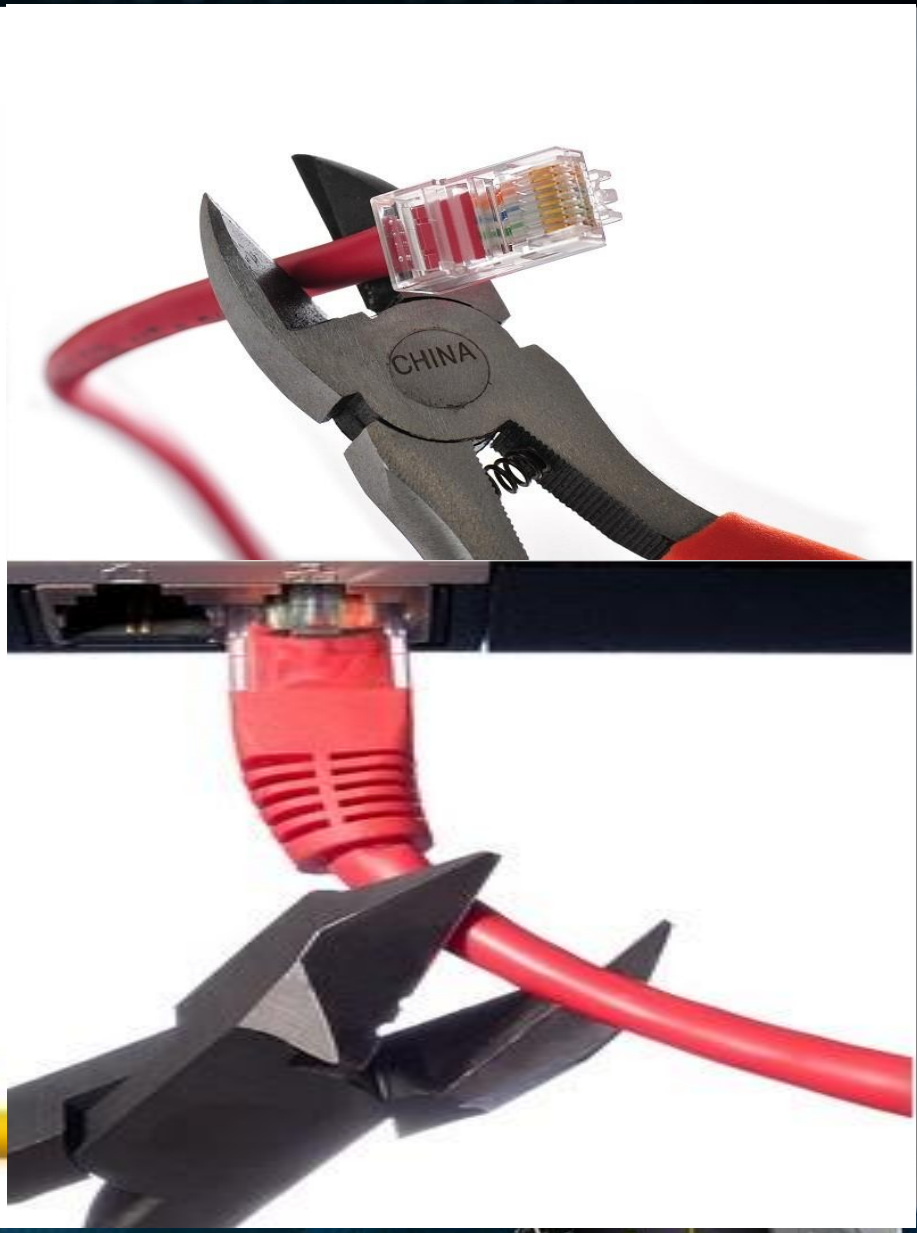
Linux ve Güvenlik


Your website is hacked!
HACKED
LINUX

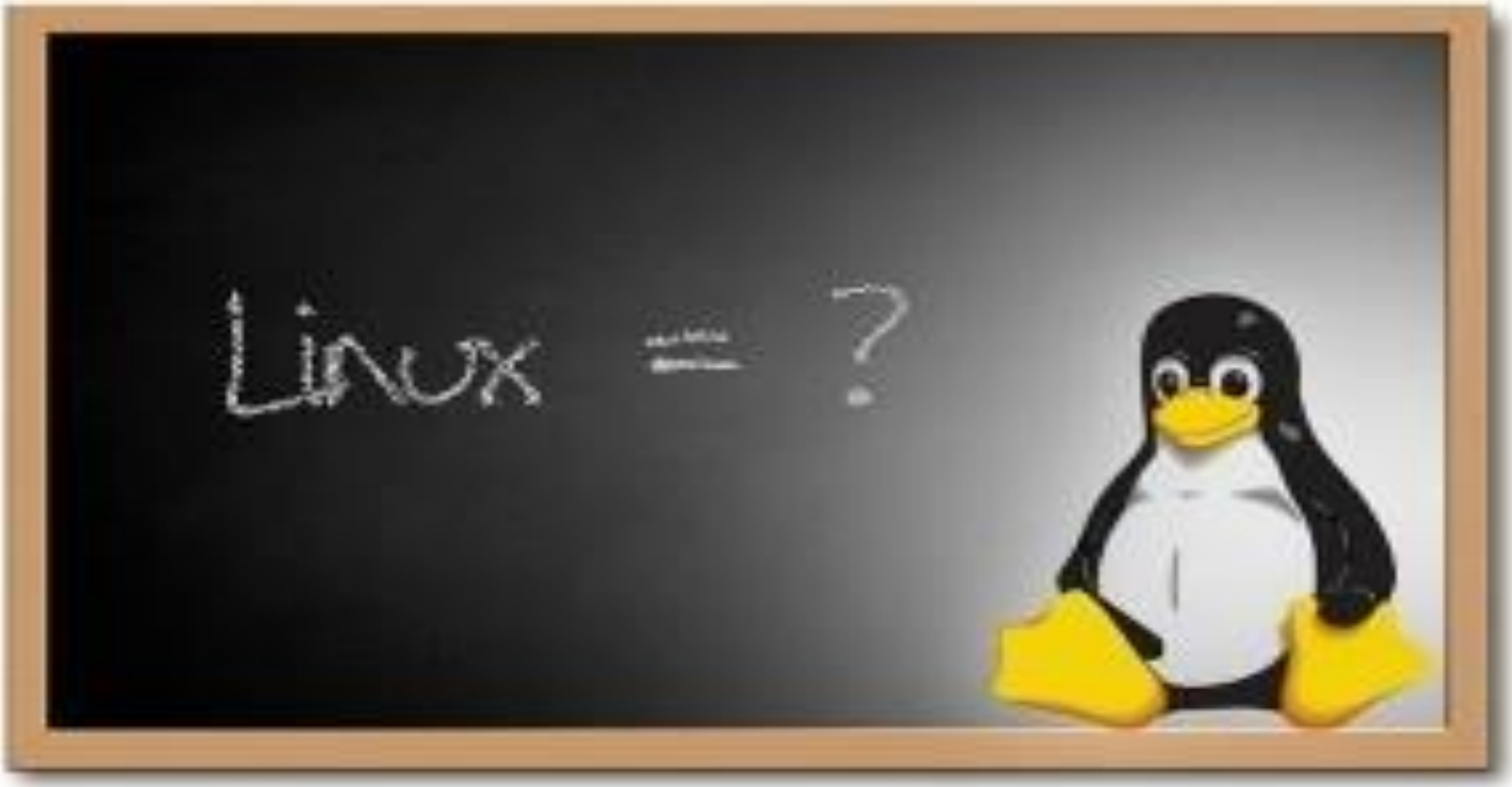

computer
security
phishing
firewall
attack
hacking
spyware
internet
malware
infection
cyber
networks
detection
hacker
intruder
trojan
spam
virus
infected
crime
network
groups
hackers
information
terrorism
offensive
purposes
criminal
people
unsolicited
websites
packages
allegedly
resources
warfare
target
document
individual
communications
copyrights
distributed
time
trafficking
counts
organized
service
crimes
between
electronic
individuals
university
systems
services
increasingly
activities
documented
defined
access
technical
nation
facilitated
included
directly
concern
defense
government
entering
group
well
considered
cases
cyberterrorism
going
including
stored
devices
physical
obscene
sending
rooms
system
victim
future
mail
combatting
face
international
unauthorized
limits
server
variety
traffickers
federal
problems
hate
LINUX

En Güvenli Sistem



LINUX

Linux Hakkında Ne Biliyoruz?



