Universitātes nākotnes inženieri

1862

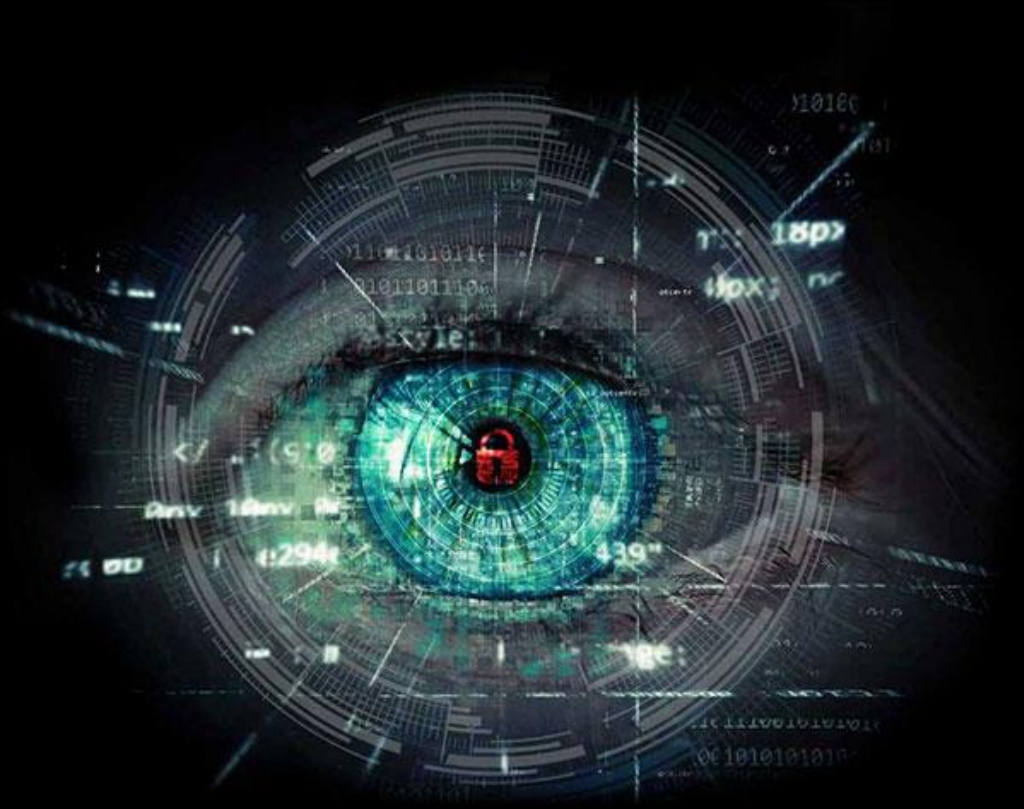
RĪGAS TEHNISKĀ UNIVERSITĀTE

«Hakeri – kā viņi veic uzbrukumus, un kā aizsargāt savu IT informāciju»

RTU lektors, Mg. Sc. Ing. Mārtiņš Bonders

18.02.2023

Lekcijas saturs



01 ➢ Kas ir «hakeri» un kāds ir viņu mērķis?

02 ➢ Kā darbojas «hakeri» un kāds ir viņu darbības algoritms

03 ➢ Kā aizsargāt savu IT informāciju no «hakeriem»?

Mg. Sc. Ing. Mārtiņš Bonders

40. gadi

- **Rīgas Tehniskās Universitātes** Informācijas Tehnoloģijas institūta **lektors** kopš 2004. gada
- Ikdienā ieņem **Chief information officer** amatu programmatūras izstrādes uzņēmumā «Luxriot»
- Specializācija – IT pārvaldība visos līmeņos, IT risinājumu arhitekts
- Pārzin IT pārvaldību, Linux, Windows operētājsistēmu administrēšanu, virtualizāciju, mākoņskaitļošanu, tīmekļa servisu pakalpojumus, IT drošības risinājumus un to aspektus
- Pirmās un vienīgās Latvijas Facebook un Linkedin datoru administrēšanas kopienas izveidotājs (200 specifiskas nozares biedri)

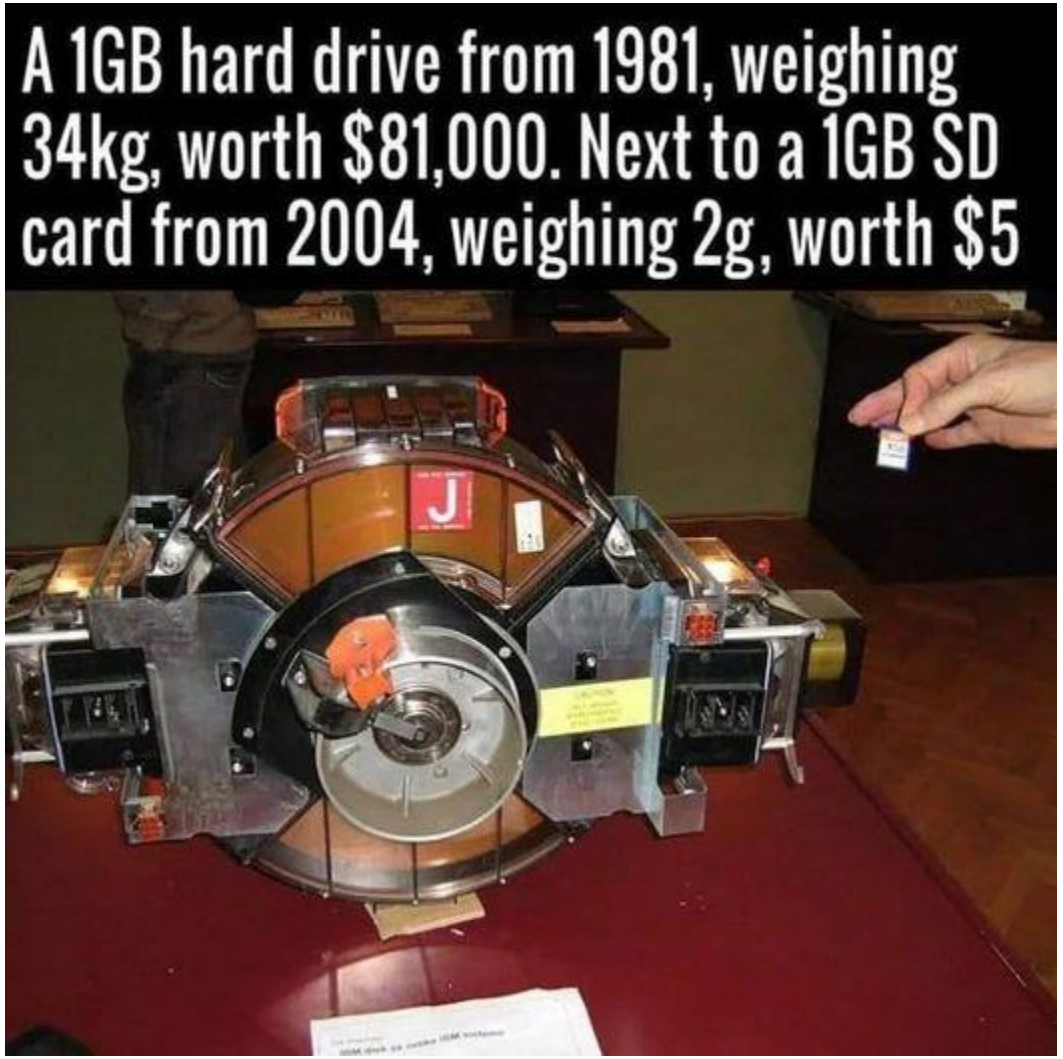
Dzīves moto: "pastāvēs, kas mainīsies", jo IT profesijā jāmācās un jāmainās ir 24/365

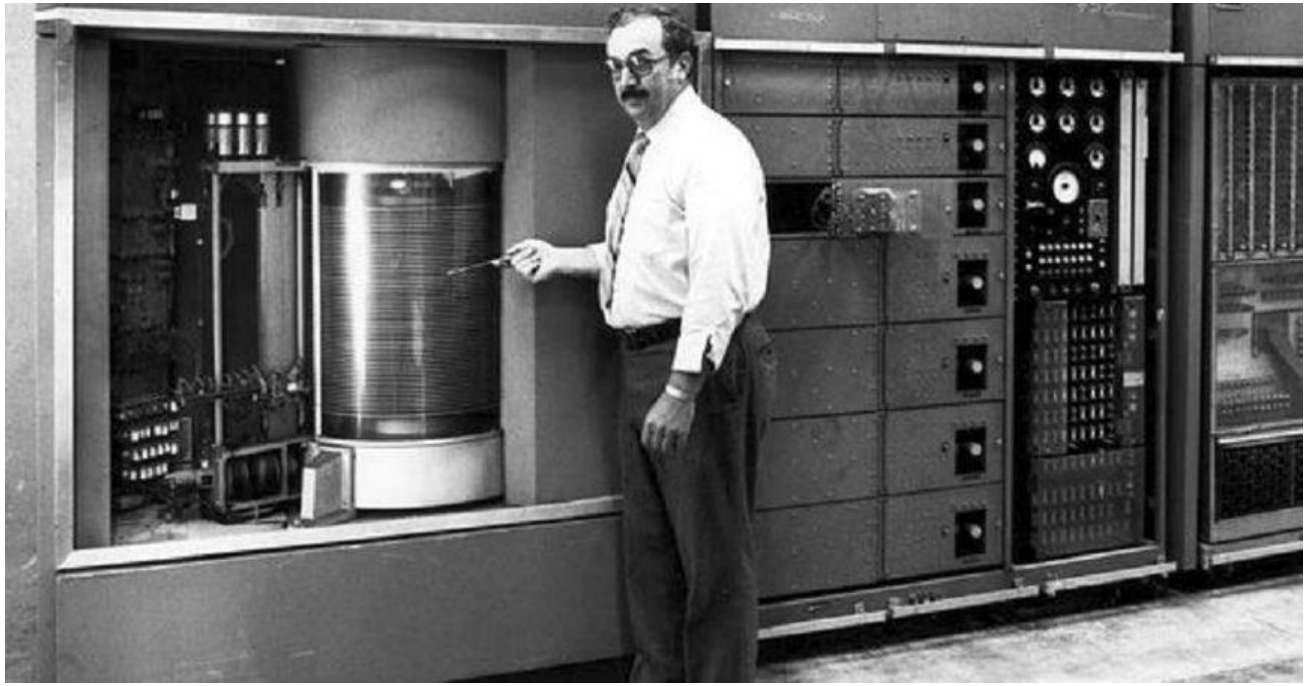
Mans pirmais dators
~ 1992 gads.

Informācija

Paroles, piekļuves dati, serveru informācija, datu atrašanās vieta, programmu versijas u.t.t.

Dati un attīstība!





1956. gads. 5MB cietais disks

2020. gads. 8388608 MB cietais disks

“Hakeris”!?

Kas ir «hakeri» un kāds ir viņu mērķis?

Definīcija: Datoru izmantošanas entuziasts, kam sagādā prieku izpētīt dažādas datoru sistēmas un atrast pieeju tajās uzglabātajai informācijai. (http://www.akadterm.lv/term.php?term=ur%C4%B7is&list=ur%C4%B7is&lang=LV) **1998.**

Definīcija: Urķis, datorlauzis jeb hakeris (angļu: hacker) ir tehniski izglītots datoru entuziasts. Hakerus var iedalīt **divās** kategorijās — urķos un datorlaužos. **Datorlauži tāpat kā urķi ir tehniski izglītoti, taču viņi savas zināšanas izmanto, lai nepilnvaroti piekļūtu aizsargātiem datiem**, bet urķiem šāda nodarbe var būt **vaļasprieks**. (https://lv.wikipedia.org/wiki/Ur%C4%B7is)

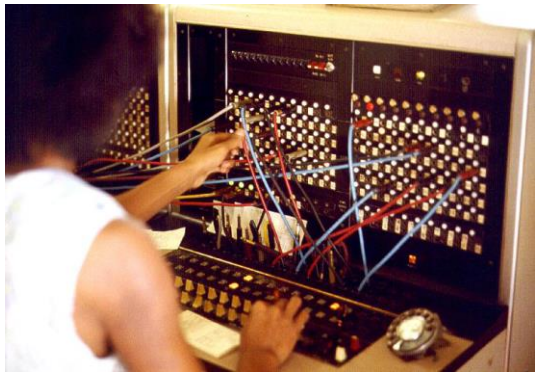
- ❑ Kredītkartes dati, finanšu noziegumi
- ❑ Serveru pārņemšana
- ❑ Serveru atteice
- ❑ Lietotāja vārdi + paroles
- ❑ Kontroles pārņemšana
- ❑ Vandālisms
- ❑ Špionāža

“Hakeris”!?

