

# IT biztonság az oktatásban, avagy a nyitott kapuk döngetésének művészete

**Arányi Gábor**

IT biztonsági mérnök - etikus hacker - PE PhD hallgató



# Beszélnünk kell róla, mert:

- hatalmas és szerteágazó az infrastruktúra
- kevés erőforrás áll rendelkezésre, az NKI erőforrásai szintén végesek
- a jövő szakembereit kell új szemléletre oktatni
- már elég néhány videót megnézni, letölteni néhány alkalmazást és tömegesen lehet támadásokat kivitelezni
- „a másiknál kell gyorsabban futni, nem az oroszlánnál”

## Az IT biztonság tudatosság még nem épült be a fejlesztői-, oktatói-, üzemeltetői gyakorlatba, mert:

- közvetlenül nem látható az eredménye, azonban erőforrást köt le
- „Miért pont minket támadnának meg?” gondolkodás a jellemző
- általában az egyetlen mérce: „csak működjön, lehetőleg azonnal”
- sokszor örökölt, inhomogén, kevésbé dokumentált hardveres és szoftveres platformok alkotják a teljes infrastruktúrát, amihez inkább nem nyúlunk hozzá



# Klasszikus hibák I.

- szabványos portok használata ott, ahol nem lenne muszáj
- alapértelmezett bannerek, szolgáltatás „ujjlenyomatok” hirdetik a kiszolgálói környezet részleteit (OS, szolgáltatás típusa, verziók)
- átláthatatlan szolgáltatás platform
- régi szoftver verziók futnak, láthatóan nincsen patch menedzsment
- a végpontvédelmi-, és a kiszolgálói menedzsment felületek publikusak
- könnyen túlterhelhető infrastruktúrák (alulméretezés, nem megfelelő erőforrás kihasználás)

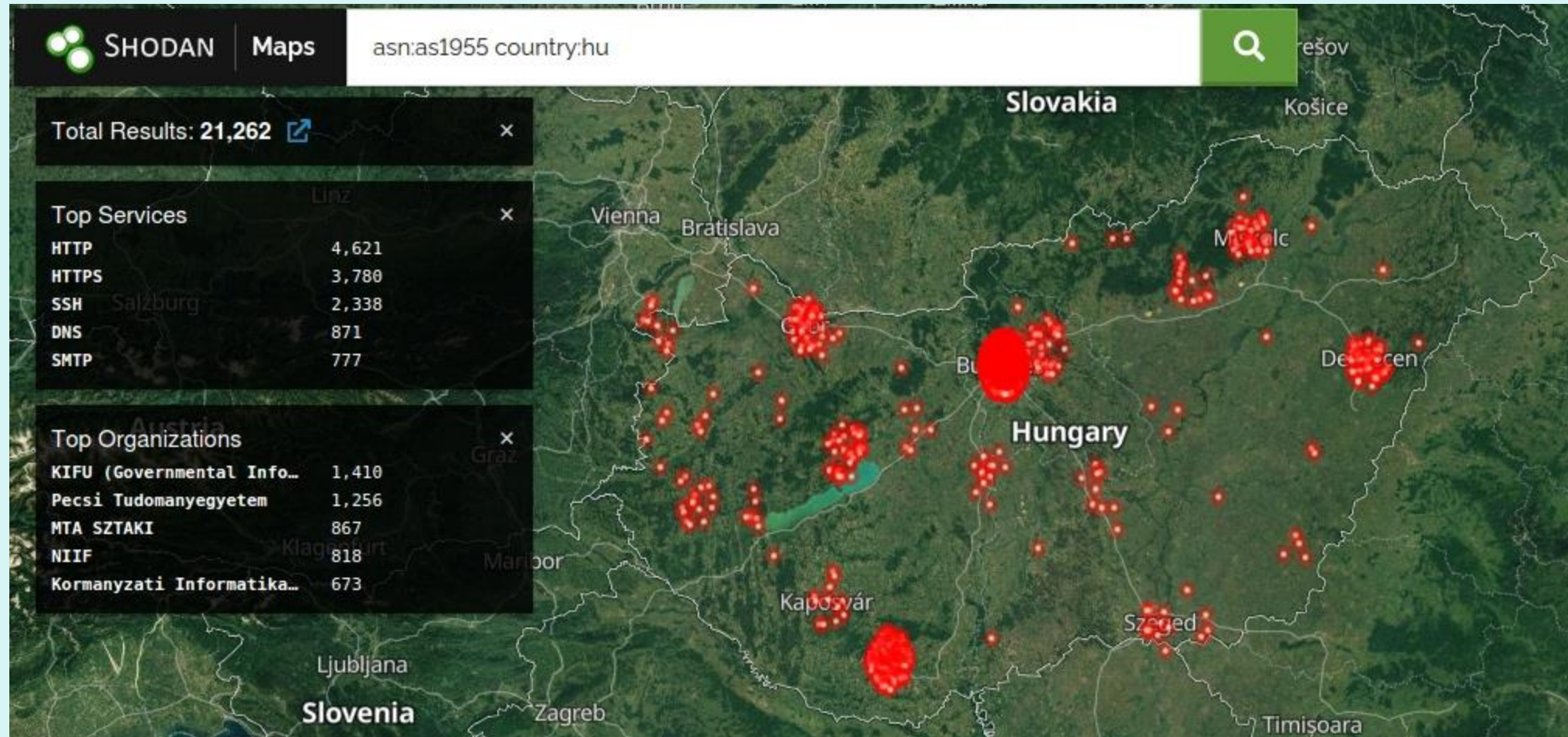
# Klasszikus hibák II.