Minimum Sistem

Minimum Sistem Maximum Güvenlik

- Linux'unuzda yüklü her programı ya da servisi kullanıyor musunuz?

- Emin değilseniz kontrol edin;
  - yum list installed
    - yum list PkgName
      - yum remove PkgName
  - Dpkg list
    - Dpkg info PkgName
      - aptget remove PkgName

Minimum Sistem

Minimum Sistem Maximum Güvenlik

- Linux'unuzda yüklü her programı ya da servisi kullanıyor musunuz?

- Emin değilseniz kontrol edin;
  - yum list installed
    - yum list PkgName
      - yum remove PkgName
  - Dpkg list
    - Dpkg inf o PkgName
      - aptget remove PkgName

Inetd
xinetd
ypserv
tftp-server
telnet-server
rsh-server

Önerilmeyen Servisler

Bu Servisleri Kullanmalımıyım?

- **inetd** : Internet Daemon
- **xinetd** : Extended Inetd
- **ypserv** : NIS sunucusu
- **tftp** : Trivial File Transfer Protocol
- **telnet** : Internet Protocol
- **rsh** : Remote Shell

LINUX

Önerilmeyen Servisler

Bu Servisleri Kullanmalımıyım?

- **inetd** : Internet Daemon
- **xinetd** : Extended Inetd
- **ypserv** : NIS sunucusu
- **tftp** : Trivial File Transfer Protocol
- **telnet** : Internet Protocol
- **rsh** : Remote Shell

Inetd
xinetd
ypserv
tftp-server
telnet-server
rsh-server

Güvenliği Yüksek Servisler

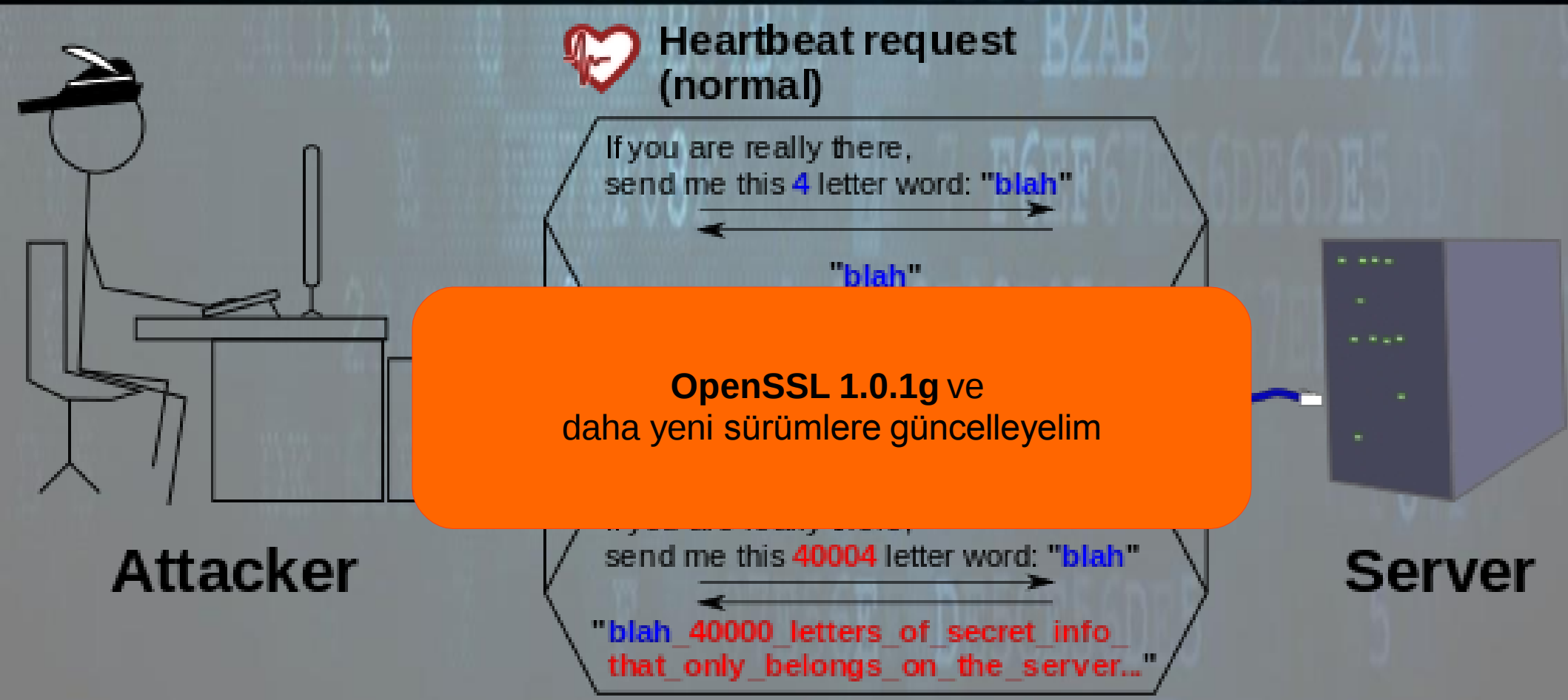
İletişimde Hangi Servisleri Kullanmalıyım?