Who was the first hacker in history?

John Draper, also known as Captain Crunch, is often named as the first ever hacker. And rather than having lots of high-tech hacking tools at his disposal, he managed to do it all with a toy whistle from a cereal packet. Here’s how:

Back in the early 1970s, the largest computer network accessible to the general public was the telephone system. And at the time, telephones were managed by an automated system that used specific analogue frequencies to place calls. Draper managed to exploit this using a toy whistle that came free in boxes of Cap’n Crunch cereal (hence the nickname). He would use this to make free long distance and international calls. This technique was known as “Phreaking”.



The first internet hacker

One of the first internet hackers, and certainly the first to gain mainstream media attention, was Robert Morris back in 1989. His was the first “Denial of service” attack in history and it was caused by a worm Morris had developed at Cornell University the year before.

According to Morris, he didn’t intend to cause any harm, but rather to highlight security flaws. But unfortunately, due to a fault in the code, the worm replicated excessively, causing extensive damage that lasted for days.

https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/

Kas notiek pasaulē?

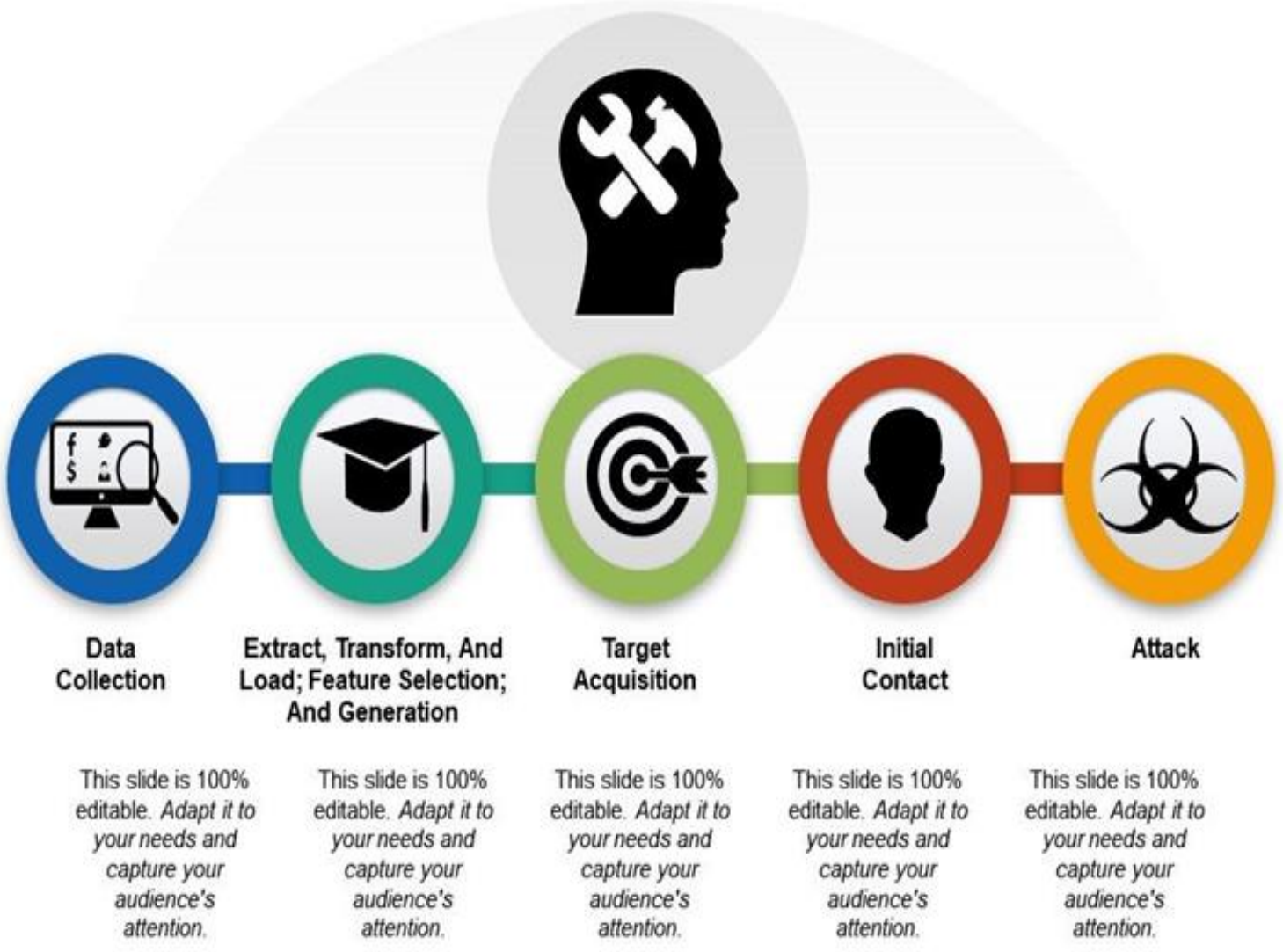
Katru sekundi notiek miljoniem mēģinājumu kompromitēt, uzlauzt vai kā citādi ierobežot kāda servisa darbību. 80% no šī darba veic «automatizēti boti/roboti».

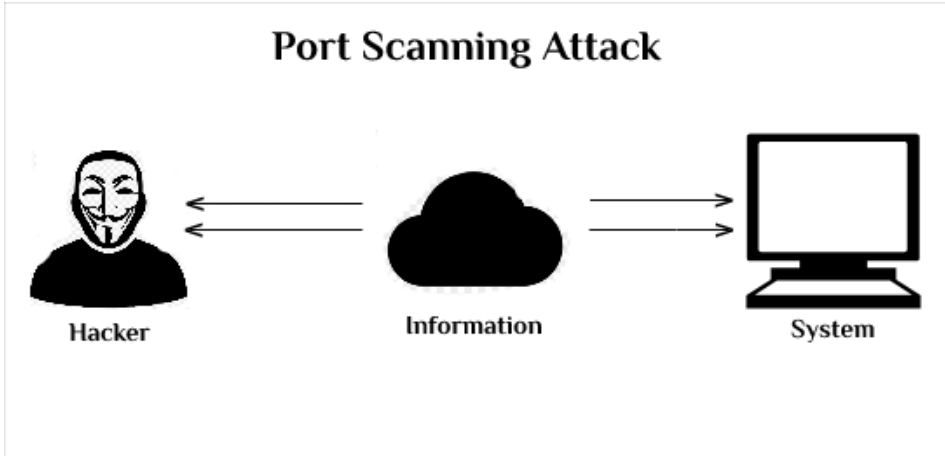
Tiešsaistes informācija

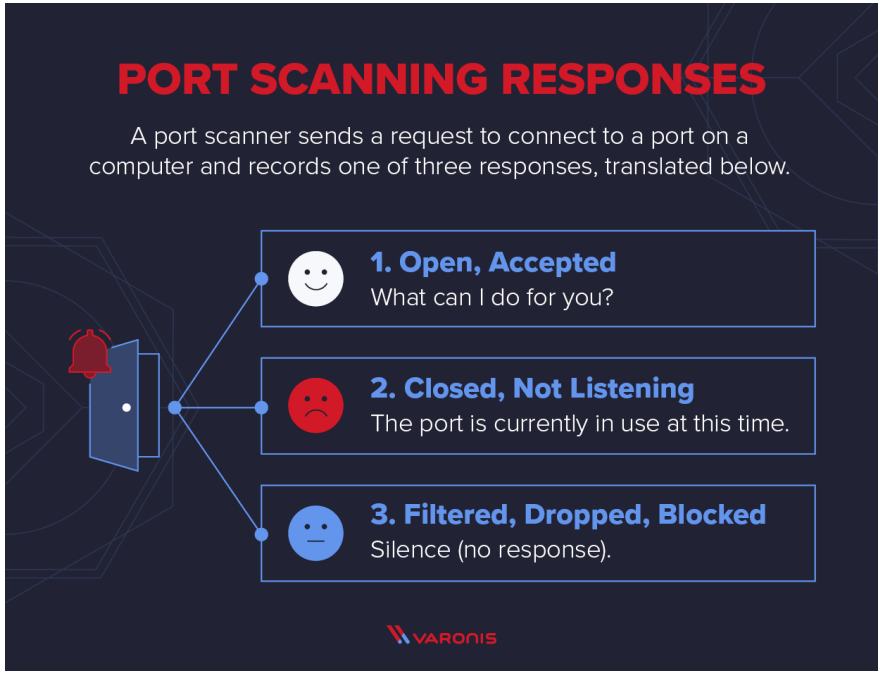
1. Fortinet Threat Map (fortiguard.com)
2. Live Cyber Threat Map | Check Point
3. Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
4. Digital Attack Map

1. https://haveibeenpwned.com
2. Shodan Search Engine
3. Censys Search

Hakera darbības algortims







Ubrukumu var veikt «visam»!

WikiLeaks says CIA hacked Samsung smart TVs

30 Comments / f Share / Tweet / Stumble / Email

Last Updated Mar 8, 2017 11:12 AM EST

WikiLeaks says Samsung smart TVs were hacked to enable spying on consumers.

In a trove of documents released Tuesday, WikiLeaks included code that it says shows the CIA worked with U.K. intelligence officials to turn microphones in TVs into listening devices.

Samsung smart TVs have microphones so viewers can make voice commands, such as requests for movie recommendations. The commands typically aren't transmitted outside the home unless users activate the feature. If the TV is off, there's no listening being done.

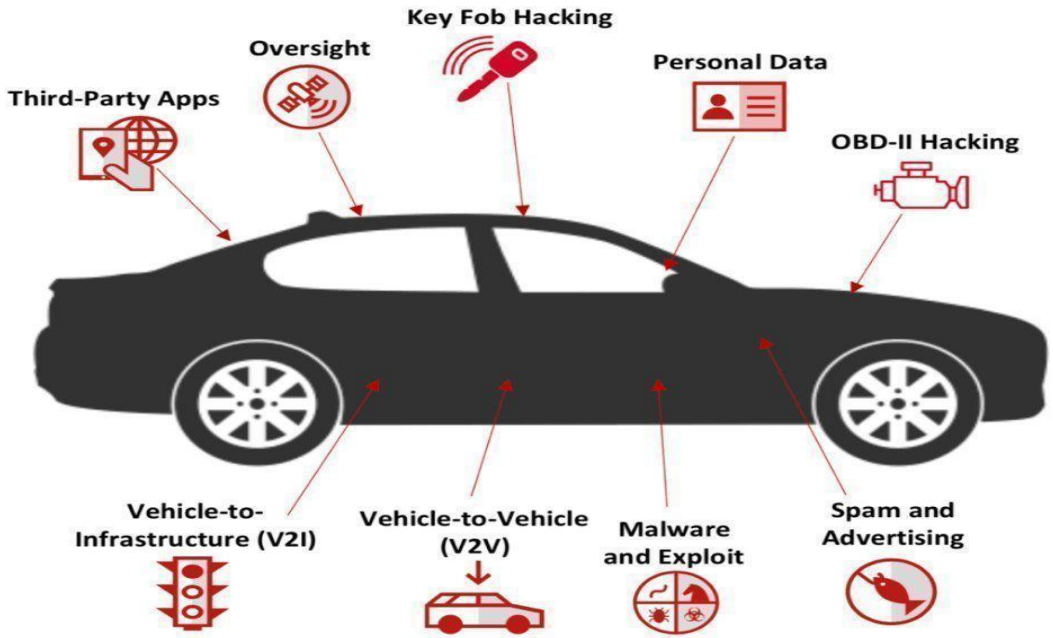
Play VIDEO

WikiLeaks releases documents on CIA hacking

But WikiLeaks claims that documents it obtained show that through a program called Weeping Angel, the target TV appears to be off when it is actually on -- and listening.