- „szabotőr” felhasználók (lesz saját NAS-om, WiFi-m)
- gyakran nincsen semmilyen védelmi mechanizmus integrálva a célrendszerekbe (tűzfal, IDS/IPS, WAF)
- ping, traceroute működik
- alapértelmezett konfigurációk használata, akaratlanul publikált tartalmak (pl.: WebDAV, anonymous FTP, SMB null session, stb.)
- elérhetőségek, személyes adatok könnyen begyűjthetőek

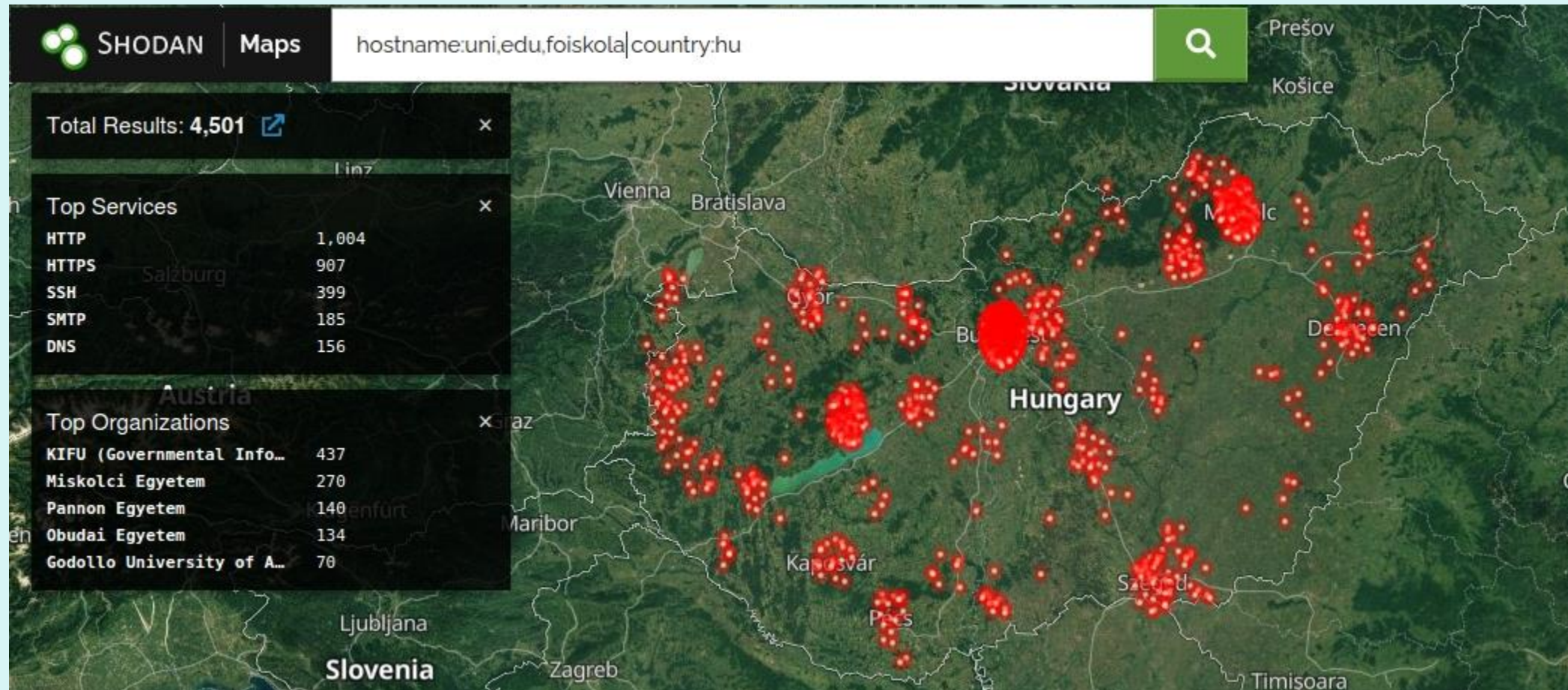
# Klasszikus hibák III.

