Sare Segurtasuna

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Sare Segurtasuna

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-issks-31

Sare Segurtasuna

- Interneterako konexioa
- Perimetroaren defentsa
- Proxy
- Firewall, DMZ
- Honeypot, honeynet
- VPN
- Eraso ohikoenak

Interneterako konexioa

Informazioaren **Konfidentzialtasuna** eta **osotasuna** protokolo kriptografikoen bidez

Erabiltzaileentzako autentikazio zerbitzua

Sarbideen kontrola

Zerbitzuen erabilera gainbegiratzea

Interneterako konexioa

Sarearen eta zerbitzuen **prestasuna** bermatzea

Ordenagailuetara sartzeko kontrola

Intrusio-saiakerak saihestea

Defentsa Perimetrala

Barruko eta kanpoko sarearen artean hesi bat sortzea

Trafiko guztia monitorizatutako eta babestutako puntu batetik bideratzea

Konexio batzuk bakarrik baimendu

Barne-sarean hain murriztaileak ez diren arauak

Proxy

Bitartekari gisa jarduten duen zerbitzaria

Bezeroak eskaerak egiten dizkio proxy-ari, eta hark kudeatzen eta urruneko zerbitzariei bidaltzen dizkie

Segurtasun handiagoa ematen du nabigazioan, zerbitzariak ez baitaki nor konektatu den benetan

Bezeroak kanpoko mundutik isolatzen ditu

Proxy

NAT (Network Address Translation) protokoloaren bidez zerbitzariak helbideen itzulpena burutzen du, ordenagailuen barne IP-ak kanpo IP bakarrean bihurtuz

Interneteko zein zerbitzu erabili ahal izango diren eta nork

IP eta Interneteko domeinu jakin batzuetarako sarbidea blokeatzea

Proxy

Cache-ak sortu nabigazioa bizkortzeko

Erabiltzaileen zerbitzuen erabileraren eta banda-zabaleraren auditoria

Antivirus perimetrala

Alderantzizko Proxy-a

Kanpotik enpresaren zerbitzarietarako sarbide kontrolatua, adibidez web zerbitzarietarako sarbidea

Karga banatu (load balancing)

Firewall

Sareko elementua (hardwarea edo softwarea), paketeak iragazten dituena administratzaileak aldez aurretik definitutako politikaren arabera, iturria eta helmuga kontuan hartuta

Proxy-arekin ez bezala, konexio zuzenak (baimenduak) egin daitezke kanpoko makinekin

Firewall

Baimendu gabeko trafikoa blokeatzea: Interneteko zerbitzuak, helbide jakin batzuk, etab.

