Datu drošība un cilvēciskais faktors, izmantojot mobilās iekārtas bezvadu tīklos

Didzis Balodis, CISSP, GPEN
DPA IT drošības virziena vadītājs

2013.gada 23.oktobris

Saturs

- Fakti un skaitļi
- Prakse
- Risinājumi

Didzis Balodis

DPA IT drošības virziena vadītājs

- Vairāk kā 10 gadi IT industrijā (sākot no 1999.g)
- Administrēšana, izstrāde, drošība
- Pēdējie 5 gadi – IT konsultācijas, audits un drošības audits, ielaušanās testi (veikti vairāk kā 50 auditi)
- Hobijs - bezvadu tīklu drošība

Sertifikāti:

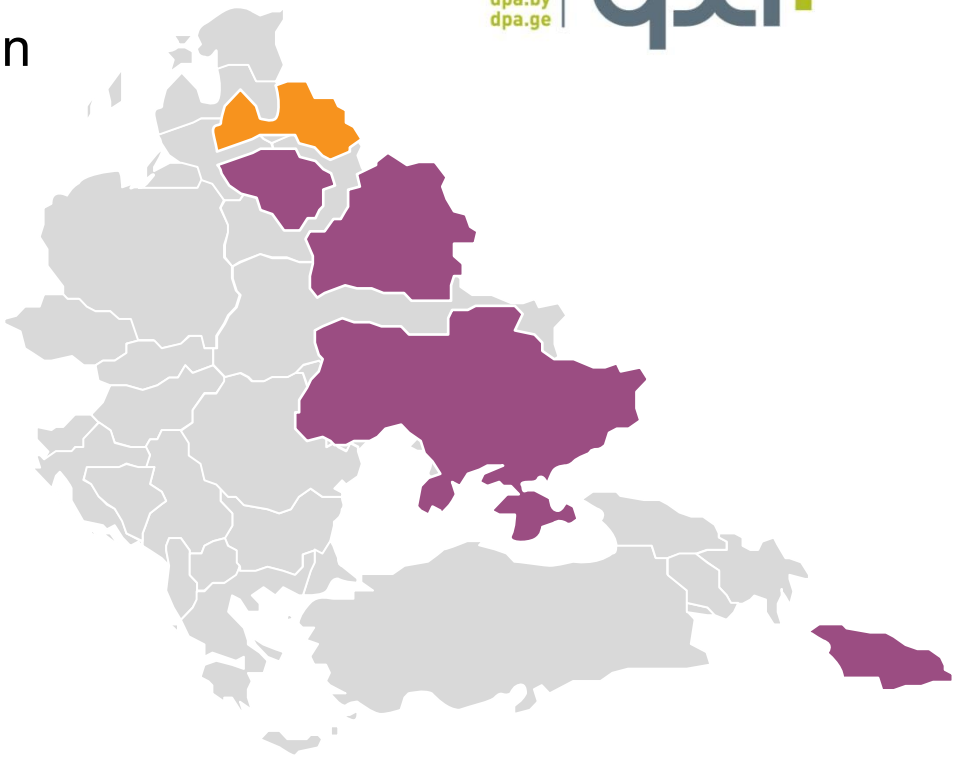
- CISSP- Certified Information System Security Professional
- GPEN – GIAC Certified Penetration Tester

DPA drošības pakalpojumi

IT auditi un ielaušanās testēšana:

- Atbilstības auditi LR normatīviem un labākās prakses standartiem
- Tīkla ielaušanās testi
- Bezvadu tīklu auditi
- Web aplikāciju drošības testēšana
- Sociālās inženierijas testēšana
- Darbinieku IT drošības apmācība