- sokszor nincsen forrás IP-szűrés, többfaktoros autentikáció, tanúsítvány alapú hitelesítés
- semmilyen log alapú riasztási mechanizmus (pl.: email, SMS) nem kerül kiépítésre
- gyenge jelszavak, kikapcsolt autentikációs házirendek
- nincsen semmilyen anti-bruteforce mechanizmus, csillapítás
- otthagyott tartalmak, magára hagyott környezetek

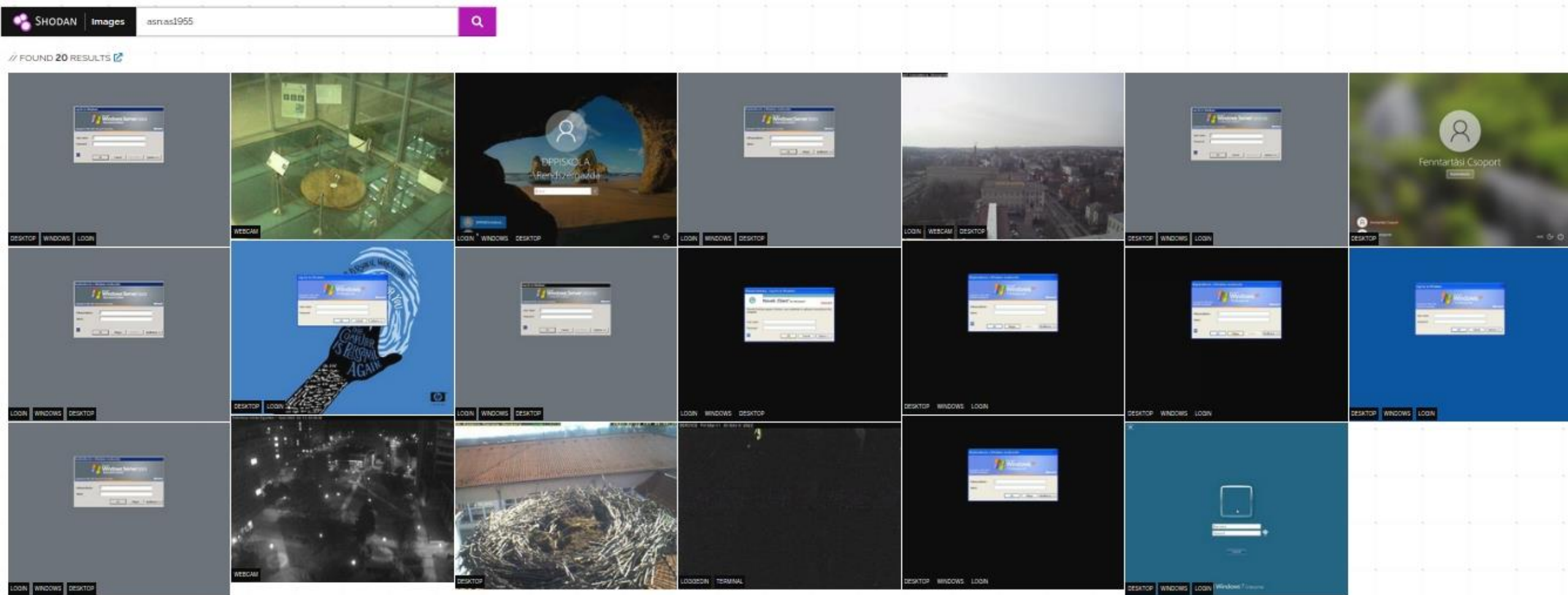


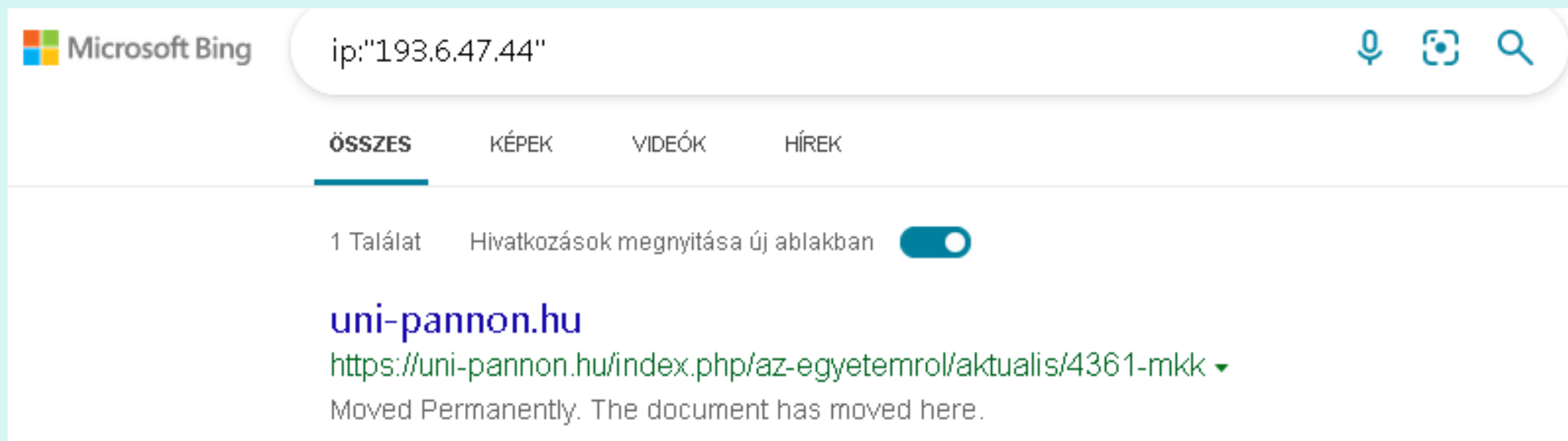
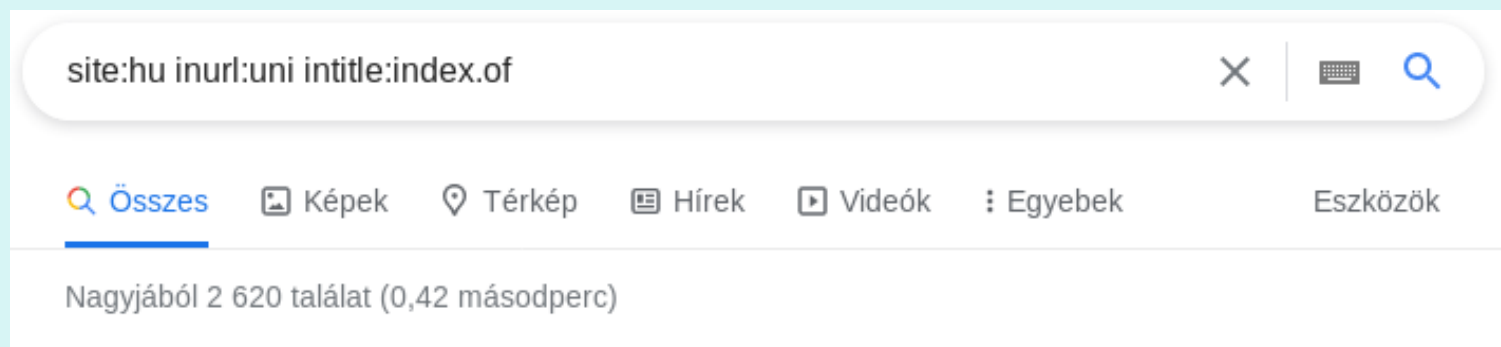












[Explore](#)
[Downloads](#)
[Pricing](#)

TOTAL RESULTS

# 26

TOP ORGANIZATIONS

	Egyetem	3
	Konyvtar	2
	Egyetem	2
	Iskola	1
	Egyetem	1

[More...](#)

TOP PRODUCTS

ProFTPD	6
Microsoft ftpd	3
HP JetDirect ftpd	1
HP-UX ftpd	1

View Report
 Download Results
 Historical Trend
 View on Map

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Hungary, Budapest

```

220 ProFTPD Server (Hilab) [::ffff:193.225.87.18]
230-Welcome, archive user anonymous@224.86.193.173 !
230-
230-The local time is: Fri Mar 11 01:54:01 2022
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <root@hilab.ikk.sztaki....
          
```