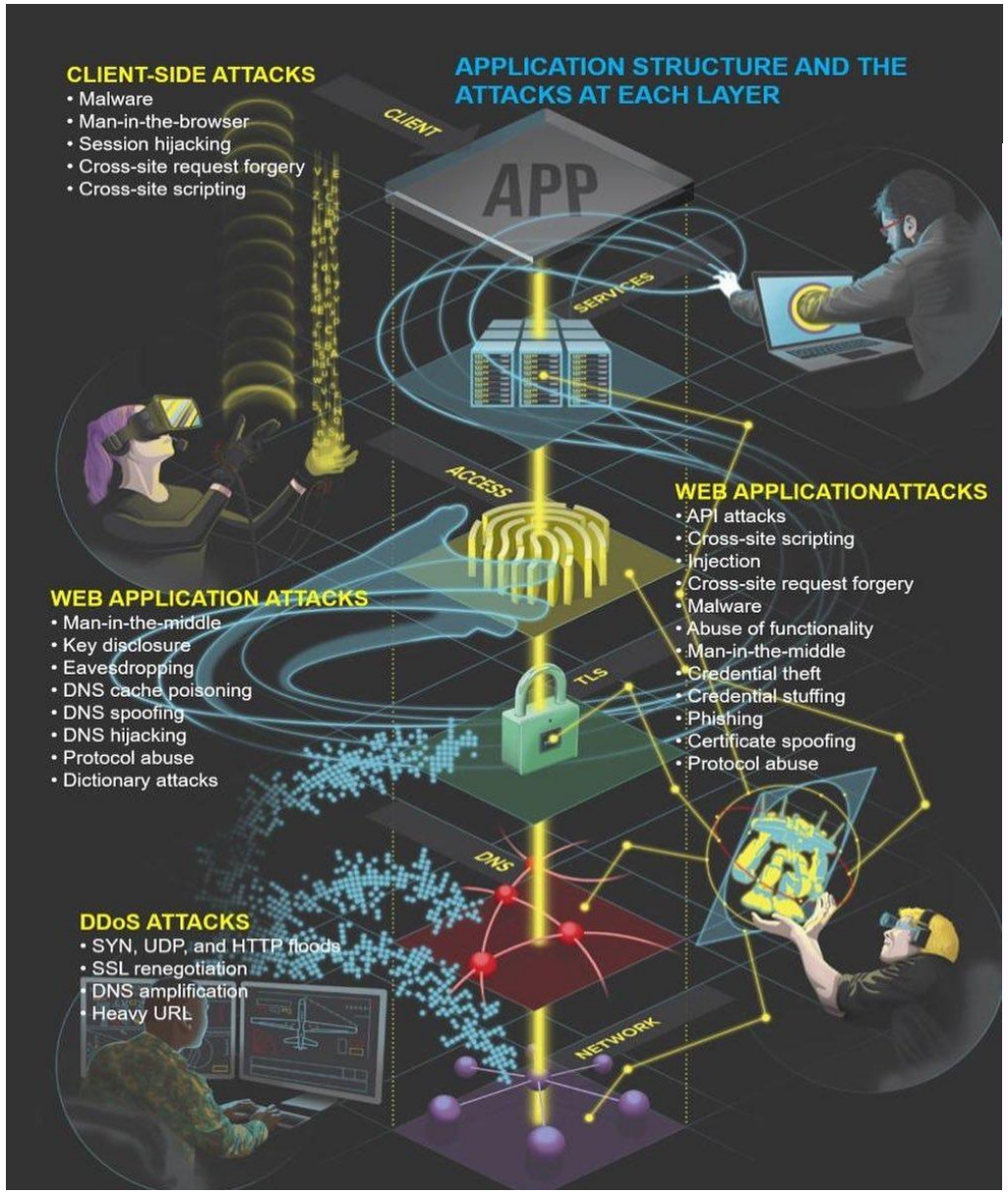
WikiLeaks says the audio goes to a covert CIA server rather than a party authorized by Samsung. In such cases, audio isn't limited to TV commands but could include everyday

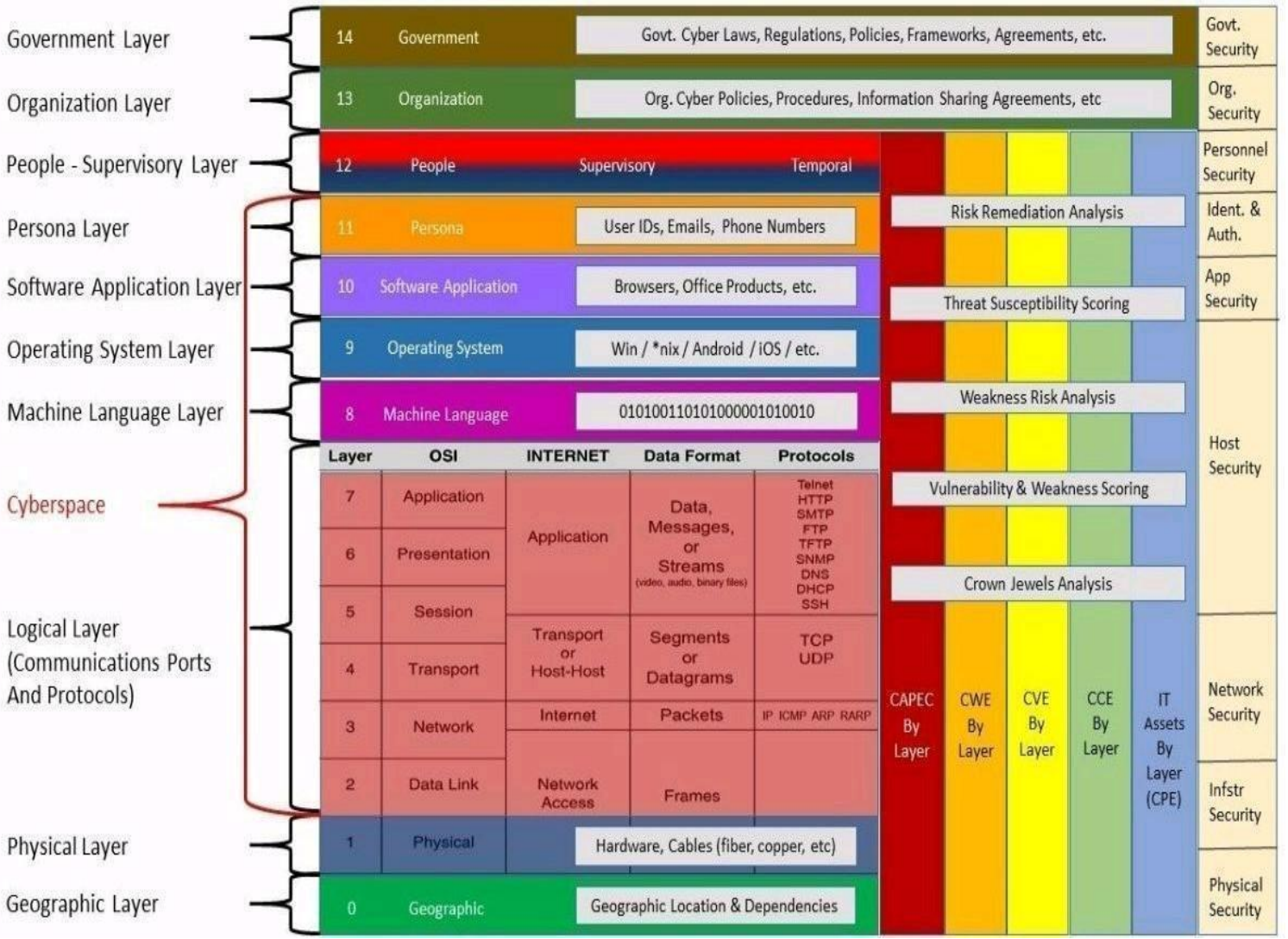
Major Modern Cars Security Risk



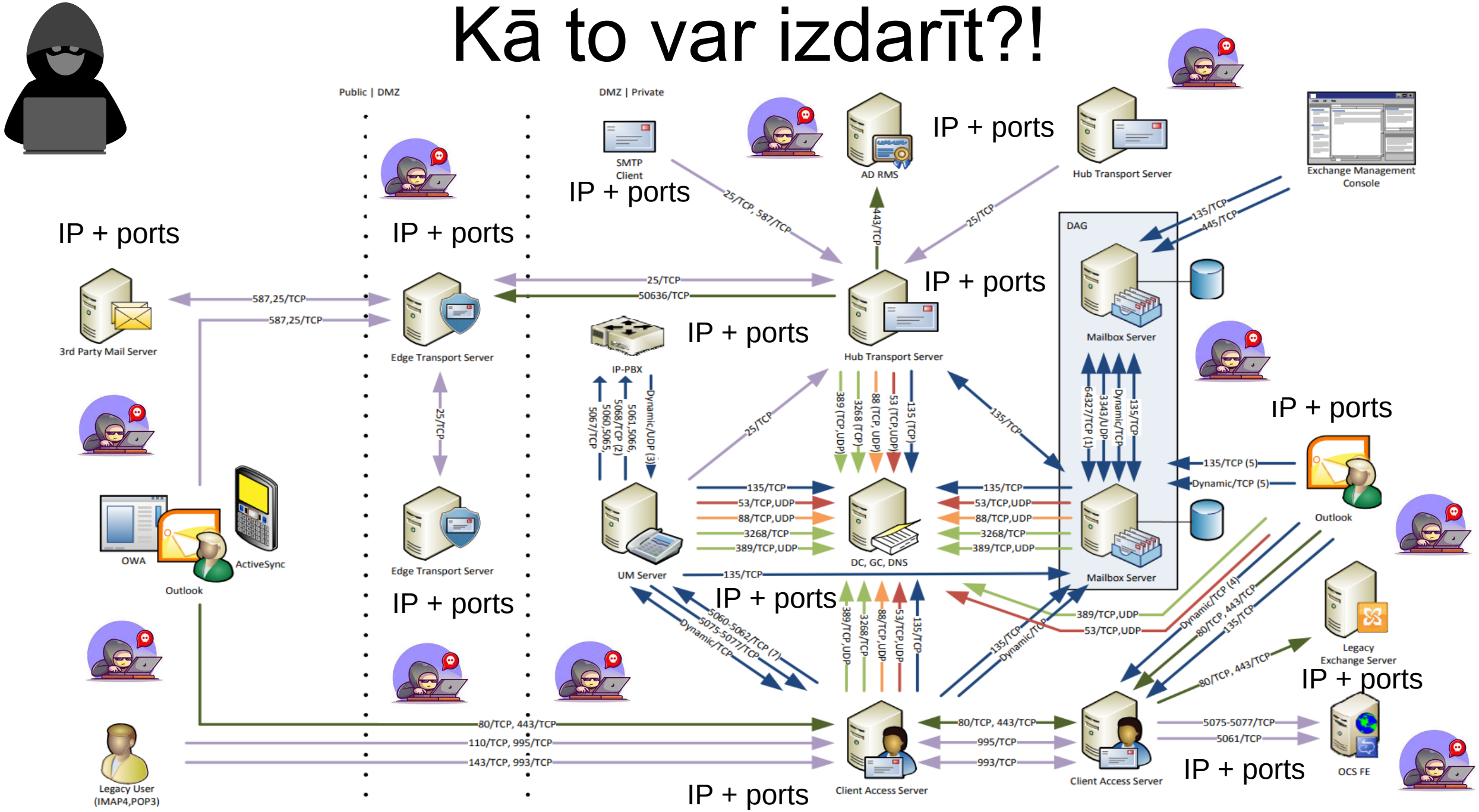
Viss, kas ir pieslēgts datortīklam, ir jaaizsargā. Visu, kam ir IP adrese, var «uzlauzt».

Kā to var izdarīt?!





Kā to var izdarīt?!



Hakeri ir informēti!

Common Ports

packetlife.