dpa.lv
dpa.lt
dpa.ua
dpa.by
dpa.ge



Sertifikāti

CISSP®

CISA®

Certified Information Systems Auditor™

Statistika 2013

96%

viegli uzbrukumi

Statistika 2013

79%

gadījuma raksturs

Statistika 2013

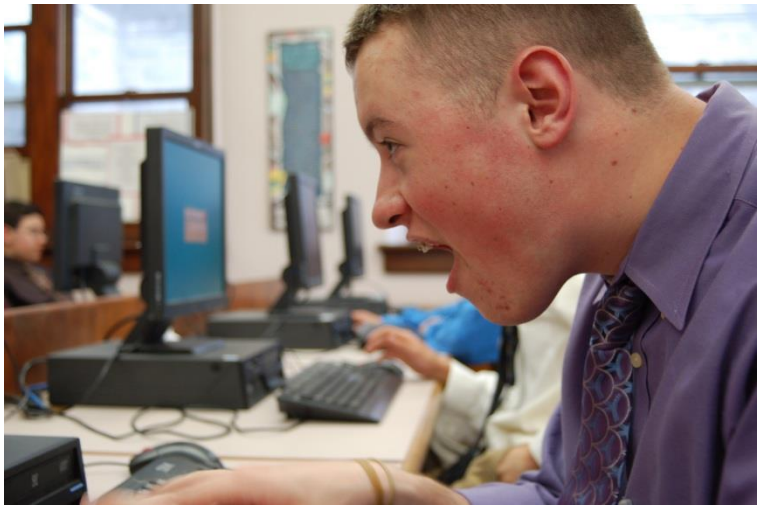
85%

netika laicīgi atklāti

Lietotājs – vājākais ķēdes posms IT drošībā

Phishing

Malware



Avots: www.stockvault.net

Soc. engineering

Mobile threats

Riski bezvadu tīklos

Lietotājiem:

Datu pārķeršana/ noklausīšanās	Viltus piekļuves punkts (Rogue AP)	Uzbrukumi ierīcēm

Īpašniekiem:

Vāja vai noklusētā parole/ paroles nav	WEP šifrēšana	Uzbrukumi ierīcēm, pēc tam, kad iegūta pieeja tīklam

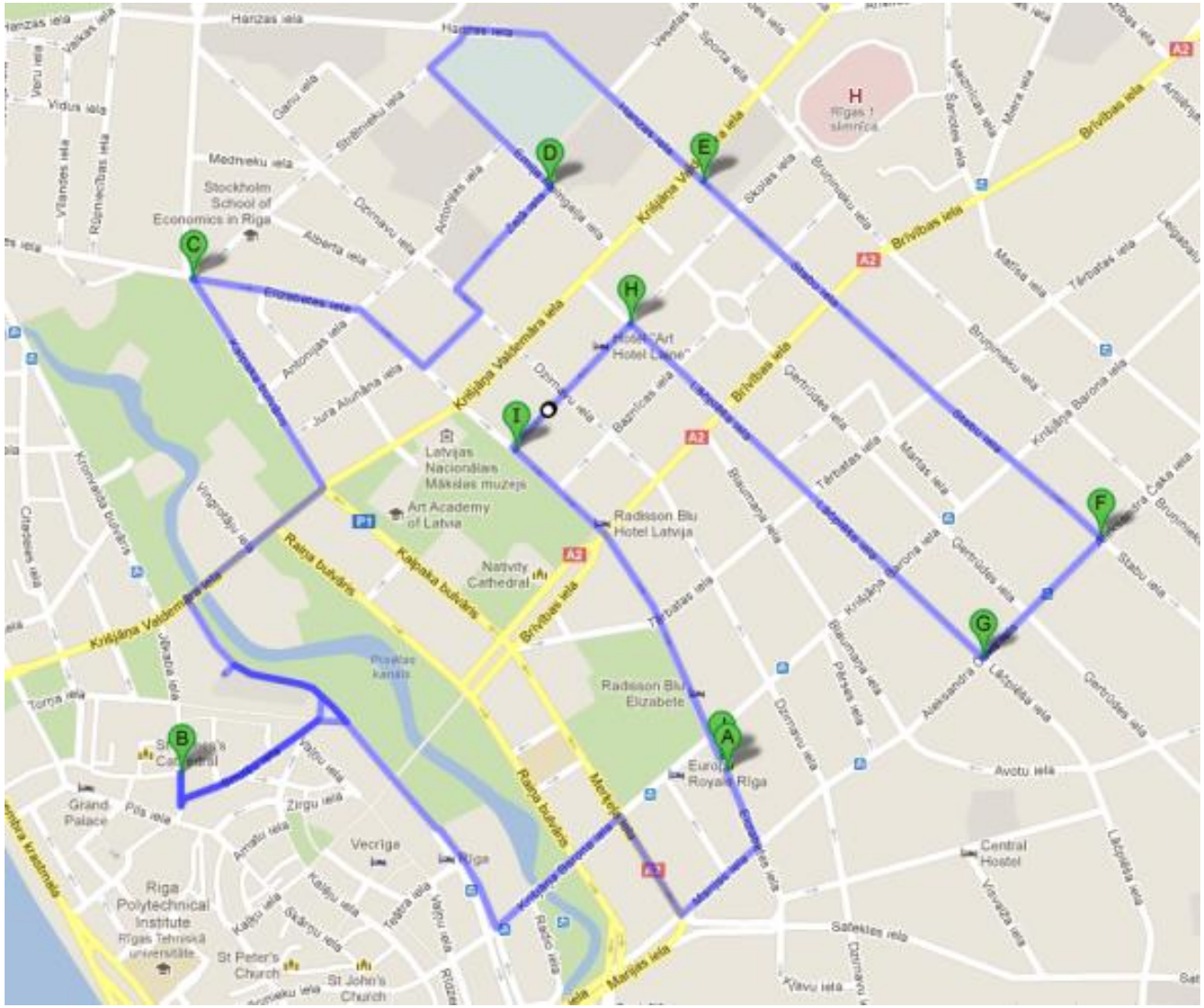
DPA pētījums (1)