Pécsi Tudományegyetem

Hungary, Pécs

```

220 Welcome to PTE-TTK ftp.
230 Login successful.
214-The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
RNT0 SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP ...
          
```

195.199.157.57



ftp://[redacted]admin/kepek\_csesztregi\_gep/asztal/Desktop/

Index of ftp://[redacted]/admin/kepek\_csesztregi\_gep/asztal/Desktop/

↑ Up to higher level directory



Name	Size	Last Modified ↑
Åšj mappa		2/3/22 10:26:00 AM GMT+1
Å-sszefoglalÅ³ tÅ¡blÅ¡zatok		2/3/22 10:26:00 AM GMT+1
Å-NÅ%RTÅ%KELÅ%SEK		2/3/22 10:26:00 AM GMT+1
Å%V VÅ%GI 2018		2/3/22 10:26:00 AM GMT+1
Å%RTÅ%KELÅ%SEK)		2/3/22 10:26:00 AM GMT+1
Å%RTÅ%KELÅ%SEK		2/3/22 10:26:00 AM GMT+1
Veronka		2/3/22 10:26:00 AM GMT+1
Tanmenet vÅ©gsÅ' 2017		2/3/22 10:26:00 AM GMT+1
TANANYAG		2/3/22 10:26:00 AM GMT+1
Suli		2/3/22 10:26:00 AM GMT+1
RÅ©gi Firefox adatok		2/3/22 10:26:00 AM GMT+1
Pince		2/3/22 10:26:00 AM GMT+1
Papa		2/3/22 10:25:00 AM GMT+1
nÅ©gy Å©v		2/3/22 10:25:00 AM GMT+1
MÅ%RÅ%SEK		2/3/22 10:12:00 AM GMT+1
MINÅSÅTÅ%S		2/3/22 10:12:00 AM GMT+1
LEVELEK		2/3/22 10:12:00 AM GMT+1



