clarified security

we break security to bring clarity

Me kõik oleme haavatavad

Mehis Hakkaja
CEO/Founder/Owner
mehis@clarifiedsecurity.com
http://linkedin.com/in/mehishakkaja

clarified security
we break security to bring clarity

Räägime haavatavusest ja ründamisest

läbistustestijate

ja

punase meeskonna

silme läbi

clarified security
we break security to bring clarity

1) Läbistustestimine & Punase Meeskonna teenus

kuni 100 rakendust aastas & päris ründaja emuleerimine

2) Käed küljes koolitused *(~4000 osalejat)*

Web Application Security ***(WAS)***, *Secure Logging* ***(LOGSEC)***

Hands-on Hacking series ***(HOHE, HOHEFU/CTF, HOHA)***

Hands-on Threat Hunting / Hunt the Hacker (HtH)

3) Küberõppused *(Red Team vs Blue Team)*

2010 May - "**Baltic Cyber Shield**", 6 Blue Teams (***BT***), Red Team (***RT***) size ~20
2012 Mar - "**Locked Shields**", 9 BT, RT ~40
2013 Apr - "**Locked Shields**", 10 BT, RT ~40
2014 May - "**Locked Shields**", 12 BT, RT 50+
2015 Apr - "**Locked Shields**", 15 BT, RT 50+
2016 Apr - "**Locked Shields**", 20 BT, RT 60+
2017 Apr - "**Locked Shields**", 20 BT, RT 60+
2018 Apr - "**Locked Shields**", 21 BT, RT 65+
2019 Apr - "**Locked Shields**", 23 BT, RT 75+

1. **NATO CCDCoE** LOCKED SHIELDS
2. ***Cyber Range eXercise - CRX 2015 – 2019***
3. ***NATO Cyber Coalition*** *content* ***CC13 -CC18***
4. ***NATO CWIX*** *deliverable (CTF)* ***@CWIX17***

clarified security
we break security to bring clarity

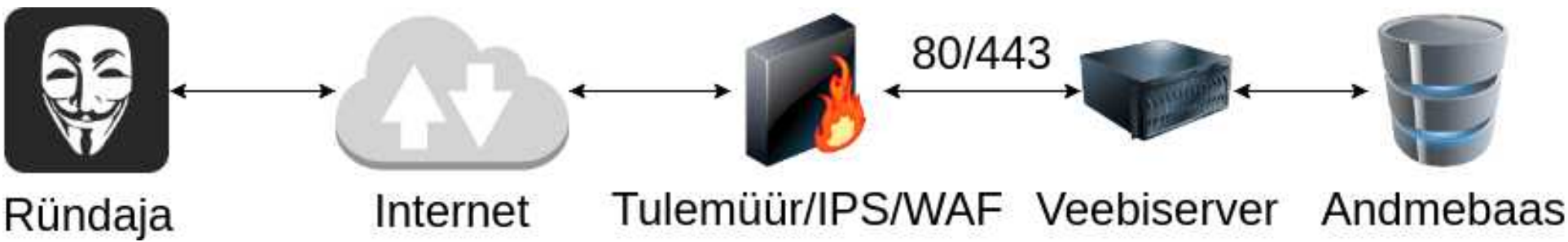
Rakenduste ründamine *(otsetee avatud uksest)*

~ 80 ... 100 rakenduste käsitsi läbistustesti aastas (OWASP **ASVS** & **MASVS**)

Eestis enamasti ka: **ID kaart, M-ID, Smart ID, Pangalink**, **X-Tee**, TARA, SiVa, SiGa ...

Saatan peitub detailides (teostuse isepärades) !

- *Turvalisest autentimisest möödapääsemine*
- *Pangalink ja e-poed*
- *SQLi / Blind SQLi näiteks internetipangas*
- *Lihtsalt rumalad vead (e.g. serveri tapmine 1 päringuga)*
- *Sessioonide kaaperdamine (üldjuhul vajab natuke kasutaja abi)*
- ...