Uzdevums:

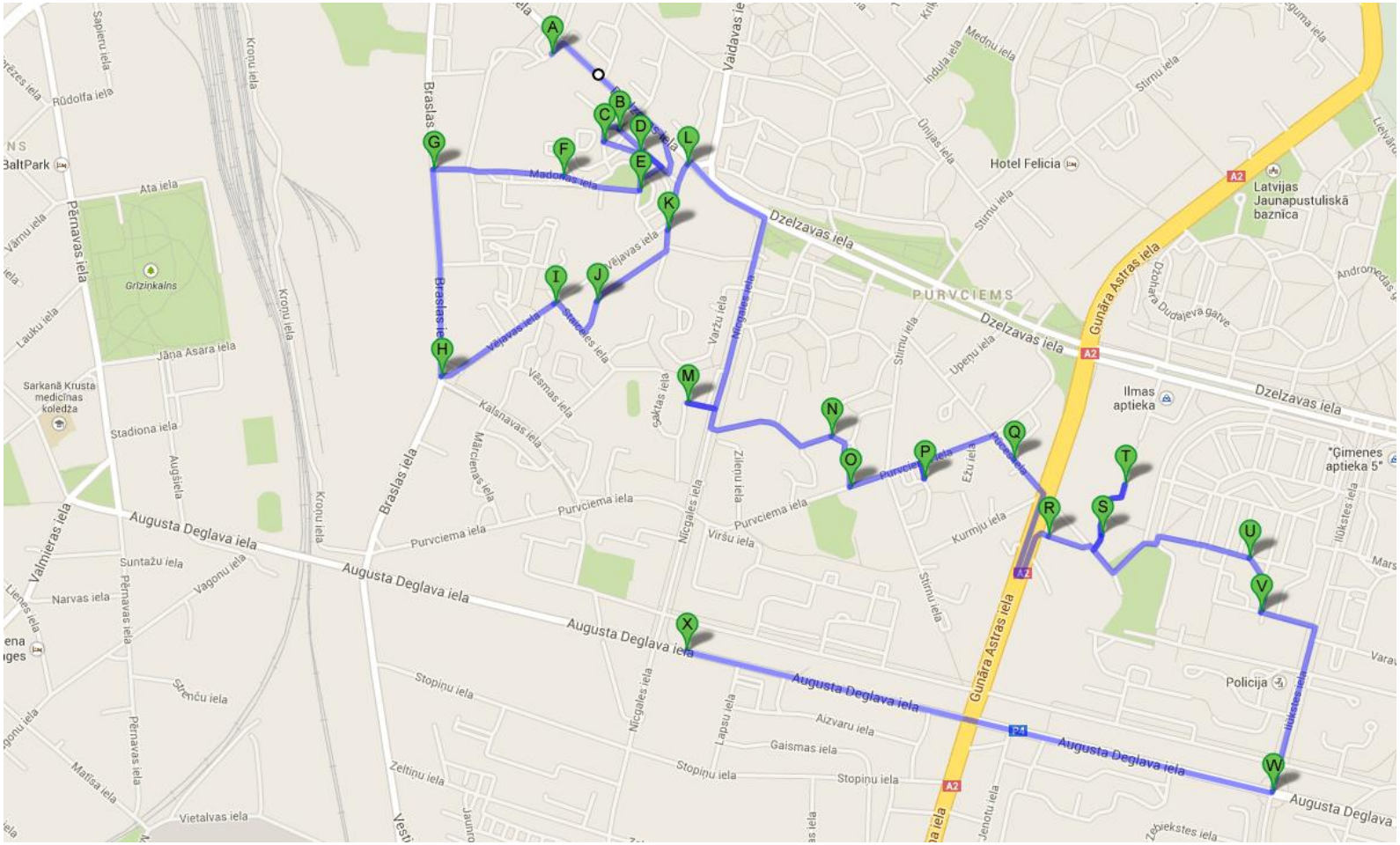
Apzināt wi-fi tīklu specifiku Rīgas centrā un mikrorajonā:

- Šifrēšanas veids
- Atvērtie tīkli
- Nosaukumi (SSID)

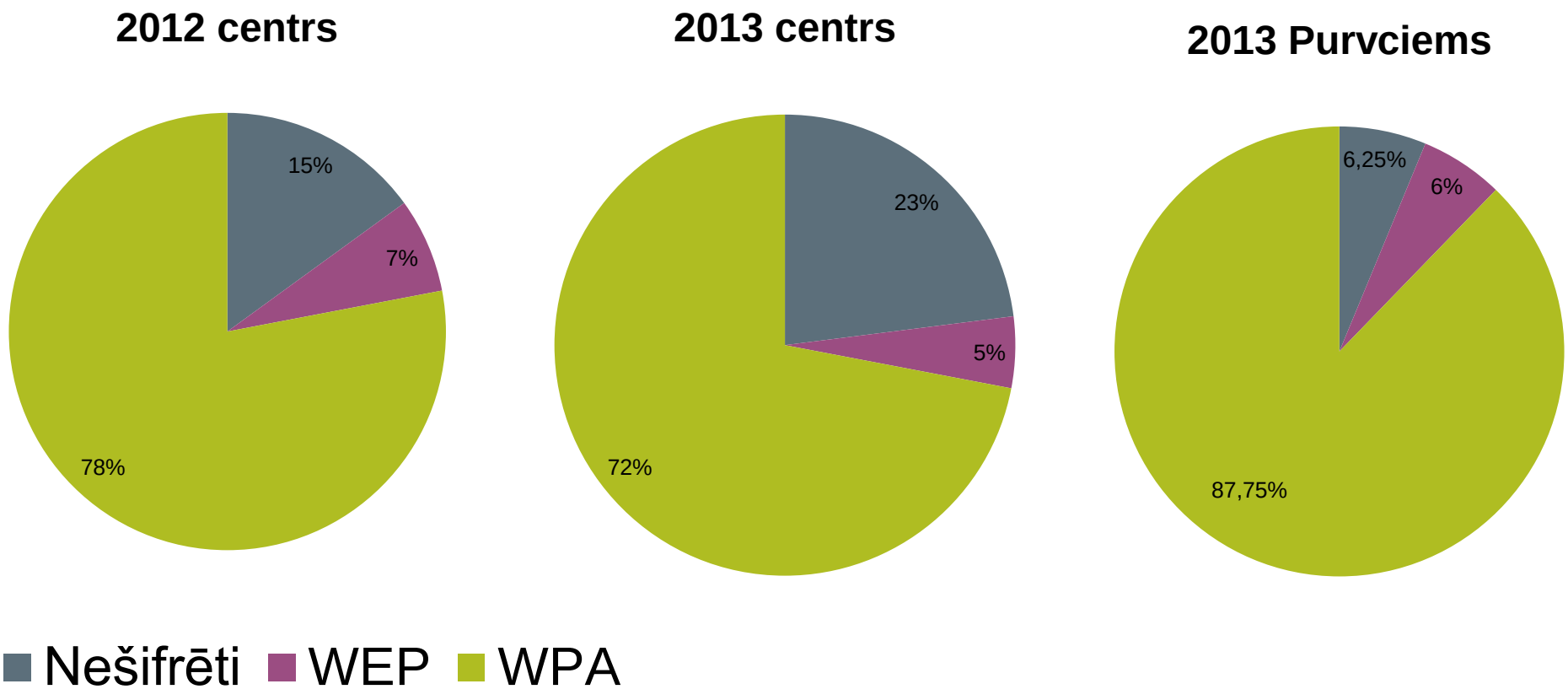
DPA pētījums (2)