- OpenSSH
- SFTP
- FTPS

Heartbleed Nasıl Çalışıyor?

LINUX

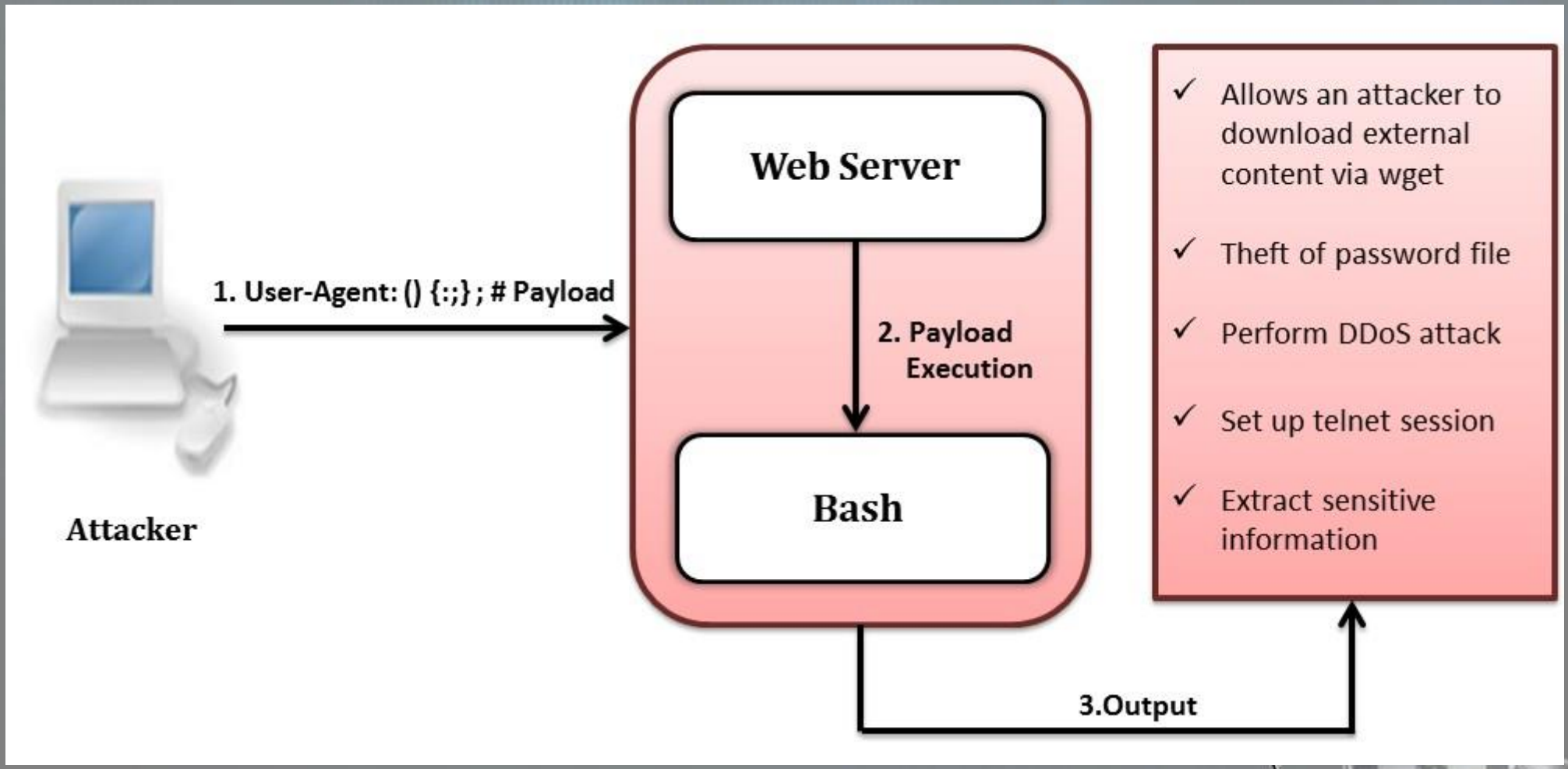
Heartbleed Nasıl Çalışıyor?