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Serve
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFu
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbo
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		

Legend

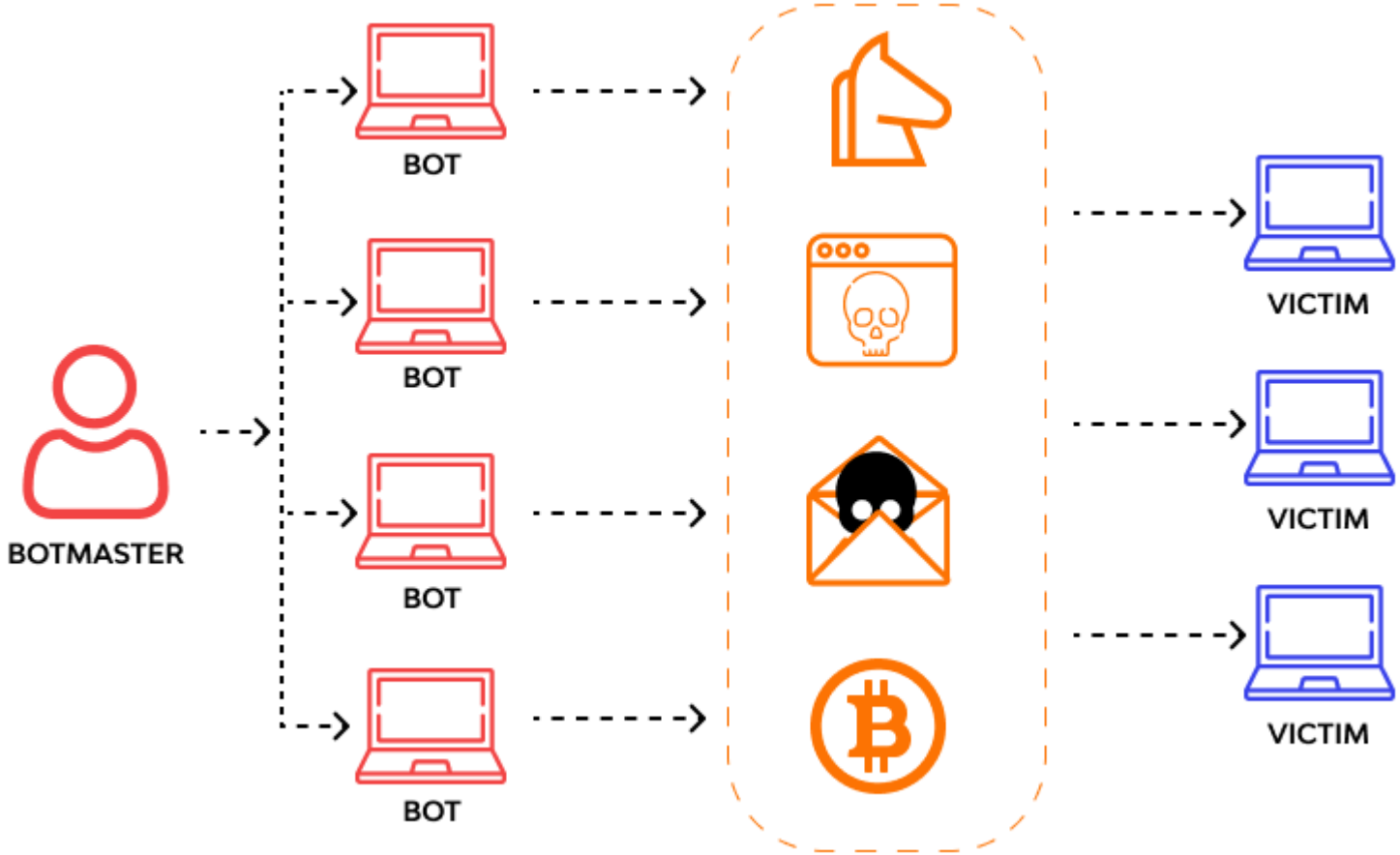
- Chat
- Encrypted
- Gaming

Port	Request type
7	ECHO
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
37	Time
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
79	Finger
80	HTTP
110	POP3
115	Simple File Transfer Protocol (SFTP)
137	NetBIOS Name Service
139	NetBIOS Datagram Service
143	Interim Mail Access Protocol (IMAP)
156	SQL Server
161	SNMP
194	Internet Relay Chat (IRC)
389	Lightweight Directory Access Protocol (LDAP)
443	HTTPS
445	Microsoft-DS
458	Apple QuickTime
546	DHCP Client
547	DHCP Server

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

“ Botnet” ideja

Botnets ir tīkli, kas sastāv no tālvadības datoriem vai "robotprogrammatūras". Šie datori ir inficēti ar ļaunprātīgu programmatūru, kas ļauj tos attālināti vadīt. Daži robottīklu tīkli sastāv no simtiem tūkstošu vai pat miljonu datoru.



Kur dzīvo hakeri?

Tumšs tīmeklis (Dark Net/Web) ir termins, kas attiecas uz noteiktu **tīmekļa vietņu grupu**, kas atrodas **šifrētā tīkla telpā**.

Gandrīz visas Darknet vai Dark Web vietas slēpj īpašnieka personas datus, izmantojot Tor šifrēšanas rīkus. *Daļa ēnu interneta lietotāju ir militārās, valdības un tiesībaizsardzības organizācijas. Viņi izmanto Darknet, lai saglabātu atrašanās vietas un informācijas konfidencialitāti.*

Darknet ir arī populārs žurnālistiem, emuāru autoriem, aktīvistiem un sabiedriskajiem darbiniekiem, kuri baidās no politiskas vajāšanas, bet vēlas pēc sensacionālas politiskās izlūkošanas. *Ēnu internets ir īpaši populārs valstīs ar totalitāru režīmu un stingru cenzūru.*

Darknet valūta nav dolārs vai eiro. Tā ir Bitcoin!

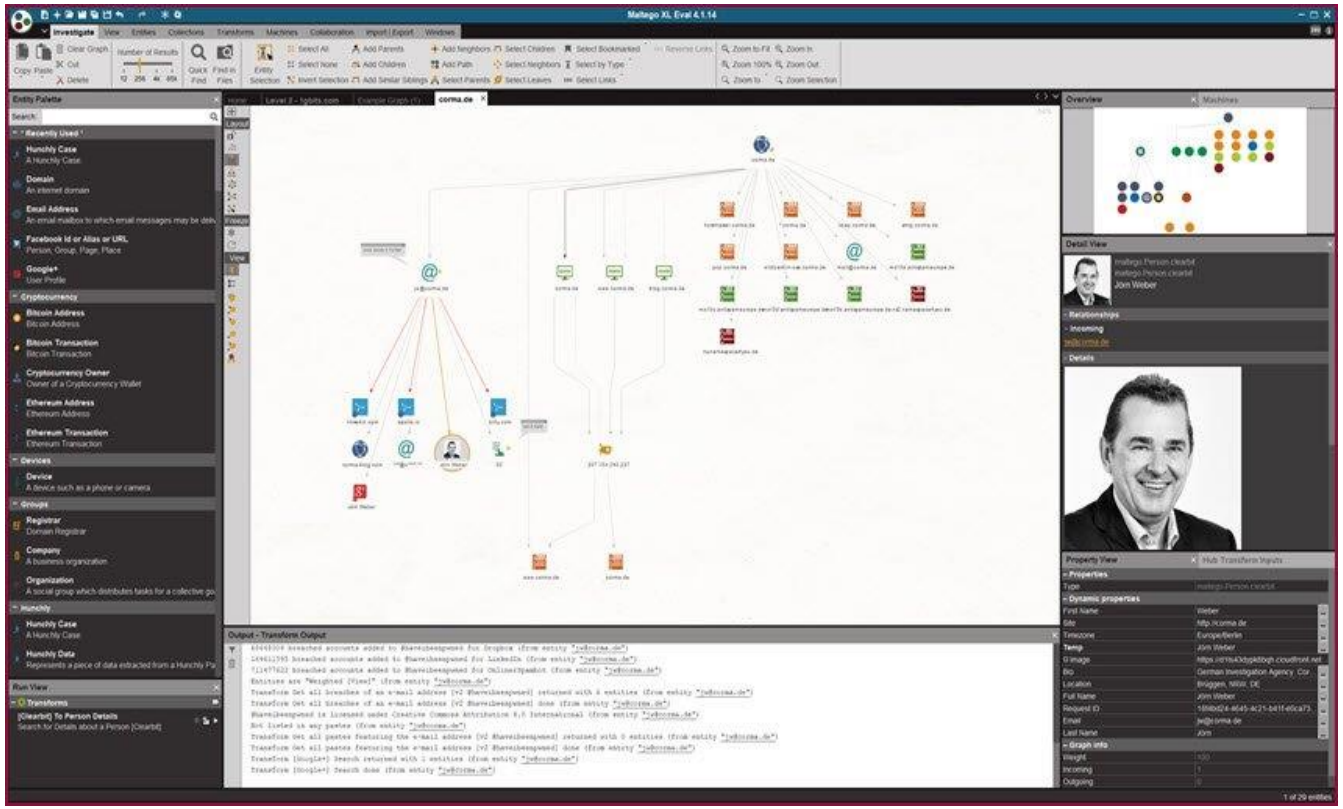
https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html

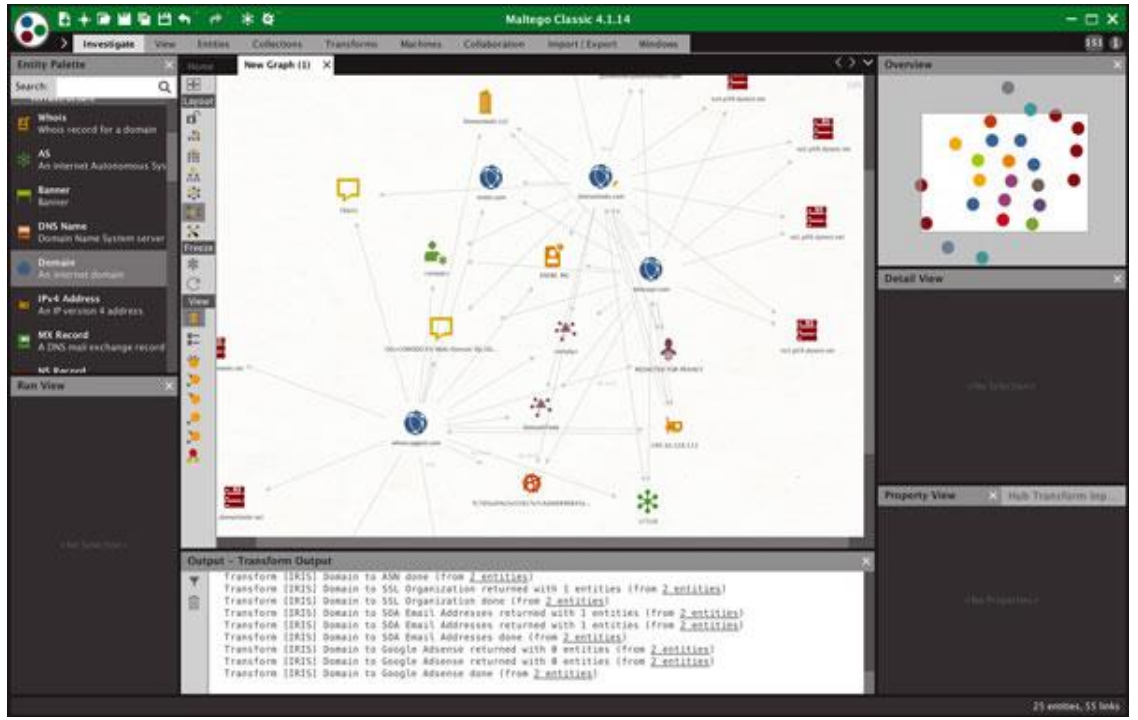
https://vpnoverview.com/privacy/anonymous-browsing/dark-web-websites-worth-visiting/

Hakeri ir labi ekipēti!

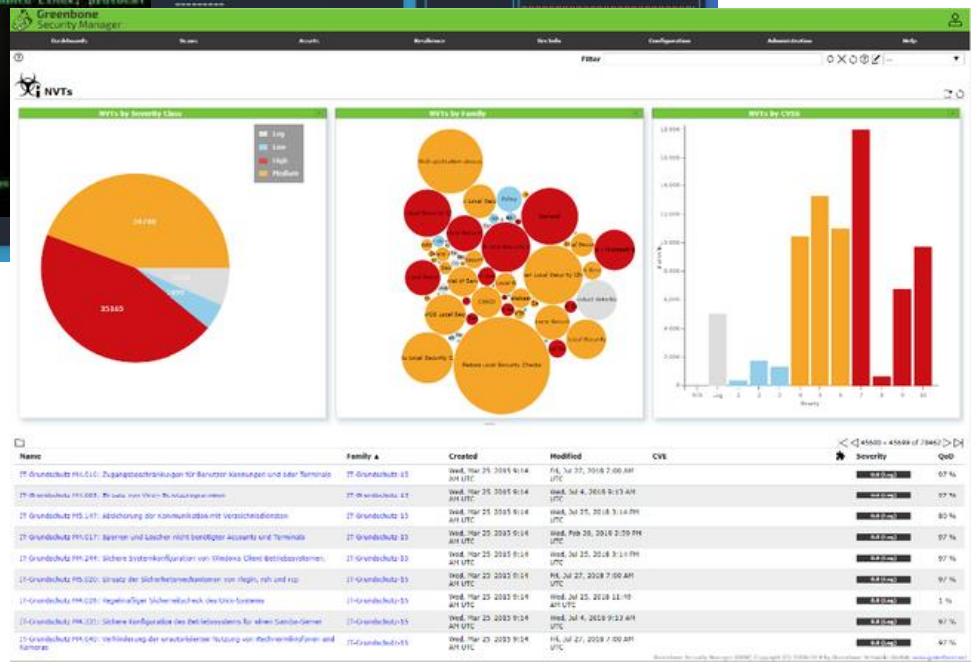
Mūsdienās praktiski visi interneta lietotāji atstāj savas **digitālās pēdas vai nospiedumus**. Šo nospiedumu «pētniekiem» ir pieejami daudz rīki, kuri **automatizē** datu savākšanu no viss dažādākajiem datu avotiem. Sākot ar e-pastu un beidzot ar dzīvesvietas adresi un īpašumā esošo kaķu šķirni.