DPA pētījums (3)



DPA pētījums (4)



Pilns pētījums: http:\\blogs.dpa.lv

Atvērtie tīkli (1)

Atvērtie tīkli (2)

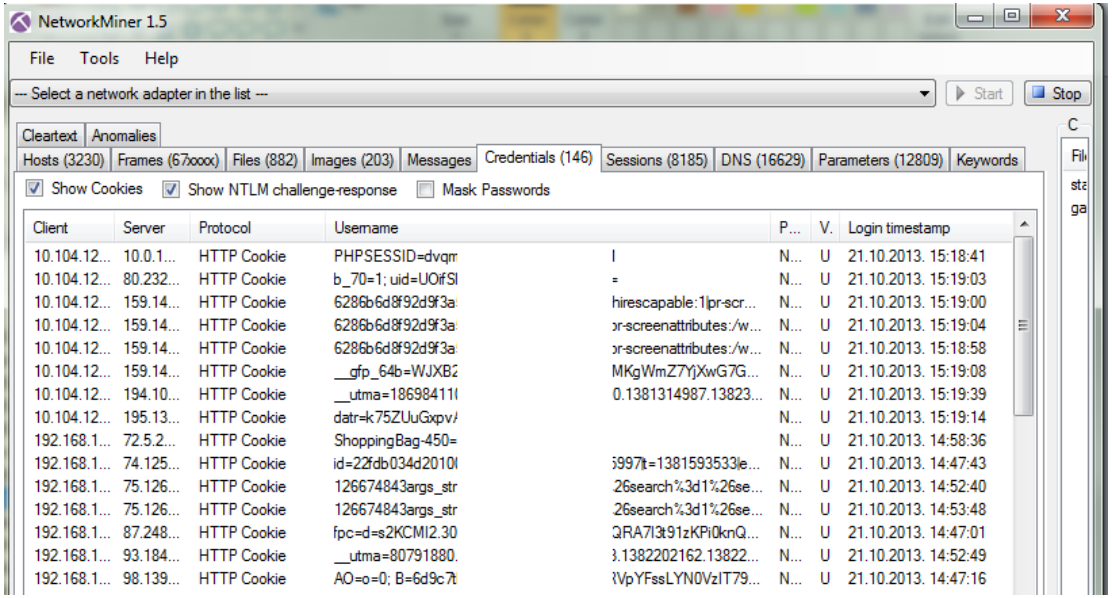
Atvērtie tīkli (3)

Atvērtie tīkli (4)

Atvērtie tīkli (5)

1. Scenārijs. Stunda atvērtajā tīklā

- 100 MB trafika
- 203 attēli
- Vairāk kā 3000 IP adreses
- Vairāk kā 100 session ID