OpenSSL 1.0.1g ve
daha yeni sürümlere güncelleyelim

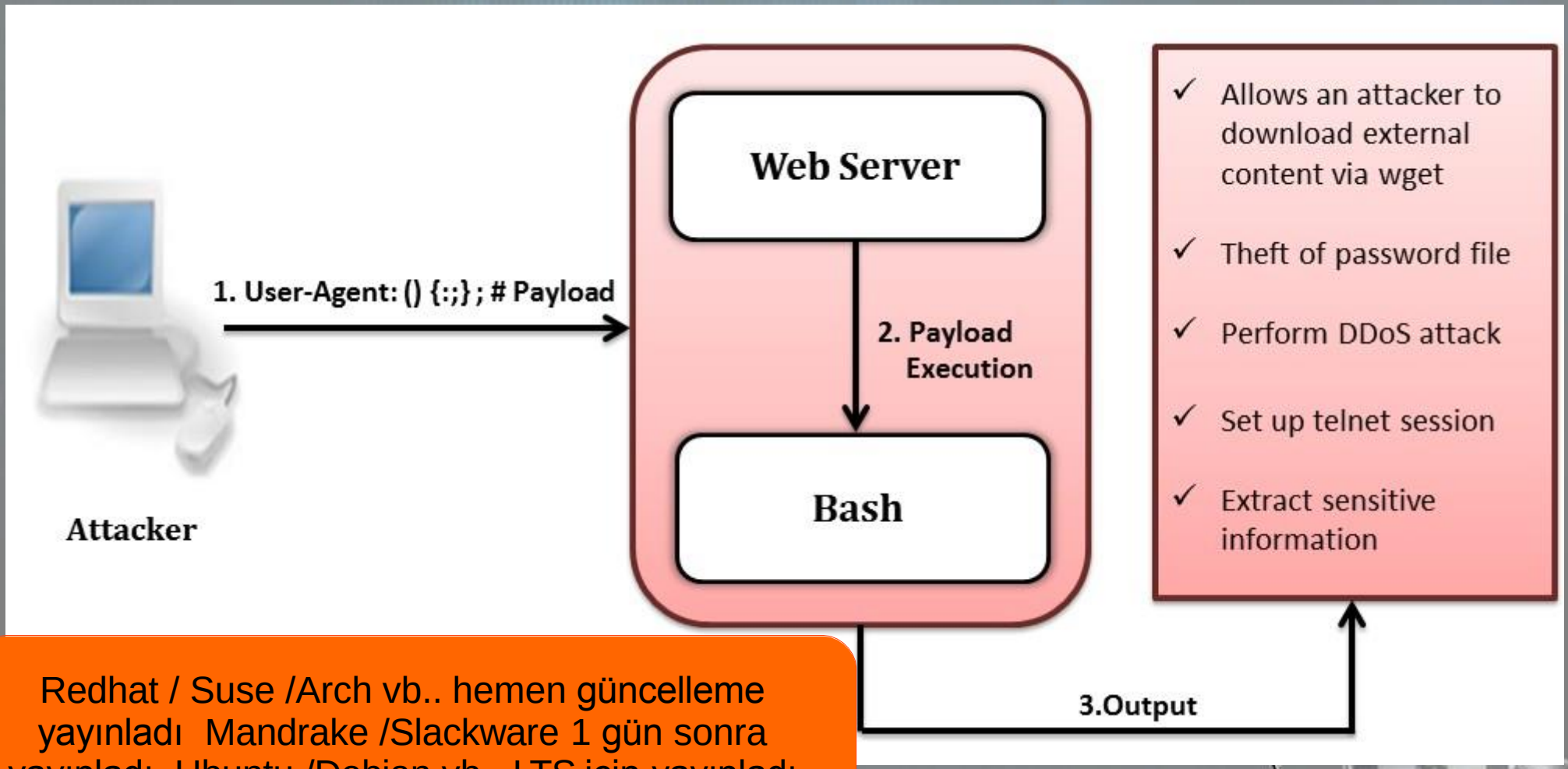
Shellshock (Bashdoor)