Erakundeko barne ordenagailuak ezkutatzea, gerta daitezkeen erasoen aurrean

Ezkutatu barne-sarearen topologiari buruzko informazioa

Sartzen eta irteten den trafiko guztiaren erregistroa

Firewall

Erabilitako banda-zabaleraren muga, trafiko edo protokolo motaren arabera

Hainbat zerbitzuk erabilitako banda-zabaleraren gaineko estatistikak

Erasoak edo intrusio-saiakerak monitorizatzea

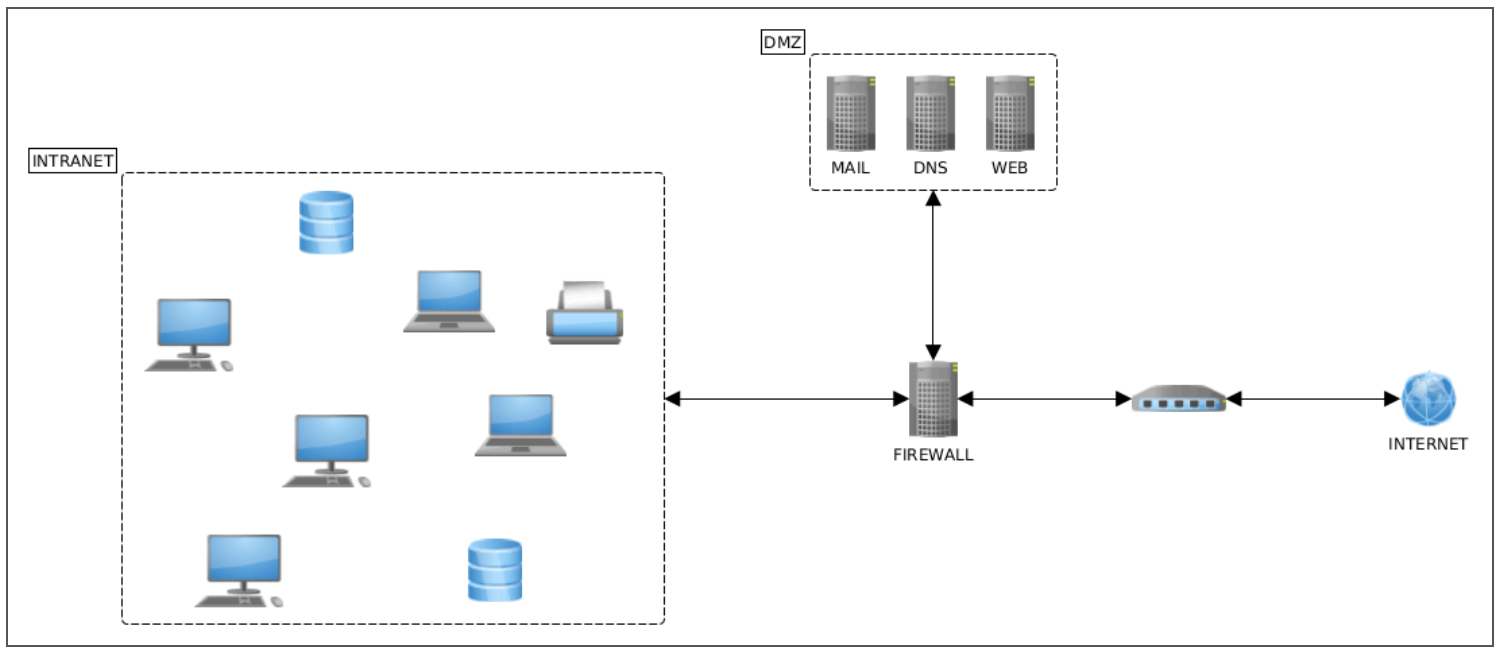
DMZ

Intranetaren eta Interneten artean dagoen zonaldea, segurtasun-arazoen eraginpean dauden zerbitzu publikoak (posta, ftp, etab.) dituena

Sare desberdinen arteko sarbidea mugatzen duen firewall bat edo bi erabiliz sortzen da

DMZtik ezin da zuzenean intranetera sartu

DMZ



Access Control List (ACL)

Iragazteko arauak

Kontuan hartuta: datu-paketeen jatorria eta xedea, protokoloa, zerbitzua (portua)

Access Control List

Regla	Acción	IP Origen	IP Destino	Proto-colo	Puerto Origen	Puerto Destino
1	Aceptar	172.16.0.0/16	192.168.0.4	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.8	tcp	cualquiera	80
3	Aceptar	172.16.0.0/16	192.168.0.2	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Firewall motak

Datu-paketeen mailan: paketeak jatorriaren/helmugaren arabera iragaztea, portuak, etab.

Dinamikoak (Statefull Packet Inspection): datu-paketeez gain, saioei buruzko informazioa ere kontuan hartzen dute (Flags)

Aplikazio-pasabideak: protokoloaren eta saioaren arauak hartzen dituzte kontuan, ez bakarrik banako paketeen datuak

Firewall

- **Politika murriztailea (zerrenda zuria)**: dena ukatzen da, esplizituki onartzen dena izan ezik
- Politika baimentzailea (zerrenda beltza): guztia onartzen da, esplizituki ukatzen dena izan ezik

Firewall: iragazki orokorrak

Difusio-helbidea (Broadcast) duten paketeak blokeatzea, DoS erasoak ekiditeko

Barne-helbideei dagokien jatorrizko helbidea duten sarrera paketeak blokeatu, nortasun-ordezpenaren ekiditeko (Spoofing)

RFC 1918 (Address Allocation for Private Internets) espezifikazioan dauden helbideak dituzten pakete guztiak blokeatu

Firewall: iragazki orokorrak

127.0.0.1 jatorrizko helbidea bezala duten paketeak blokeatu

Ping edo Traceroute eskaerei erantzunez barne-sarearen topologiari buruzko informazioa eman dezaketen ICMP kontrol-protokoloko paketeak blokeatzea

Firewall: iragazki orokorrak

Routerren bideratze-taulak aldatzeko aukera ematen duten ICMP Redirect paketeak blokeatzea

Baimendutako gutxienekoa baino tamaina txikiagoa duten edo goiburuan balio desegokiak duten pakete guztiak blokeatzea

Firewall: blokeatu behar diren portuak

Urruneko konexioak: Telnet (23), SSH (22), FTP (21)

NetBIOS protokoloa Windows-en

RPC eta NFS zerbitzua UNIX sareetan

HTTP, SSL, SMTP, POP, IMAP, DNS, LDAP zerbitzariak ez diren makinetan

Firewall: mugak

Ingenieritza sozialeko erasoak

Eraso fisikoak: adib. USB

Protokolo mailako erasoak, adib. HTTP

Kanpoan infektatu diren eramangarriek sartutako birusak

Log-en analisia: Common Log Format

```
127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700]
                                "GET /apache_pb.gif HTTP/1.0" 200 2326
```