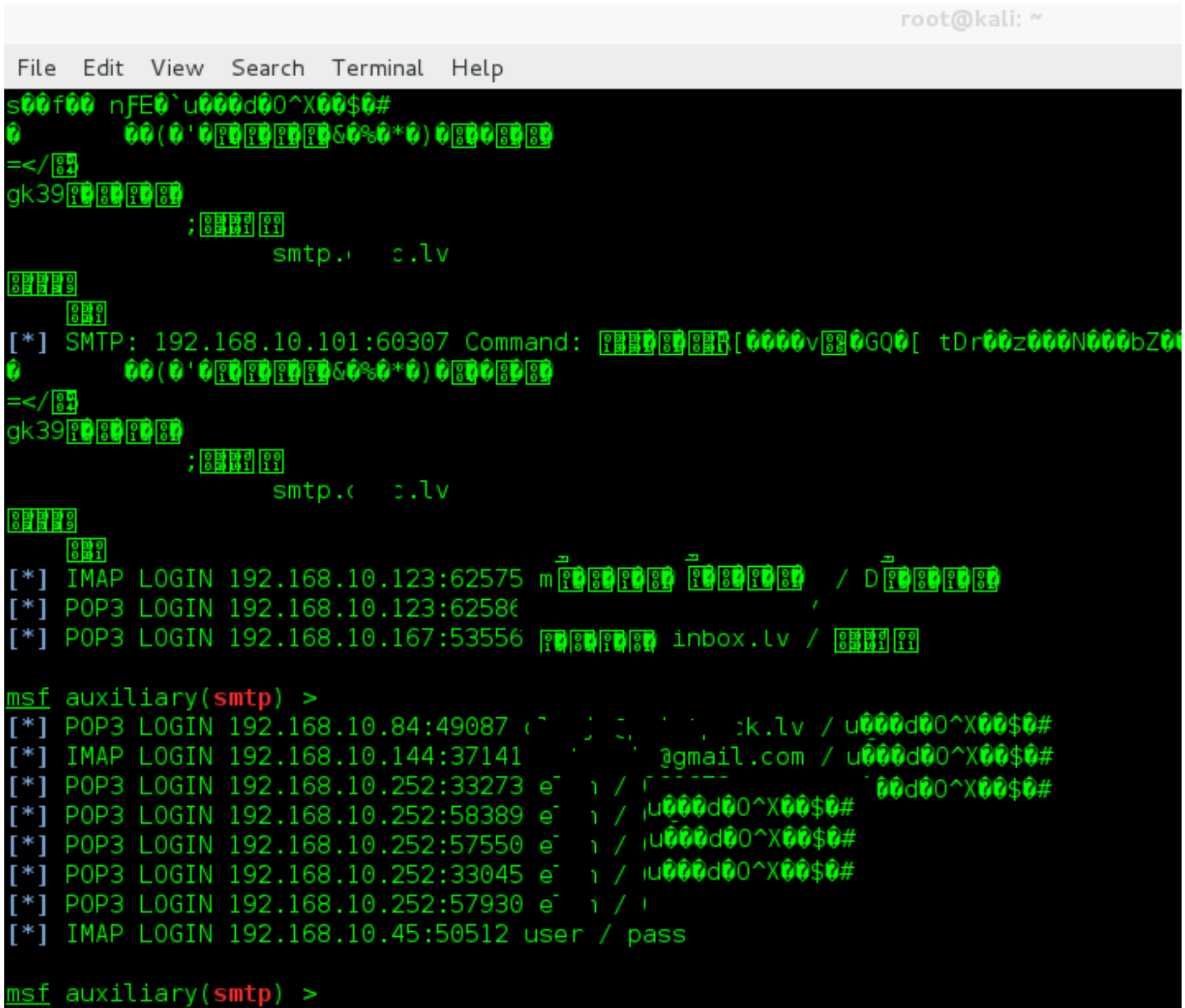
2 .Scenārijs. Viltus AP (1)

Mobilā ierīce ar wi-fi ->

Viltus AP (airbase-ng + dnsspoof)->

Datu pārtveršana

2 .Scenārijs. Viltus AP (2)



3. Scenārijs
Live probe requests

Kopsavilkums

- **Ar Wi- Fi izmantošanu saistītie riski bieži vien līdz galam nav apzināti:**
  - Publisko tīklu izmantošana
  - Privāto tīklu ierīkošana
  - Droša izmantošana uzņēmumos un iestādēs

Būtiska loma ir gala lietotāju izglītošanai kā arī pareizai tehnoloģiju pielietošanai.

Lietotāju izglītošanas princips

Sociālā inženierija

+

Apmācība

+

Sociālā inženierija

Lietotāju mācību programma

- Ikviens ir mērķis
- Sociālā inženierija
- Droša e-pasta lietošana
- Interneta pārlūkošana
- Sociālo tīklu izmantošana
- Mobilo ierīču drošība
- Paroles
- Datu un informācijas aizsardzība
- Bezvadu tīklu droša lietošana
- Darbs no mājām vai ceļā
- Iekšējie draudi
- Fiziskās drošības aspekti
- Datora drošība mājās
- Drošības incidents

Avots: www.stockvault.net

Jautājumi?