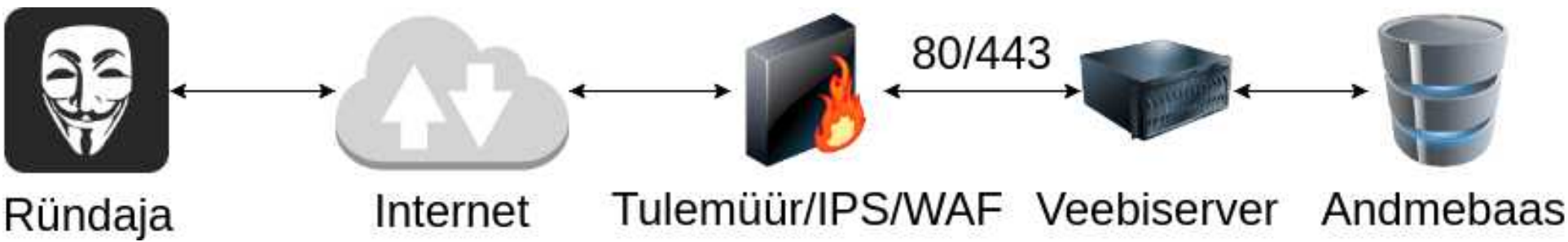
Läbistustestimine on juba „vana kooli” värk

Veebirakenduste läbistustestimise vajadusest saadakse Eestis juba üsna hästi aru:

- ärikriitiline / sensitiivsete andmetega rakendus = läbistustesti regulaarselt
- Vigu tehakse, leitakse, parandatakse – turvalisus on protsess
- Paraku, kui puudub turvajuht JA turvaspetsialist(id), siis protsess hästi ei toimi :(

Kui puudub vajadus interaktiivuse järele, palun peida CMS sisevõrku ja tooda staatilist sisu avalikku hostingusse *(või vähemalt piira admin liidese juurdepääs)*

… AGA kui avalik otsetee on testitud ja piisavalt kaitstud?



Läbistustestimine hõlmab palju enamat ning sel on väga selge vajadus ja eelised, AGA ka piirangud.

Räägime edasi aga hoopis teist moodi, uudsemast
päris elu matkivast ründamisest
ja sellest õppimisest

clarified security
we break security to bring clarity

(Punane Meeskond) **Red Team**

An independent group

that challenges an organization

to improve its effectiveness

by assuming an adversarial role.

(Ründeilmingute otsimine) **Threat Hunting**

Pro-actively searching for attack indicators &

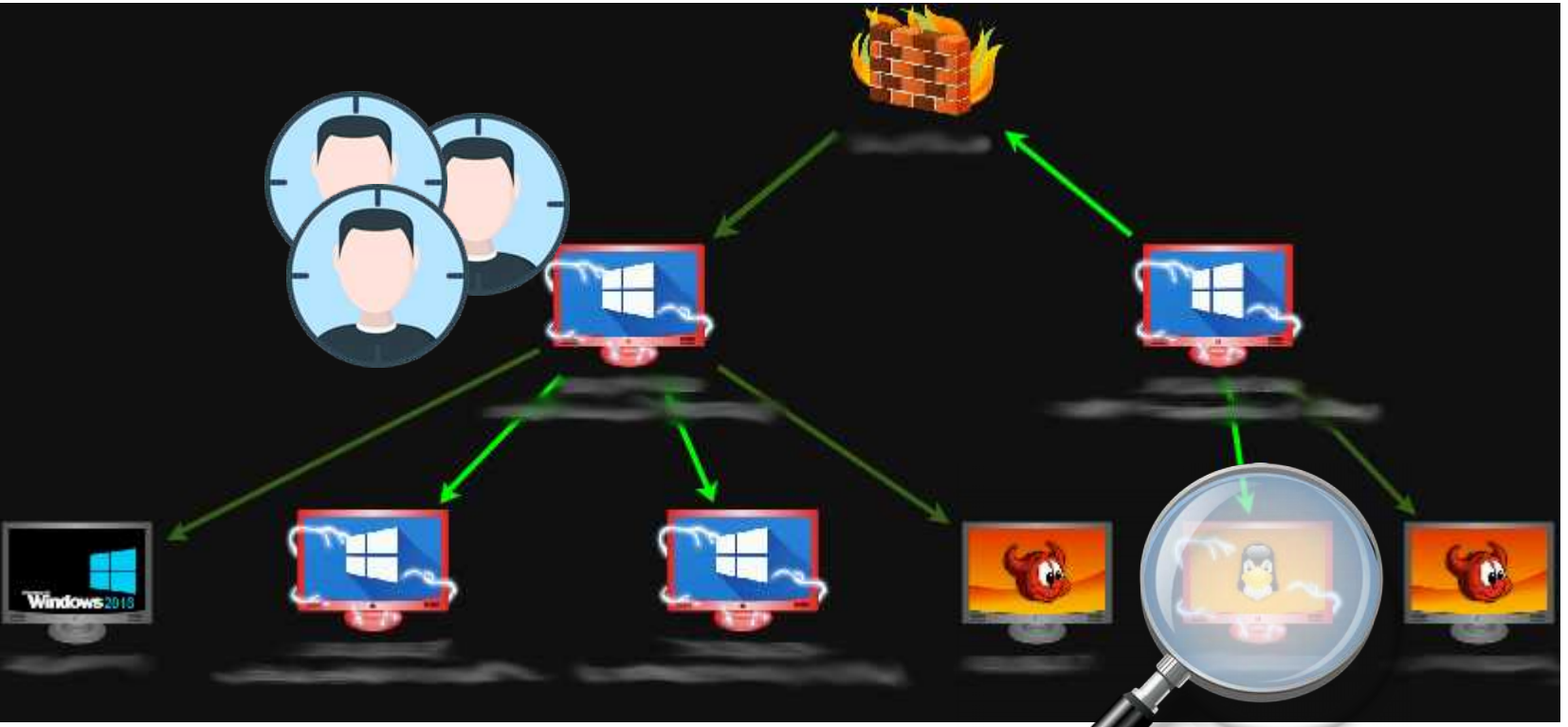
attackers that are lurking in your network.