env x='() { :;}; echo vulnerable' bash c "echo this is a test"



Shellshock (Bashdoor)

env x='() { :;}; echo vulnerable' bash c "echo this is a test"



Redhat / Suse /Arch vb.. hemen güncelleme yayınladı Mandrake /Slackware 1 gün sonra yayınladı Ubuntu /Debian vb.. LTS için yayınladı

LINUX

Kernel / Software Update

Linux'unuz her zaman güncel kalmalı.

- Güvenlik güncellemelerini sisteminiz otomatik yüklemeli
- Redhat ve türevleri için güvenlik güncellemeleri maillerini alıyor şekilde ayarlayın
- Debian ve türevleri için apticron'u aktif edebilirsiniz.

redhat LINUX

 # vim /etc/yum/yum-updatesd.conf

emit_via = email

email_to = eposta@gmail.com
email_from = system@system.com

debian

 # apt-get update
 # apt-get install apticron

vi /etc/apticron/apticron.conf
EMAIL="eposta@gmail.com"

Kernel Güvenliği

SELinux (SecurityEnhanced Linux)

- **SELinux / AppArmor / Grsecurity**
- MAC – Mandatory Access Control
- DAC – Discretionary Access Control

 # sestatus

```
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      28
```

 # semanage

LINUX

Kernel Güvenliği

SELinux | AppArmor | Grsecurity

SELinux	AppArmor	Grsecurity
Güçlü erişim kontrolü	Kolay anlaşılır araçlar ve policy	Kullanımı Kolay
Uzmanlar için	Yeni / Uzmanlar için	Yeni Kullanıcılar için
RedHat vb.. , Debian vb..	Suse vb..	Her Linux'a uygun

Kullanıcılar / Şifreler

Aynı Şifrenin Tekrar Kullanılmasını Engelleyelim

pam_unix / pam_unix2 modüllerini yüklemelisiniz.
Eski şifrelerimiz **/etc/security/opasswd** dosyasında tutulacaktır.