ftp://[REDACTED].hu/

### Index of ftp://[REDACTED].hu/

↑ Up to higher level directory

Name	Size	Last Modified
 5U4LUMKB		6/14/20 2:00:00 AM GMT+2
File: AV.lnk	2 KB	3/14/22 3:13:00 PM GMT+1
File: AV.scr	6125 KB	3/14/22 3:13:00 PM GMT+1
File: feladat.txt	1 KB	5/11/17 2:00:00 AM GMT+2
File: info.zip	68 KB	2/22/22 4:51:00 PM GMT+1
 NOP5P5N6		6/14/20 2:00:00 AM GMT+2
File: Photo.lnk	2 KB	3/14/22 3:13:00 PM GMT+1
File: Photo.scr	6125 KB	3/14/22 3:09:00 PM GMT+1
File: Video.lnk	2 KB	3/14/22 3:13:00 PM GMT+1
File: Video.scr	6125 KB	3/14/22 3:11:00 PM GMT+1
File: welcome.msg	1 KB	5/19/15 2:00:00 AM GMT+2



ftp://[redacted]admin/programok/

Index of ftp://[redacted]/admin/programok/

↑ Up to higher level directory

Name	Size	Last Modified	
admin_test_programs		1/20/22	3:03:00 PM GMT+1
File: [redacted]-2018-06-21T14-50-17.mysql.gz	553 KB	6/21/18	3:50:00 PM GMT+2
doksik		8/30/18	12:25:00 PM GMT+2
File: FileZilla_3.25.2_win64-setup.exe	6850 KB	8/30/18	10:13:00 AM GMT+2
ISO-k		8/30/18	12:37:00 PM GMT+2
File: KeePass-2.39.1-Setup.exe	3168 KB	6/28/18	8:55:00 AM GMT+2
File: mappa_belep.bat	1 KB	9/30/13	4:57:00 PM GMT+2
File: mappa_kilep.bat	1 KB	9/30/13	4:44:00 PM GMT+2
[redacted]_weboldal_mentes		8/30/18	12:04:00 PM GMT+2
File: NTLite_setup_x64.exe	9513 KB	8/30/18	10:25:00 AM GMT+2
phpExcelReader		8/30/18	10:29:00 AM GMT+2
programok		8/30/18	12:40:00 PM GMT+2
rcsetup153		8/30/18	12:23:00 PM GMT+2
File: Send-WOL.ps1	1 KB	8/30/18	10:29:00 AM GMT+2
SzerverTankonyv		8/30/18	10:32:00 AM GMT+2
File: TeamViewer_Setup.exe	18863 KB	1/8/18	2:09:00 PM GMT+1
web_backup		3/13/20	12:41:00 PM GMT+1
wifi		8/30/18	10:34:00 AM GMT+2

Index of ftp://[redacted]/home/egyeztetni!!!  
/1.2.392.200036.9123.100.50.121111600360012211108095923000564045-PACS-orig/

↑ Up to higher level directory

Name	Size	Last Modified
File: 1.2.392.200036.9123.100.50.1211116003600102111081015185499...	695853 KB	11/26/21 3:22:00 PM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081018113464...	2036069 KB	11/8/21 11:41:00 AM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081019532259...	278031 KB	11/8/21 11:17:00 AM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081029341540...	1097970 KB	11/26/21 3:34:00 PM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081041013299...	1780 KB	11/8/21 11:41:00 AM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081052484758...	1774 KB	11/8/21 11:49:00 AM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081053014601...	1773 KB	11/8/21 11:49:00 AM GMT+1
File: 1.2.392.200036.9123.100.50.1211116003600102111081057293187...	1779 KB	11/8/21 11:54:00 AM GMT+1