(assume that you are / will get compromised)

Are you an attractive target? To whom & why?

clarified security
we break security to bring clarity

Red Teaming *(kui otse ei saa, siis ringiga)*



OS?

AV?

…

Browser(s)?

What Office?

MFA?

VPN?

E-mail?

Monitoring?

Threat Hunting?

IR processes?

…

*** Lihtsaima vastupanu teekonnad “kroonjuveelideni”**

Valideerib kogu organisatsiooni turvalisust!

clarified security
we break security to bring clarity

Red Teaming *(Punane Meeskond ründab)*

3-4 nädalat tööd, 3-4 kuu perioodi jooksul

Paljud pakkujad / tellijad alustavad "*assumed compromise*" lähtepunktist

Meie pigem eelistame teostada kogu ründe elutsüklit:

- *OSINT, pre-phishing, (spear) phishing, water-hole & supply chain attacks*
- *living off the land, escalation, lateral movement ... **repeat** → "crown jewels"*
- *Not limited to cyber only (depending on ROE)*

= realistlikum, rohkem (õpi)väärtust organisatsioonile

Küberõppus **vs** oma organisatsioon/IT/turva/vahendid/inimesed/protsessid

Miks sihikindel ründaja on edukas?

Iga õnnestumine ja **ka ebaõnnestumine** viib eesmärgile lähemale!

Kas rünnatav(ad) panevad üksikintsidentidest ka “suure pildi” kokku?

Kohalik küberkuritegevuse “eduloo” näide:

Vladimir **Tšaštšin** (+6) / Rove Digital / **DNS Changer** pahavara …

2010a NASA arvutite nakatamise tõttu sattus FBI huviorbiiti, kannatajateks liskaks ka, eraisikud, Google, Facebook, iTunes ja NetFlix, USA maksuamet

FBI operatsioon “**Ghost Click**” kulmineerus 8 nov. 2011 haaranguga Eestis …

Võttis omakas **4+ miljoni arvuti nakatamise ~100 riigis (~500 000 USAs)**

“monetization” reklaami asendamisega *(vähemalt 14M USD …)*

AGA sellele **eelnes aastaid “radari alt lendamist”** ja **“töö käigus õppimist”**

Kui paljud meist siin väiksel „Maarjamaal” on **järjepidevateks sihitud rünneteks valmis?**

Logging & Monitoring
Threat Hunting
Incident Response
Attribution
Risk Management
...