Ayar dosyalarımız ;
Debian : /etc/pam.d/common-password
Redhat : /etc/pam.d/system-auth
Suse : /etc/pam.d/common-auth

password sufficient pam_unix.so use_authtok md5 shadow remember=13
password sufficient pam_unix2.so use_authtok md5 shadow remember=13

-rw-------. root root system_u:object_r:shadow_t:s0 /etc/security/opasswd

Kullanıcılar / Şifreler

Hatalı Deneme Yapan Kullanıcıyı da Engelleyin!

Faillock yardımızına koşacaktır.

Kullanıcı bazlı engelleme yapabilirsiniz.

İstediğiniz sayıda hata yapan kullanıcıyı engelleyebilirsiniz.

İstediğiniz süre hesabı kapalı kalabilir.

LINUX

Kullanıcılar / Şifreler

Şifresiz hesaplar var mı kontrol edilmeli!

Shadow dosyasından kontrol edebilirsiniz

Yada : **awk -F: '($2 == "") {print}' /etc/shadow**

Kullanıcılar / Şifreler

Root yetkisine sahip tek account olmalı!

UID = 0 olan yani root yetkili tek hesap olmalı

awk -F: '($3 == "0") {print}' /etc/passwd

Sadece şu olmalı ;
root:x:0:0:root:/root:/bin/bash

Kullanıcılar / Şifreler

Su yerine Sudo kullanılmalı!

Root olarak işlem yaparsanız şifre sorulmaz.
Sudo ile 1 kez şifre girip 15dk şifresiz işlem yapabilirsiniz.

Sudoers dosyasındaki kurallar titizlikle hazırlanmalı.

moderator ALL=/sbin/halt, /bin/kill, /bin/cp, /bin/mv

user ALL= NOPASSWD: /sbin/halt

kullanıcı dev0=/usr/sbin/*

Portlar

Açık portları kapatmalısınız!

Dinlenilen portlar bizim için en önemli noktalardır.
Tespit etmek ve kullanan uygulamayı görmek için;

netstat -tulpn

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      2998/master
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      3123/mysqld
tcp        0      0 0.0.0.0:60714           0.0.0.0:*               LISTEN      2810/rpc.statd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1689/rpcbind
tcp        0      0 127.0.0.1:5942          0.0.0.0:*               LISTEN      2659/teamviewerd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2641/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      919/cupsd
tcp6       0      0 ::1:25                  :::*                    LISTEN      2998/master
tcp6       0      0 :::45348                :::*                    LISTEN      2810/rpc.statd
tcp6       0      0 :::111                  :::*                    LISTEN      1689/rpcbind
tcp6       0      0 :::80                   :::*                    LISTEN      2636/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      2641/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      919/cupsd
```

Portlar

Açık portları kapatmalısınız!

Dinlenilen portlar bizim için en önemli noktalardır.
Tespit etmek ve kullanan uygulamayı görmek için;

netstat -tulpn

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local                                                ram name
tcp        0      0 127.0.                                            ter
tcp        0      0 0.0.0.                                            qld
tcp        0      0 0.0.0.                                            .statd
tcp        0      0 0.0.0.                                            bind
tcp        0      0 127.0.                                            mviewerd
tcp        0      0 0.0.0.                                            d
tcp        0      0 127.0.                                            d
tcp6       0      0 ::1:25                                            ter
tcp6       0      0 :::453                                            .statd
tcp6       0      0 :::111                                            bind
tcp6       0      0 :::80                   :::*          LISTEN      2636/httpd
tcp6       0      0 :::22                   :::*          LISTEN      2641/sshd
tcp6       0      0 ::1:631                 :::*          LISTEN      919/cupsd
```

Açık ve istenmeyen portları Iptables ile kapatabilirsiniz!

Iptables / TCPWrappers

Linux Kernel'i sisteminizi Firewall gibi kullanmanızı destekler

- Iptables kullanıcı düzeyinde bir uygulamadır.
- Dışardan gelen trafiği filtreleyerek sadece istenen trafiğin içeri girmesini sağlar.
- TCPWrapper hostbased ACL sistemidir, hangi servislere hangi istemci erişebilir bunun kurallarını kontrol eder.

Kernel Conf.