smb://[redacted]/install/

Name	Size	Type	Date Modified
▶ AOMEI Backupper All Editions WinPE Boot Legacy & UEFI v5.7.0 [FileCR]	--	Folder	Thu 02 Sep 2021 06:39:22 PM CEST
▶ EasyUEFI Enterprise 4.2 Multilingual	--	Folder	Tue 03 Nov 2020 09:19:31 PM CET
▶ Shadow Defender 1.5.0.726	--	Folder	Mon 28 Sep 2020 10:08:04 AM CEST
▶ NetDrives-1.0.2	--	Folder	Thu 23 Jul 2020 01:31:47 PM CEST
Microsoft Toolkit 2.6.2 Final (Windows & Office Activator) [SadeemPC].zip	58,2 MB	Archive	Wed 20 Oct 2021 11:57:12 AM CEST
NetDrivesData.xml	9,7 kB	Markup	Mon 18 Oct 2021 06:28:47 PM CEST
AdobeCreativeCloudCleanerTool.exe	8,5 MB	Program	Fri 01 Oct 2021 06:30:33 PM CEST
AdobeCreativeCloudCleanerTool.dmg	1,7 MB	Unknown	Fri 01 Oct 2021 06:30:31 PM CEST
.DS_Store	6,1 kB	Binary	Fri 01 Oct 2021 06:29:58 PM CEST
ChromeSetup.exe	1,3 MB	Program	Sun 29 Aug 2021 08:07:53 PM CEST
Active Boot Disk v15.0.6 Win10 PE x64.iso	417,1 MB	Unknown	Tue 03 Nov 2020 09:19:30 PM CET
▶ Affinity	--	Folder	Tue 07 Dec 2021 09:03:52 PM CET
▼ Maxon	--	Folder	Tue 09 Nov 2021 06:33:33 PM CET
▶ Maxon CINEMA 4D Studio R20.059	--	Folder	Mon 28 Sep 2020 10:05:39 AM CEST
▶ MAXON_License_Server_WIN_MAC	--	Folder	Sun 08 Dec 2019 01:26:03 PM CET
.DS_Store	6,1 kB	Binary	Mon 01 Nov 2021 02:04:59 PM CET
Maxon CINEMA 4D Studio S22.118 + Crack (Windows).zip	365,2 MB	Archive	Tue 03 Nov 2020 09:19:33 PM CET
▶ Adobe	--	Folder	Tue 02 Nov 2021 11:28:50 AM CET
▼ Microsoft	--	Folder	Tue 19 Oct 2021 06:59:46 PM CEST
▶ Windows 7 Professional [A2zCrack.com]	--	Folder	Thu 14 Oct 2021 05:19:38 PM CEST
▶ Microsoft Office 2019 for Mac v16.53 + Fix (macOS) {CracksHash}	--	Folder	Fri 08 Oct 2021 06:55:27 PM CEST
.DS_Store	6,1 kB	Binary	Tue 09 Nov 2021 06:33:41 PM CET
Windows 10 X86 21H1 PRO incl Office 2019 EN.ISO	5.2 GB	Unknown	Thu 14 Oct 2021 05:01:24 PM CEST