Kali linux OS rīks **Maltego,** ir viens no populārākajiem **sociālās inženierijas** rīkiem, kurš automatizēti var ievākt informāciju par **personas vai personas grupas datiem**. Tas parāda **attiecības/saistību starp cilvēkiem, sociālajiem tīkliem, organizācijām, vietnēm, domēniem, DNS nosaukumiem, IP adresēm, saistībām, dokumentiem, attēliem, failiem u.c. digitālajām pēdām.**





Hakeri ir labi ekipēti!



- **Kali Linux**
- **Parrot Linux**
- **NMAP**
- **OpenVAS**
- **u.t.t.**

Penetration Testing tools

There are various tools that an Ethical Hacker or Penetration Tester could utilize to do the test. Some of the popular tools used in penetration testing are

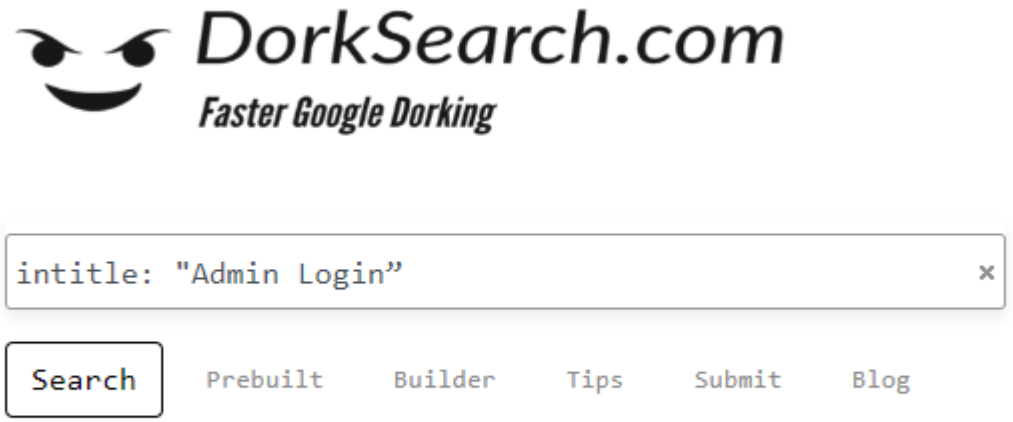
Nmap
Metasploit
Kali Linux
Wireshark
Netsparker
Astra
John the Ripper
Sqlmap
Burp Suite
Nessus
w3af
Acunetix
Aircrack-ng
Retina
Hydra

Hakeri ir labi ekipēti!

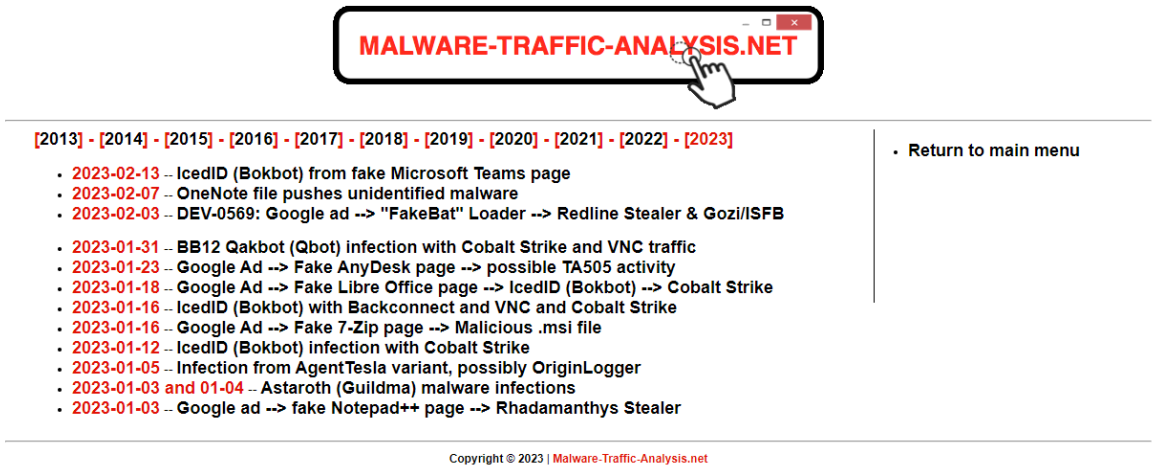
https://dorksearch.com/
intitle: "Admin Login”
https://www.yeahhub.com/top-8-basic-google-search-dorks-live-examples/

Top 17 OSINT tools to find anyone online – 2023

https://usersearch.org/updates/2022/04/10/top-16-open-source-intelligence-tools-ever-made-osint/



https://www.malware-traffic-analysis.net/

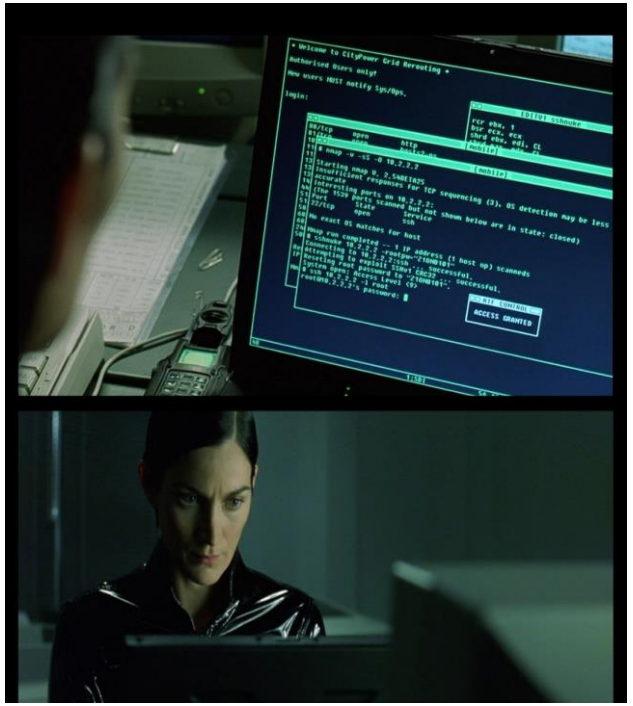


Jautājumi?

Praktiskais piemērs

Piemērā izmantotie rīki ir bezmaksas, brīvi pieejami tīmeklī un izmantojami tikai un vienīgi savas IT infrastruktūras drošībai pārbaudei un uzlabošanai!

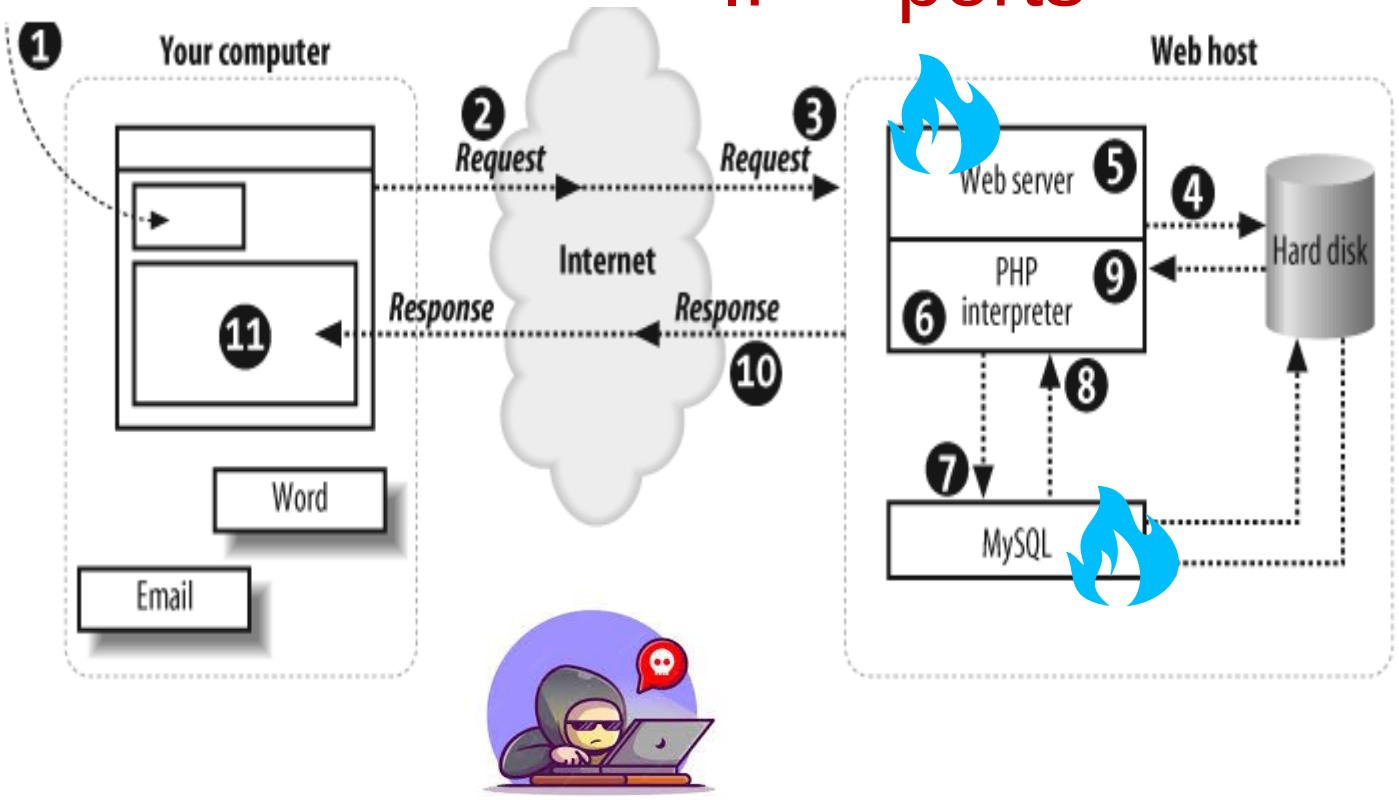
Šos rīkus ir aizliegts izmantot ļaunprātīgiem mērķiem! Par šo rīcību draud krimināllatbildība.