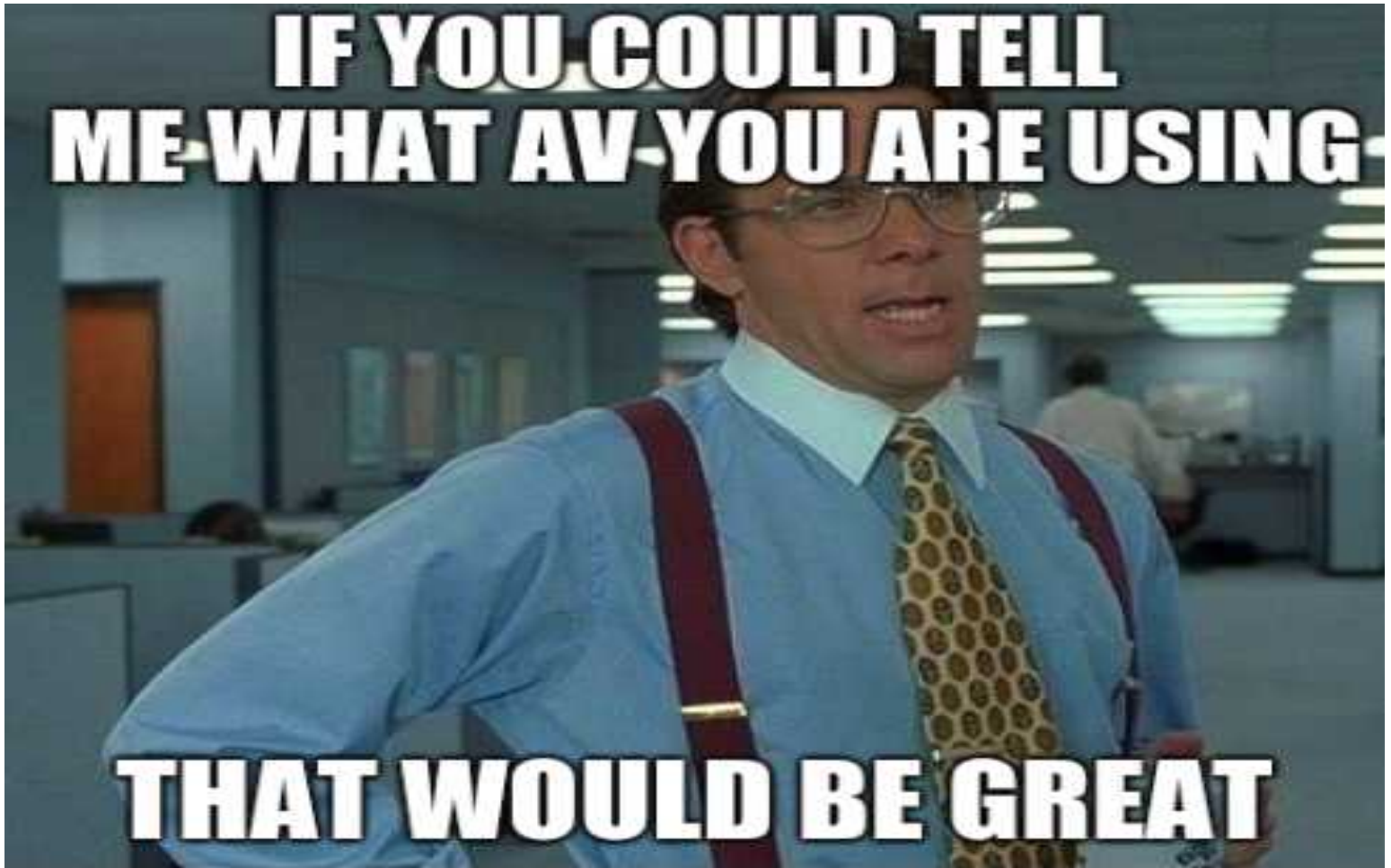
clarified security
we break security to bring clarity

Poduction

RED TEAMING

“war stories”

Kui sa ei tea vastust, lihtsalt küsi!



< jagatavatest slaididest on osa ilmestavast sisust eemaldatud >


ACCESS GRANTED


THANK YOU