- Bezero IP-a
- Bezero izena
- Erabiltzailearen izena
- Konexio data

Log-en analisia: Common Log Format

```
127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700]
                                "GET /apache_pb.gif HTTP/1.0" 200 2326
```

- Bezeroaren eskakizuna
- Itzulitako HTTP egoera
- Bidalitako Byte-ak

Intrusion Prevention System (IPS)

Sareetako segurtasun-intzidenteen aurrean modu automatizatuan hautemateaz eta erreakzionatzeaz arduratzen diren sistemak

Intrusion Prevention System (IPS)

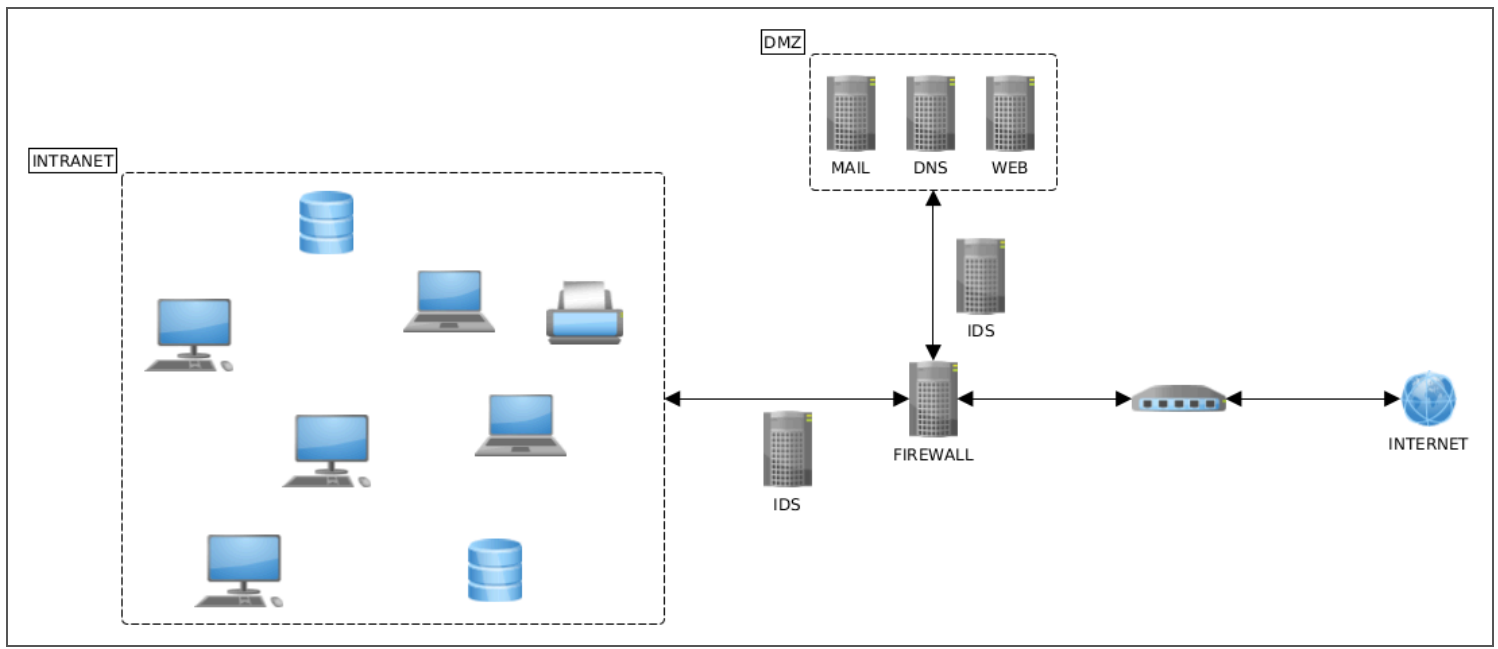
Sareko edo sistemako gertaeren iturria

Portaera normalen/ohiz kanpokoen datu-baseak

Analisi-motorra: gertaeren iturria aztertzen du, datu-basean oinarrituta

Erantzun-modulua: alarmak eta txostenak

Intrusion Prevention System (IPS)



Intrusion Prevention System (IPS)

Erantzun pasiboak: balizko intrusioak erregistratzea, txostenak sortzea

Erantzun aktiboak: TCP konexioak deuseztatzea konexioetan berriz hasteko paketeak injektatuz; suebakiak berriz konfiguratzea trafiko anomaloa iragazteko, zerbitzarien deskonexio automatikoa, kontuak/pribilegioak blokeatzea, eraso-jatorria aurkitzea eta ISPei jakinaraztea