/etc/sysctl.conf dosyasını titizlikle düzenlemeliyiz!

- Yapacağımız ayarla IP spoof'u engelleyebilir.
- Broadcastlere isteklerine ignore dönebilir.
- Spoof yapılmış paketleride loglayabiliriz.

Kernel Conf.

/etc/sysctl.conf dosyasını titizlikle düzenlemeliyiz!

- Yapacağımız ayarla IP spoof'u engelleyebilir.
- Broadcastlere isteklerine ignore dönebilir.
- Spoof yapılmış paketleride loglayabiliriz.

execshield'i aktif edelim
kernel.execshield=1
kernel.randomize_va_space=1
IP spoofing korumasını etkinleştirelim
net.ipv4.conf.all.rp_filter=1
IP source routing'i kapatalım
net.ipv4.conf.all.accept_source_route=0
#Broadcast isteklerine ignore dönelim
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_messages=1
Loglama yapalım
net.ipv4.conf.all.log_martians = 1

Logwatch / Logcheck

Logwatch sizin için logların özetini çıkartır!

iptables firewall Begin Logged 87 packets on interface eth0
From 58.y.xxx.ww 1 packet to tcp(8080)
From 59.www.zzz.yyy 1 packet to tcp(22)
From 60.32.nnn.yyy 2 packets to tcp(45633)
From 222.xxx.ttt.zz 5 packets to tcp(8000,8080,8800)
iptables firewall End
Sudo (securelog) Begin
kullanıcı => root

/bin/su 6 Time(s).
Sudo (securelog) End

Auditd

Fazlasıyla log bilgisi almak için audit ayarlanmalı!

Sistem başlatma ve kapatma olayları
Tarih ve olayın zamanı.
Kullanıcı bazlı işlem logu
Olay (düzenleme, erişim, güncelleme dosyasını ve komutları, silme yazma)
Başarı ya da olayın başarısızlıkla sonuçlanması.
Kayıtlar tarih ve saati değiştirme olayları.
Sistemin ağ ayarlarını değiştirmek için değişiklik yapılmış kim olduğunu bulun.
Kullanıcı / grup bilgilerinin değişimlerinin tutulması.
Bir dosyaya vb değişiklik yapan görün

Auditd

Fazlasıyla log bilgisi almak için audit ayarlanmalı!

Sistem başlatma ve kapatma olayları
Tarih ve olayın zamanı.
Kullanıcı bazlı işlem logu
Olay düzenleme, erişim, güncelleme dosyasını silme ve komut yazma)
Başarı ya da olayın başarısızlıkla sonuçlanması.
Kayıtlar tarih ve saati değiştirme olayları.
Sistemin ağ ayarlarını değiştirmek için değişiklik yapılmış kim olduğunu bulun.
Kullanıcı / grup bilgilerinin değişimlerinin tutulması.
Bir dosyaya vb değişiklik yapan görün

auditctl w /etc/shadow k shadowfile p rwx

auditctl a exit,never S mount

auditctl a entry,always S all F pid=1005

Saldırı Tespit Sistemi

Zararlı Yazılım, Ddos Attack, Port Scanner vb..

AIDE (Advanced Intrusion Detection Environment)
Bilgisayarı izleme ve analiz etme konusunda başarılı bir proje.

Snort
Saldırı tespit yazılımı olarak paket inceleme, loglama ve anlık trafik analiziyle daha etkili ve geniş kullanım alanına sahip bir yazılım.

Daha fazlası...

Fiziki güvenlik
Grub şifreleme
Disk partition
Disk şifreleme
Dosya şifreleme
Şifreli Emailler
Düzenli yedekleme
Buffer overflow koruması
Güvenli ve Tek Ağ
Açılışta otomatik başlayan servislerin kapatılması
X window'un silinmesi
Disk kullanım kotası kullanılması
Istenmeyen SUID ve SGID binarylerinin kapatılması
Sticky Bit + Writable dosyaların bulunması
Sahipsiz dosyaların bulunması
Kerberos kullanımı

Linux ve Güvenlik