smb://[redacted]/publikacio/

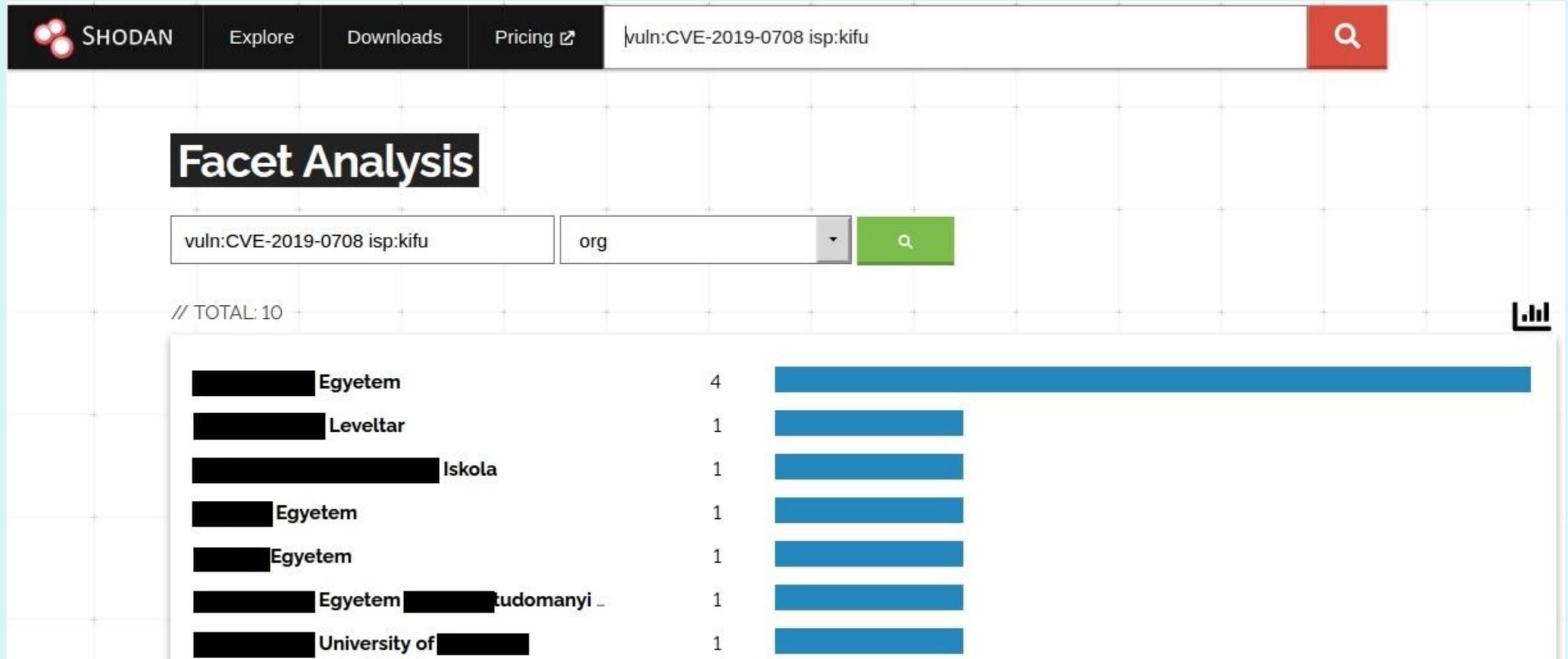
Name	Size	Type	Date Modified
▼ TK	--	Folder	Wed 02 Mar 2022 03:17:10 PM CET
▶ 4D online 57-61. szám pdf	--	Folder	Mon 14 Feb 2022 03:59:05 PM CET
▶ 4D 57 online pdf_javitott	--	Folder	Thu 10 Feb 2022 03:04:31 PM CET
▶ 4D_57	--	Folder	Sun 23 Jan 2022 07:51:08 PM CET
▶ _MACOSX	--	Folder	Tue 02 Mar 2021 02:19:26 PM CET
▶ 4D 53 online pdf	--	Folder	Tue 02 Feb 2021 09:57:40 AM CET
▶ 4D 55-56 online pdf	--	Folder	Tue 02 Feb 2021 09:42:36 AM CET
▶ 4D 52 online pdf	--	Folder	Tue 02 Feb 2021 09:32:14 AM CET
📄 Maria Auböck.docx	12,1 kB	Document	Wed 02 Mar 2022 03:17:13 PM CET
📦 4D online pdf.zip	222,6 MB	Archive	Mon 14 Feb 2022 03:56:48 PM CET
📦 4D 57 online pdf_javitott.zip	28,4 MB	Archive	Thu 10 Feb 2022 03:03:45 PM CET
📦 4D 52, 53, 55-56 DOI pdf.zip	55,6 MB	Archive	Tue 02 Mar 2021 02:15:51 PM CET


```

[+] NFS Export: /datastore [10.32.0.0/16]
[+] NFS Export: /nfsshare
[*] Scanned 5 of 45 hosts (11% complete)
[+] NFS Export: /Volumes/Promise/pataki/home/Documents/work/kopi/git/kopi-wiki-mount [192.168.0.0]
[*] Scanned 9 of 45 hosts (20% complete)
[+] NFS Export: /mnt [192.168.100.0/24]
[*] Scanned 14 of 45 hosts (31% complete)
[+] NFS Export: /exports/maildirs [10.10.0.0/16]
[+] NFS Export: /exports [10.10.0.0/16]
[*] Scanned 18 of 45 hosts (40% complete)
[+] NFS Export: /backup/B [10.50.152.150]
[+] NFS Export: /backup/dbtop_archive [10.50.152.4]
[+] NFS Export: /backup/
[+] NFS Export: /backup/
[+] NFS Export: /backup/computrend_oracle [10.50.152.102, 10.50.152.107]
[+] S Export: /media/hdd
[+] NFS Export: /srv/www/sulixinstall/iso/LiveOS [*]
[+] NFS Export: /srv/tftp [*]
[+] NFS Export: /home [172.16.33.0/24, 172.16.32.0/24, 172.16.31.0/24, 172.16.30.0/24, 172.16.29.0/24, 172.16.28.0/24, 172.16.27.0/24, 172.16.26.0/24, 172.16.25.0/24, 172.16.24.0/24, 172.16.23.0/24, 172.16.22.0/24, 172.16.21.0/24, 172.16.20.0/24, 172.16.19.0/24, 172.16.18.0/24, 172.16.17.0/24, 172.16.16.0/24, 172.16.15.0/24, 172.16.14.0/24, 172.16.13.0/24, 172.16.12.0/24, 172.16.11.0/24, 172.16.10.0/24, 172.16.9.0/24, 172.16.8.0/24, 172.16.7.0/24, 172.16.6.0/24, 172.16.5.0/24, 172.16.4.0/24, 172.16.3.0/24, 172.16.2.0/24]
[*] Scanned 23 of 45 hosts (51% complete)
[+] NFS Export: /export/.own_backup [
[+] NFS Export: /export/mail [
.hu]
[+] NFS Export: /export/home [
.hu]
[+] NFS Export: /opt/plexmedia []
[*] Scanned 27 of 45 hosts (60% complete)
[+] NFS Export: /mnt/docker_storage [10.251.1.222, 10.251.1.223, 10.251.1.224, 10.251.1.225, 10.251.1.226]
[+] NFS Export: /mnt/ [10.200.20.158, 10.200.20.166, 10.200.20.165]
[+] NFS Export: /mnt/storage2 [10.200.20.151, 10.200.20.159, 10.200.20.152, 10.200.20.128, 10.200.20.127, 10.200.20.124, 10.200.20.161]
[+] NFS Export: /mnt/storage [10.200.20.151, 10.200.20.51, 10.200.20.159, 10.200.20.152, 10.200.20.128, 10.200.20.127, 10.200.20.124, 10.200.20.161]
[+] NFS Export: /mnt/iscsi/eternus/offline
[+] NFS Export: /mnt/iscsi/eternus/image [1
[+] NFS Export: /mnt/iscsi/eternus/archive
[*] Scanned 32 of 45 hosts (71% complete)
[+] - 193.6.41.6 NFS Export: /volume1/SynologyNFS [192.168.100.0/255.255.255.0]
[+] - 193.6.41.6 NFS Export: /volume1/ECloud_Backup [192.168.100.101]
[+] - 193.224.129.167 NFS Export: /nfs [10.4.0.0/24]
[+] - 193.6.50.107 NFS Export: /var/www [