HIDS (Host IDS)

Intrusioak host batean, makina jakin batean

Kernel-aren log-en analisia

Programen osotasuna bermatzea

Baliabideei esleitutako baimenen aldizkako auditoretza

Aplikazio berriak instalatzeko prozesuaren berrikuspen xehatua

Network IDS

Sareko trafikoa monitorizatzen dute, jarduera susmagarria bilatzeko:

Paketeen bideratze anormala

IP spoofing: baliogabea den edo barne-tarteak erabiltzen ez dituen IP bat erabiltzea

DNS spoofing: DNS paketeen joan-etorria

Network IDS

Sareko trafikoa monitorizatzen dute, jarduera susmagarria bilatzeko:

SYN flooding: TCP SYN paketeen inbasioa

Ekipoen MAC helbide ezagunen eta IP helbideen arteko korrespondentzia faltsua

Intrusion Prevention System (IPS)

SNORT

Arrotzak detektatzeko arau berriak deskargatzeko aukera ematen du

Honeypots

"Amua" sistema, eraso diezaioten

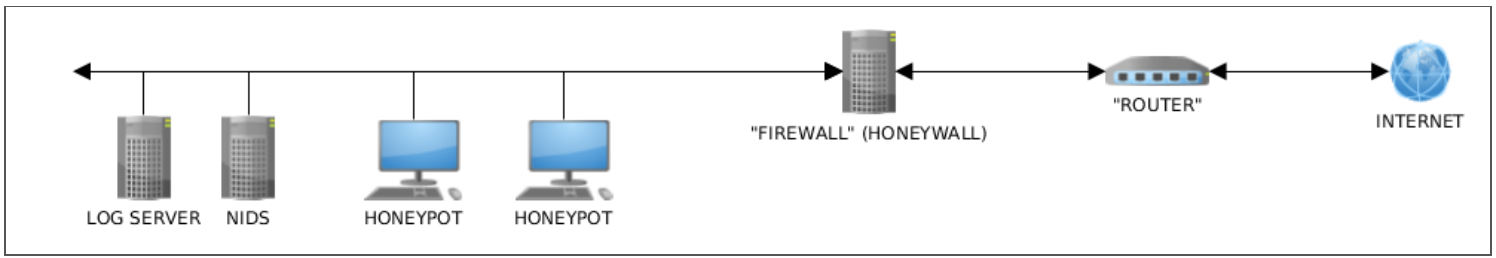
Honeynet: honeypot-en sarea

Erasoak desbideratu

Erasoei buruzko ezagutza lortzea

Malware-aren laginak lortzea

Honeypots


LOG SERVER
NIDS
HONEYPOT
HONEYPOT
"FIREWALL" (HONEYWALL)
"ROUTER"
INTERNET

Sare Birtual Pribatuak (VPN)

Segurua ez den azpiegitura erabiltzen duen sarea (Internet), barne-sare batera modu seguruan sartzeko

Barne-sarera urrutitik konektatzeko erabiltzen direnak

VPN EHU

Sare Birtual Pribatuak (VPN)

Baimentzen du:

- Erabiltzaileak, rolak eta baimenak kudeatuz autentifikatzea eta baimentzea
- **Osotasuna** hash funtzioekin
- **Konfidentzialtasuna**, informazioa enkriptazio-algoritmo baten bidez zifratuta doalako
- **Zapuztezintasuna**, datuak sinatuta transmititzen direlako

Eraso ohikoenak

Sniffing: Sarean zehar doan informazioa intertzeptatzea

Man in the middle: Informazioa intertzeptatzeaz gain, nahierara txertatu eta alda daiteke

Eraso ohikoenak

Hijacking: Sisteman baimendutako erabiltzaile bati konexioak lapurtzea

- IP Hijacking
- Session hijacking
- DNS Hijacking
- ...

Eraso ohikoenak

Spoofing (Ordezkapena)

- IP Spoofing
- MAC Spoofing
- DNS Spoofing
- ...

Eraso ohikoenak

Denial of Service (DoS): Hardwarea edo softwarea "saturatzen" da erantzuteari utzi arte

Distributed Denial of Service (DDoS):

- Hainbat makinatatik egiten da
- Batek master lanak egiten ditu eta besteak koordinatzen ditu

Eraso ohikoenak

Distributed Denial of Service (DDoS):

GitLab servers are being exploited in DDoS attacks in excess of 1 Tbps

Google mitigated the largest DDoS attack to date, peaking above 398 million rps