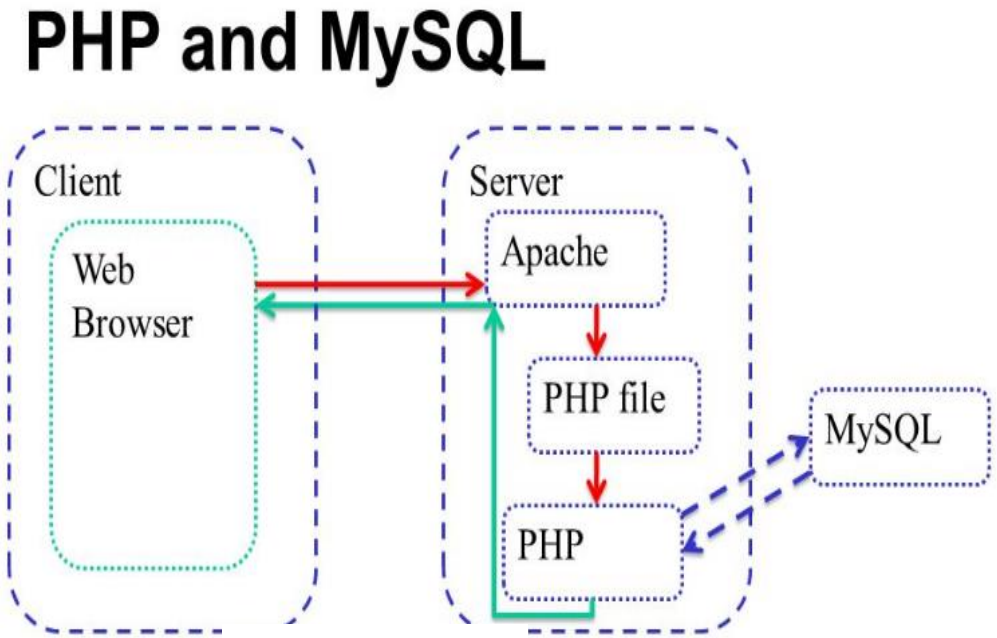


1. https://haveibeenpwned.com
2. Shodan Search Engine
3. Censys Search

Praktiskais piemērs

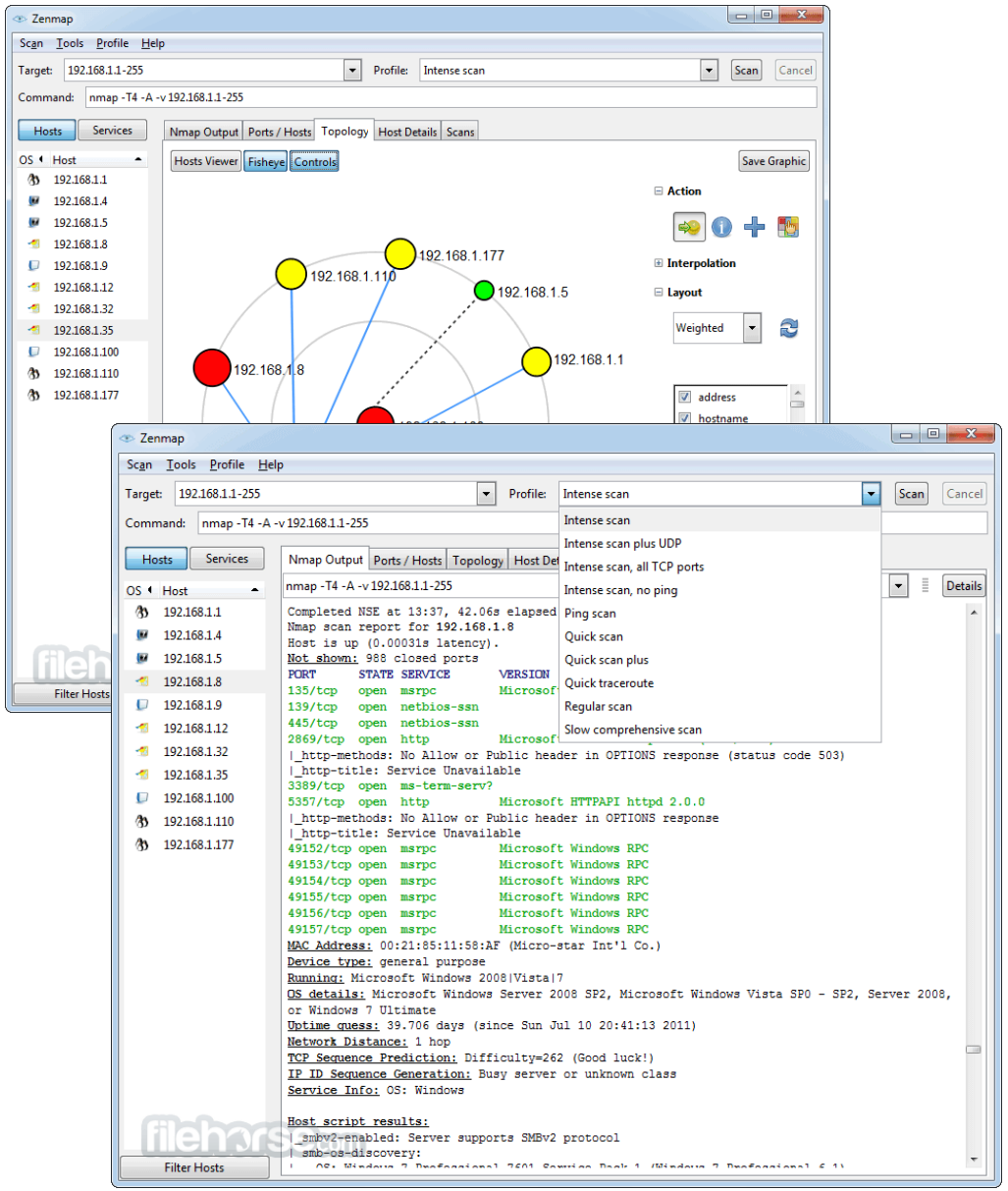
IP + ports





IP + ports

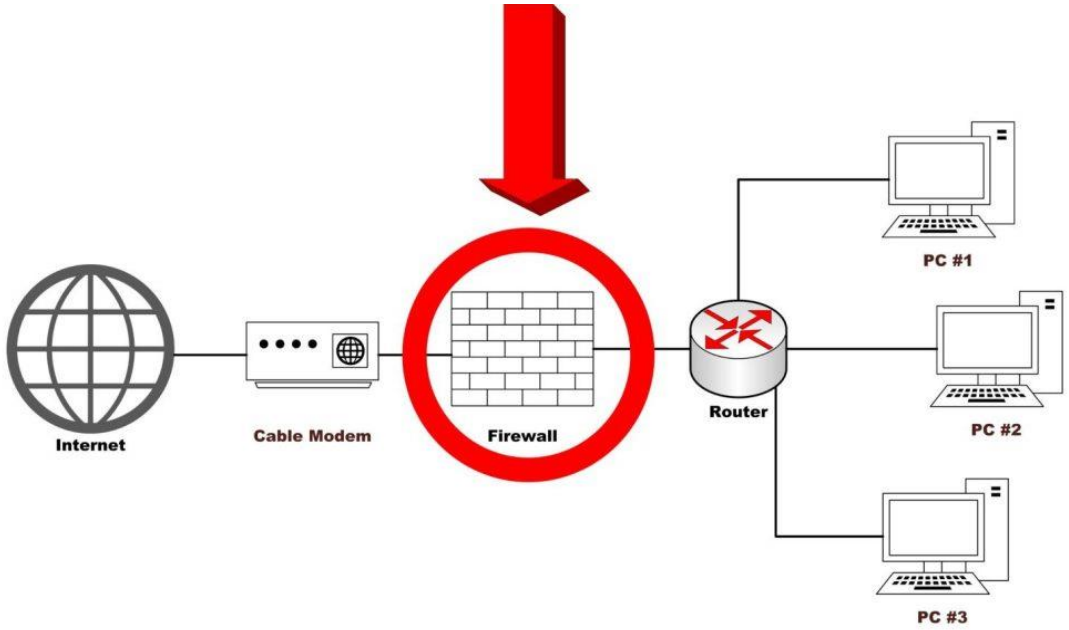
Praktiskais piemērs



Name	Familie	Erstellt	Geändert	Version	CVE	Schwereg.	QdE
Fedora Update for mingw-libpng FEDORA-2015-8	Fedora Local Security Checks	Sun Nov 29 2015	Mon Nov 30 2015	$Revision: 2177 $	CVE-2015-8126	7.5	97%
Fedora Update for mingw-libpng FEDORA-2015-97	Fedora Local Security Checks	Sat Nov 28 2015	Mon Nov 30 2015	$Revision: 2177 $	CVE-2015-8126	7.5	97%
Fedora Update for seamonkey FEDORA-2015-8	Fedora Local Security Checks	Sat Nov 28 2015	Mon Nov 30 2015	$Revision: 2177 $		10.0	97%
Fedora Update for python-pycurl FEDORA-2015-0	Fedora Local Security Checks	Sat Nov 28 2015	Mon Nov 30 2015	$Revision: 2177 $		10.0	97%
Mageia Linux Local Check: mgasa-2015-0455	Mageia Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2164 $	CVE-2015-7805	9.3	97%
Mageia Linux Local Check: mgasa-2015-0457	Mageia Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2164 $	CVE-2015-5312 CVE-2015-7497 CVE-2015-7498 CVE-2015-7499 CVE-2015-7500 CVE-2015-8241 CVE-2015-8242 CVE-2015-8317	10.0	97%
Mageia Linux Local Check: mgasa-2015-0459	Mageia Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2164 $	CVE-2014-8240 CVE-2014-8241	7.5	97%
Oracle Linux Local Check: ELSA-2015-2172	Oracle Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2163 $	CVE-2015-5277	10.0	97%
Oracle Linux Local Check: ELSA-2015-2505	Oracle Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2163 $	CVE-2015-5273 CVE-2015-5287 CVE-2015-5302	10.0	97%
Oracle Linux Local Check: ELSA-2015-2519	Oracle Linux Local Security Checks	Fri Nov 27 2015	Fri Nov 27 2015	$Revision: 2163 $	CVE-2015-7199 CVE-2015-7200 CVE-2015-4513 CVE-2015-7189 CVE-2015-7193 CVE-2015-7197 CVE-2015-7198	7.5	97%

Kā aizsargāt savu IT «kopu»?

Ugunsmūru (firewall) mērķis – aizsargāt tīklu, kontrolējot datu plūsmu saskaņā ar noteikumiem. Tā ir drošības sistēma, kas paredz speciāli programmēta datora/iekārtas ievietošanu **starp organizācijas/mājas lokālo datoru tīklu un Internetu.** Ugunsmūris aizsargā šo lokālo tīklu no nesankcionētas interneta tīkla lietotāju piekļuves un lokālā tīkla lietotājus no piekļūšanas «ļauniem» resursiem.



Ir jāievēro šādi nosacījumi:

- Visai datu plūsmai, kas ienāk lokālā tīklā, jāiet caur ugunsmūri;
- Visai datu plūsmai, kas iziet no lokālā tīkla, jāiet caur ugunsmūri;
- Ugunsmūris nodrošina aizsardzības nosacījumus un bloķē tiem neatbilstošus datus
- Ugunsmūris pats nepakļaujas uzlaušanas mēģinājumiem

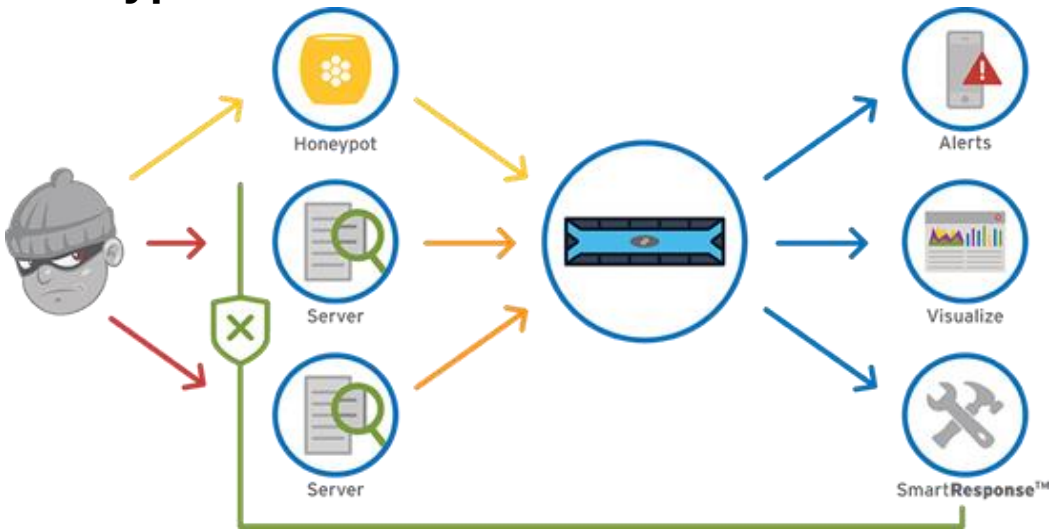
Ugunsmūra populārākās iespējas:

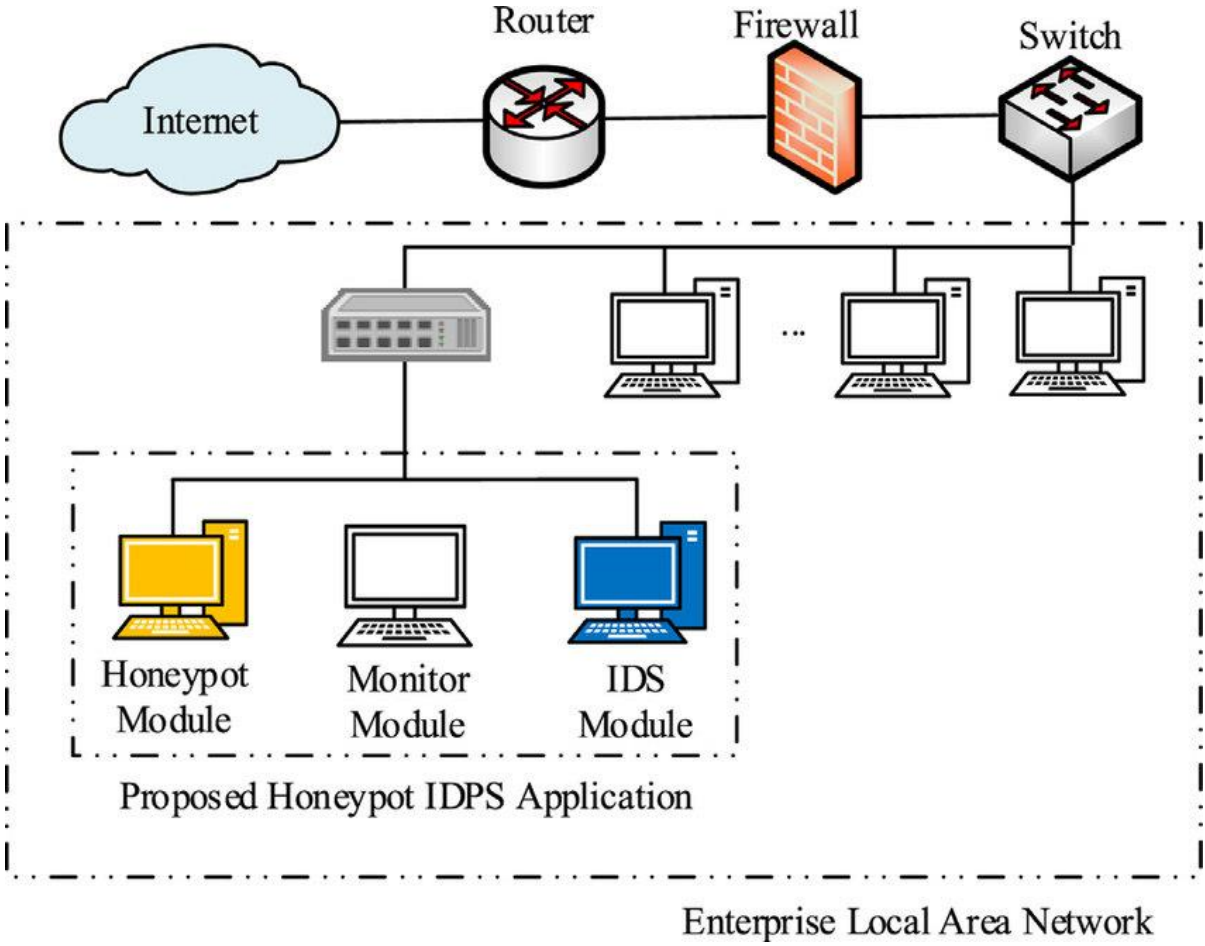
- Piekļuves filtrēšana neaizsargātiem servisiem;
- Aizsargā pret slēgtas informācijas iegūšanu no aizsargātā apakštīkla, kā arī viltus datu ievietošanu šajā apakštīklā ar neaizsargātu servisu palīdzību;
- Piekļuves tiesību kontrole tīkla mezgliem;
- Iespēja reģistrēt visus mēģinājumus iegūt piekļuvi, kā no ārējā, tā arī no iekšējā tīkla, kas ļauj veikt uzskaiti/auditu;
- Reglamentēt kārtību kādā iespējams iegūt piekļuvi tīklam;
- Paziņot par aizdomīgām darbībām, mēģinājumiem zondēt vai uzbrukt tīkla mezgliem vai pašam ugunsmūrim.

Kā aizsargāt savu IT «kopu»?

Medus pods (honeypot) izskatās kā **īsta** datorsistēma ar lietojumprogrammām un datiem, **maldinot kibernoziedzniekus**, liekot domāt, ka tas ir **produkcijas serveris/serviss**.

Piemēram, medus pods varētu imitēt uzņēmuma klientu norēķinu sistēmu - bieži uzbrukuma mērķi noziedzniekiem, kuri vēlas atrast kredītkaršu numurus. Pēc hakeru ienākšanas viņus var **izsekot un novērtēt** viņu uzvedību, lai uzzinātu, kā reālo tīklu padarīt drošāku. To uzraugu un analizē speciāla programmatūra. **IR ļoti svarīgi pareizi un efektīvi uzraudzīt un pārvaldīt savu «Honeypot».**





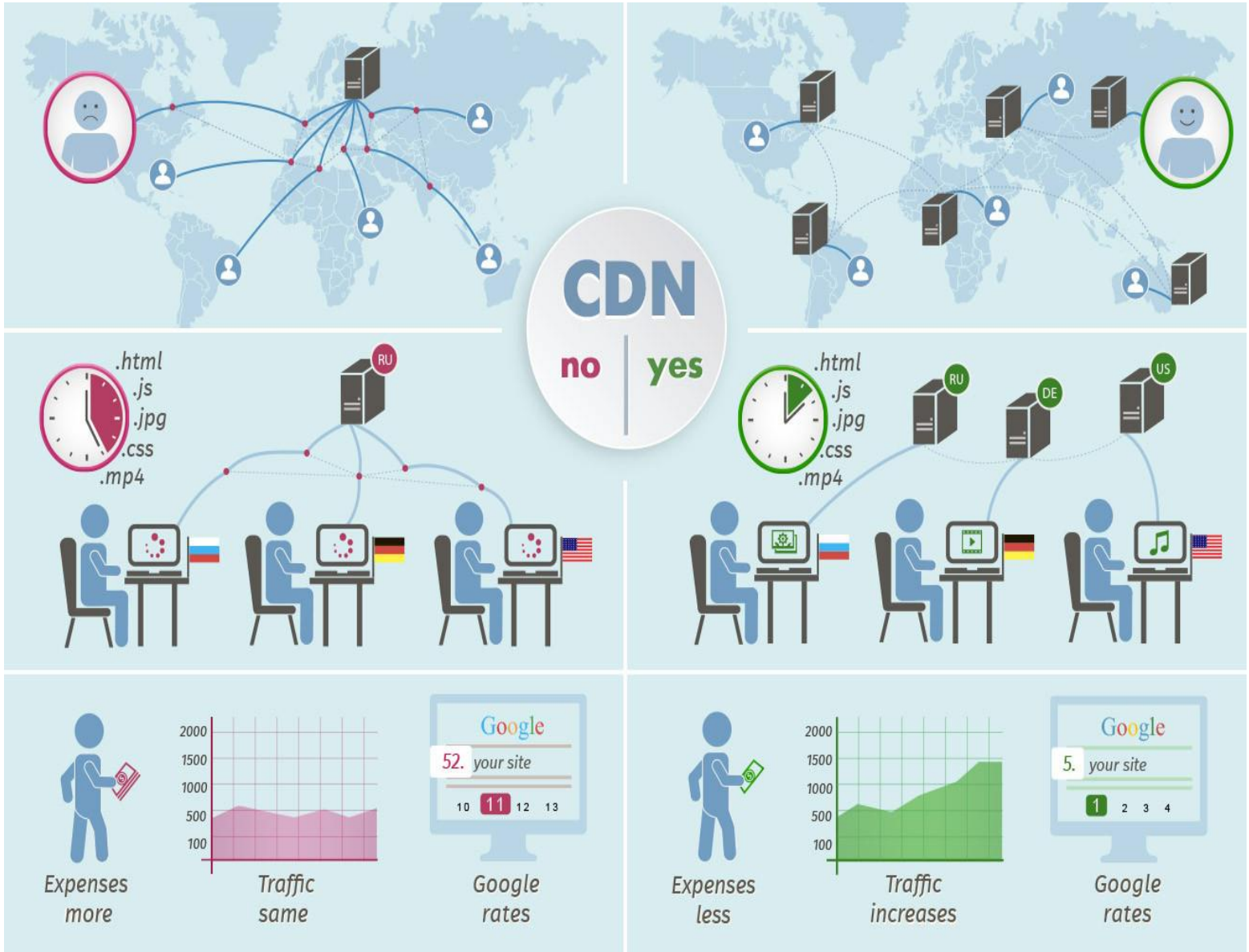
Kā aizsargāt savu IT «kopu»?

Satura piegādes tīkls (CDN) attiecas uz ģeogrāfiski sadalītu serveru grupu, kas darbojas kopā, lai nodrošinātu **ātru un drošu interneta satura piegādi.**

CDN ļauj ātri pārsūtīt datus, kas nepieciešami, lai ielādētu interneta vietnes saturu, tostarp HTML lapas, javascript failus, stila datus, attēlus un videoklipus.

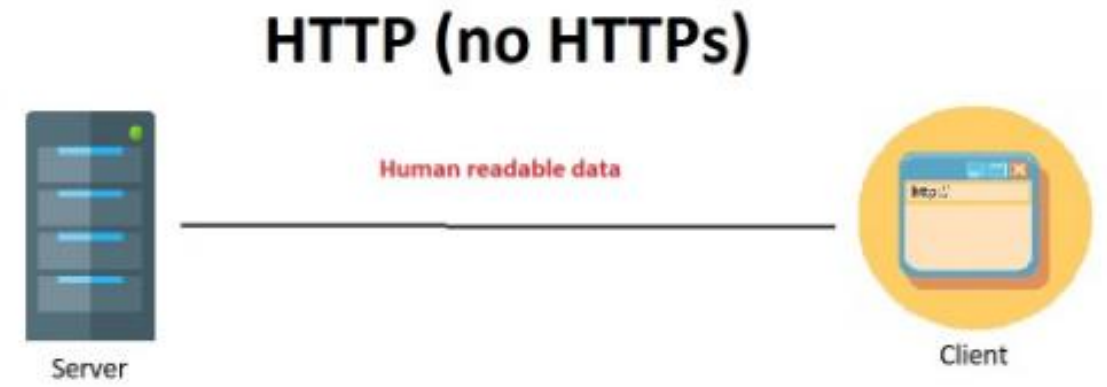
CDN pakalpojumu popularitāte turpina pieaugt un šodien lielākā daļa tīmekļa plūsmas tiek apkalpota izmantojot **tuvāko CDN**, ieskaitot plūsmu no tādām vietnēm kā Facebook, Netflix un Amazon.

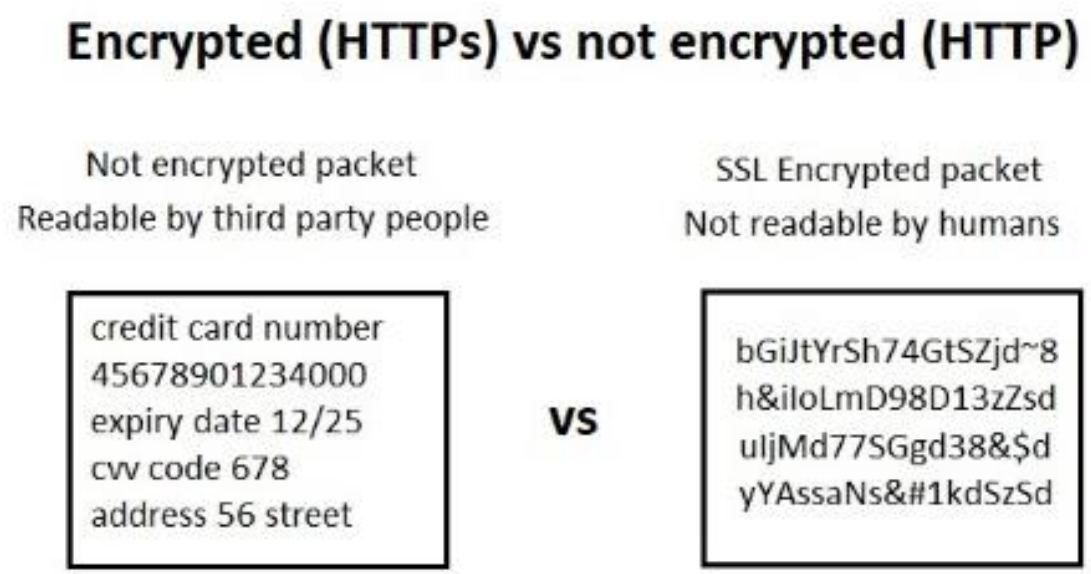
CDN tur kešatmiņā vietnes tīmekļa datus (vai nu iepriekš, vai pēc sākotnēja pieprasījuma). Tādā veidā lietotājiem **nav jāiegūst** tīmekļa saturs **no izcelsmes servera**, jo tas var aizņemt laiku. **CDN ļoti palielina DDoS aizsardzību**, jo DDoS drošības pasākumi ir sarežģīti integrēti CDN pakalpojumos.