```






**SHODAN**


[Explore](#)
[Downloads](#)
[Pricing](#)




TOTAL RESULTS  
2,750

[View Report](#)
[Download Results](#)
[Historical Trend](#)
[View on Map](#)

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)


**SHODAN**


[Explore](#)
[Downloads](#)
[Pricing](#)




TOTAL RESULTS  
231

[View Report](#)
[Download Results](#)
[Historical Trend](#)
[Browse Images](#)
[View on Map](#)

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)


**SHODAN**

[Explore](#)
[Downloads](#)
[Pricing](#)



TOTAL RESULTS  
38

[View Report](#)
[Download Results](#)
[Historical Trend](#)
[View on Map](#)

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)





← → ↻ 🏠 🔒 http://[REDACTED]:8080/EBITRPKAQAYUKMVB/userRpm/Index.htm

# TP-LINK®

- Status
- Quick Setup
- WPS
- Network
- Wireless**
  - Wireless Settings
  - **Wireless Security**
  - Wireless MAC Filtering
  - Wireless Advanced
  - Wireless Statistics
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding

## Wireless Security

☐ Disable Security

☒ WPA/WPA2 - Personal(Recommended)

Version: WPA2-PSK ▼

Encryption: Automatic ▼

Wireless Password: [REDACTED]2300  
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds  
(Keep it default if you are not sure, minimum is 30, 0 means no update)

☐ WPA/WPA2 - Enterprise

Version: Automatic ▼

Encryption: Automatic ▼

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

# javasolt megoldások I.

- rendszeres frissítés (OS, service, firmware, IoT)
- technológiai lábnyomok elrejtése (bannerek kikapcsolása, reverse proxy)
- lehetőleg nem tipikus portok használata, ping/portscan blokkolása
- port knocking, forrás IP-szűrés, autentikáció bevezetése ahol lehet
- tűzfalak (PFSense, OPNSense, CSF), IPS/IDS rendszerek (Suricata, Snort, LFD) használata
- alapértelmezett konfigurációk felülvizsgálata

# javasolt megoldások II.

- felesleges szolgáltatások leállítása
- bejelentkezések/próbálkozások naplózása
- csillapítás/bannolás (fail2ban, IPBan)
- komplex jelszavak használata (10 karakter felett, 44 vs. 26)
- célszerű többfaktoros autentikációt használni
- központi naplózás, riasztások generálása (Prometheus, Zabbix, Nagios)
- a titkosítatlan autentikációt, és/vagy adatforgalmat támogató szolgáltatásokat titkosított változatra kell cserélni

# javasolt megoldások III.

- VPN használata (OpenVPN, IPSec)
- minimális jogosultság elvének alkalmazása
- dokumentálás, követés
- tudatos tartalommenedzsment (digitális lábnyom vs. digitális ujjlenyomat)
- teljesítményoptimalizálás, terheléselosztás, skálázás
- rendszeres önellenőrzés (keresők, OSINT eszközök, sérülékenységvizsgálatok)



# Story time

- IIS7 Neptun
- oktatói Neptun hozzáférés MS Excelben
- publikus tanszéki „scan” mappa
- Moodle DoS
- open relay SMTP kiszolgáló
- rogue AP-k

# Köszönöm a figyelmet!

??? Kérdések ???