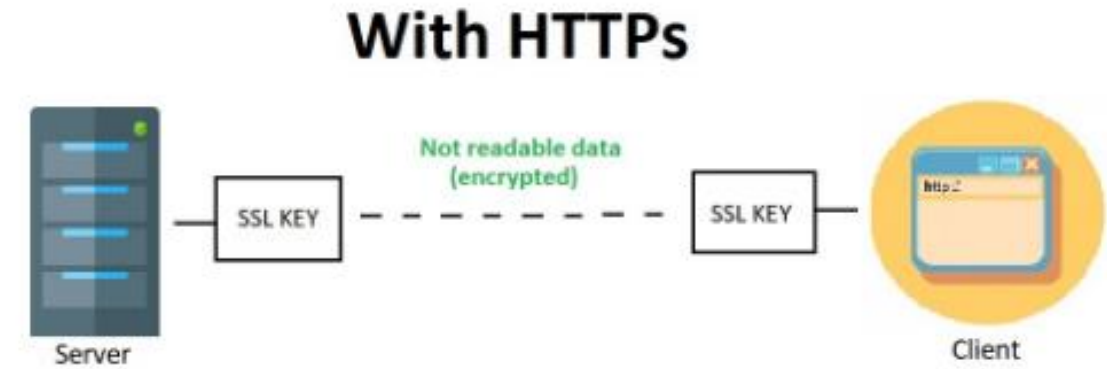


Kā aizsargāt savu IT «kopu»?

Gan **HTTP**, gan **HTTPS** serveri var darboties pielāgotos portos.
Pēc noklusējuma **HTTP** izmanto **80** un **HTTPS 443** portu.
Tīmekļa serveri var darboties 8080 portā, atkarībā no lietojumprogrammas, portus var brīvi izvēlēties.





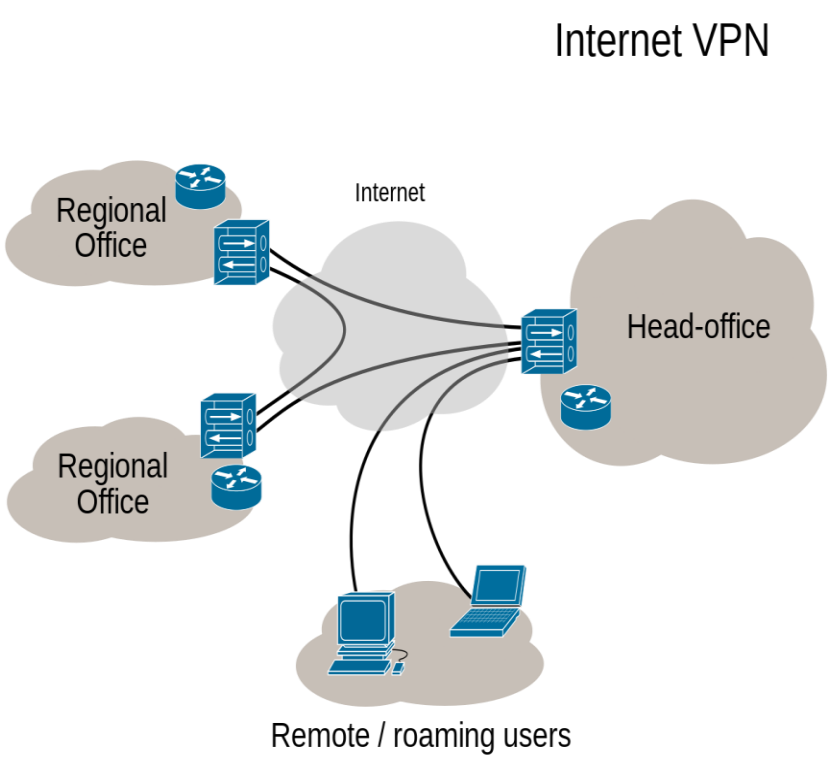


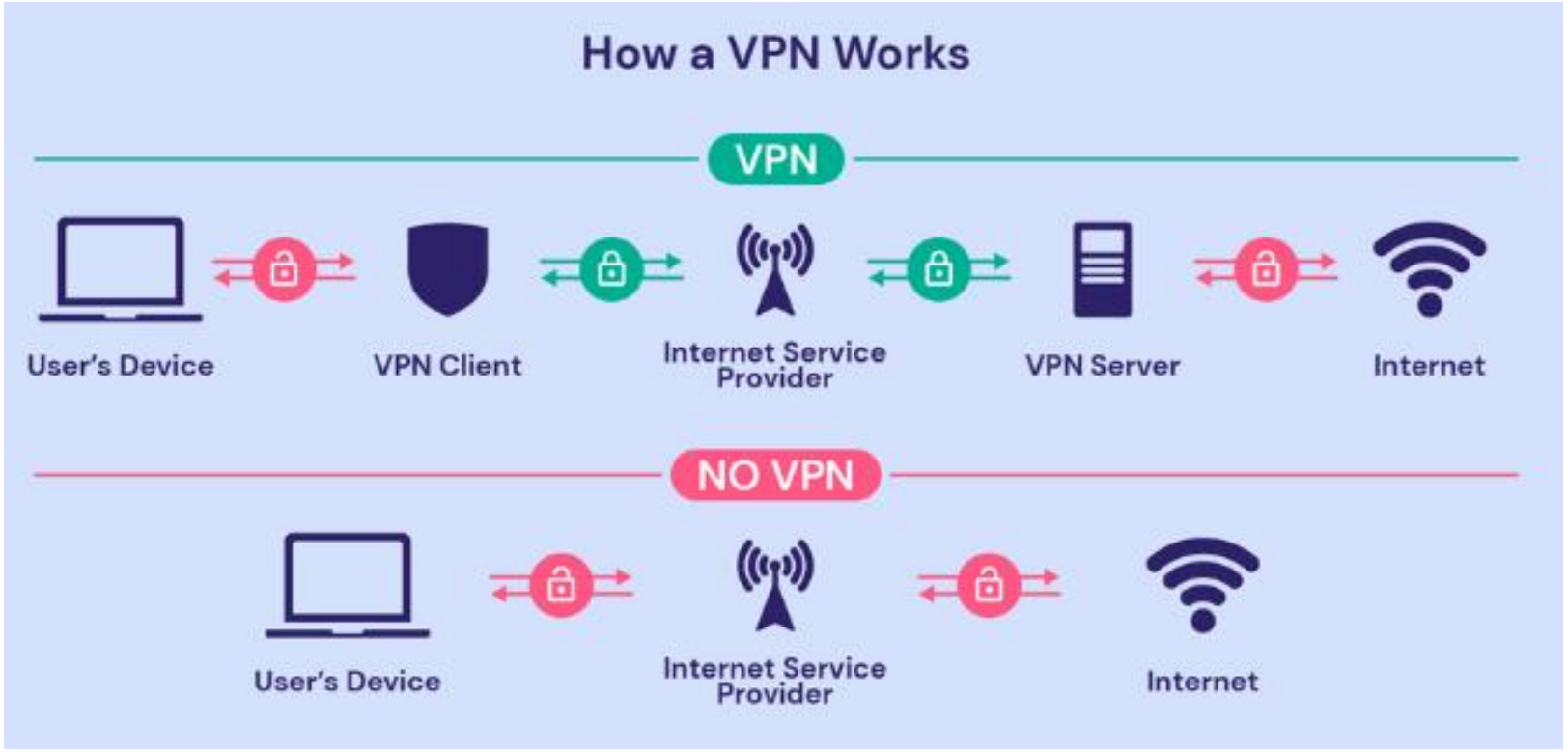
Kā aizsargāt savu IT «kopu»?

- Papildus personas identifikācija ir vitāls drošības garants. **Vienmēr, ja iespējams, izmantojam 2 faktoru autentifikāciju!!** Ja hakeris būs ieguvis jūsu paroli, viņš «aplauzīsies» nākamajā solī, kad būs jāievada SMS no jūsu mobilā telefona.
- **Nekad nelietojiet visur vienādas paroles!!** Ja hakeris ir uzzinājis paroli «AAA» servisam, bet kā 2faktoru autentifikācija ir jūsu e-pasts ar tādu pašu paroli, tam nebūs jēgas. «Single-point-of-failure».

1. Magnētiskā karte, USB u.c. fiziska iekārta
2. Parole (jebkurā veidā un ierīcē). Lielie, mazie burti, cipari, speciālie simboli.
3. Multi-faktoru autentifikācija. Parasti parole + kods (sms, e-mail, lietojums, PIN, sejas atpazīšana u.t.t.)
4. **Biometrijas dati**

Kā aizsargāt savu IT «kopu»?

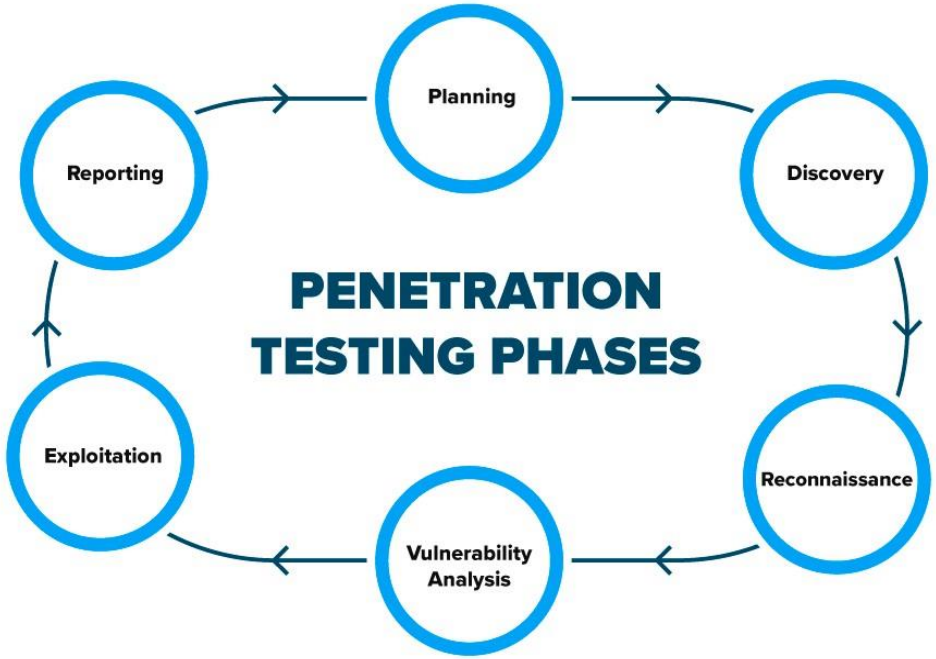




Virtuālais privātais tīkls (VPT) jeb ***VPN*** (angļu: *virtual private network*) ir vispārējs nosaukums tehnoloģijām, kuras nodrošina vienu vai vairākus tīkla savienojumus (virtuālu tīklu) kāda tīkla vai vairāku tīklu (piemēram, interneta) ietvaros. Lai nodrošinātu datu nepārtveršanu publiskajos tīklos, tiek izmantota kriptogrāfija.

Kā aizsargāt savu IT «kopu»?

- Ir noderīgi pārbaudīt vai Jūsu parole nav atrodama kādā paroļu datu bāzē no kāda iepriekš kompromitēta servisa. https://haveibeenpwned.com/
- Ik pa laikam ir noderīgi pārliecināties, ka Jūsu uzņēmuma IoT ierīces nav iekļautas kādā no uzlauzto ierīču sarakstā. https://www.thingful.net/
- Regulāri iepazīties ar jaunākajiem drošības riskiem. Šādu vietņu mūsdienās ir ļolti daudz. https://www.bleepingcomputer.com/news/security/
- Visur lietot 2 faktoru autentifikāciju. https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up
- Regulāri veikt ielaušanās (**penetration test**) visai uzņēmuma insfrastruktūrai



Kā aizsargāt savu IT «kopu»?

Ugunsmūris

Antivirus

2FA autentif.

Drošas paroles

VPN

Būt IT 24/7
Izglītoties!

Kā aizsargāt savu IT «kopu»?

- ✓ Install an anti-spyware package
- ✓ Keep your OS, apps and browser up-to-date
- ✓ Ignore spam
- ✓ Back up your computer
- ✓ Shut it down
- ✓ Use virtualization
- ✓ Secure your network
- ✓ Use encryption
- ✓ Turn off Bluetooth
- ✓ Don’t use unsecured public Wi-Fi
- ✓ Get a security app
- ✓ Switch off autocomplete
- ✓ Clear your browsing history

Jautājumi?

Paldies un tiekamies RTU!

Mārtiņš Bonders
martins.bonders@rtu.lv