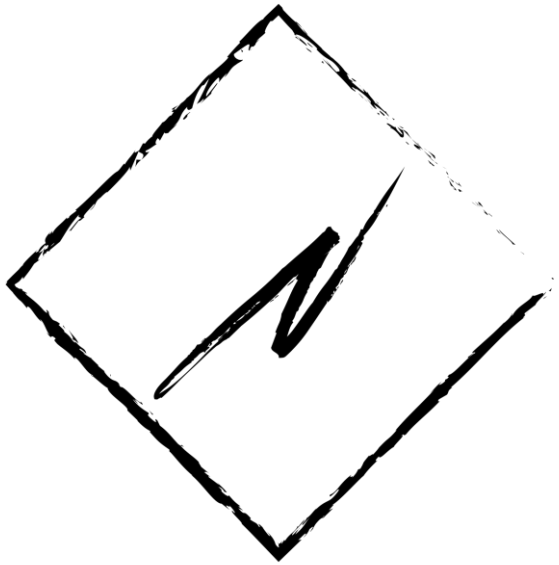
# Ethical hacking and Penetration Testing

Introduction to commercial-grade penetration testing. Building workspace

Author: Kutlymurat Mambetniyazov (@manfromkz)

# Whoami



- Kutlymurat Mambetniyazov (@manfromkz)
- Master of Computer Science
- OSCP, eWPTXv2, eCPTXv2
- Security expert at NitroTeam
- Blog – https://murat.one
- Channel – https://t.me/onebrick
- CVE-2020-29143, CVE-2020-29142, CVE-2020-29140, CVE-2020-29139, CVE-2021-34187

# Identifying the goals of lesson

- Short review of this course
- Understanding basic terms
- Building workspace

# About this course

This course is almost fully practical.

You will learn:

- ethics of hacking
- work with Kali Linux
- various methods of attacking web applications and infrastructure
- scanning networks to find vulnerabilities
- thinking like a hacker
- writing commercial-grade report

# Subjects of this course

1. Introduction to commercial-grade penetration testing. Building workspace
2. Information gathering. Open source intelligence (OSINT)
3. Social engineering techniques
4. Web applications security
5. Web application attacks. Automatic tools

# Subjects of this course

6. Infrastructure security. Reconnaissance
7. Infrastructure attacks. Metasploit Framework
8. Basics of Android application & WiFi attacks
9. Cybersecurity training platforms
10. Writing commercial-grade report

# Basic terms

- **Penetration testing (ethical hacking)** – simulation of hackers' attack
- **Pentester** – specialist, who performs penetration testing
- **Red teams** are offensive security professionals who are experts in attacking systems and breaking into defenses.
- **Blue teams** are defensive security professionals responsible for maintaining internal network defenses against all cyber-attacks and threats.

# Ethics. Hacker manifesto

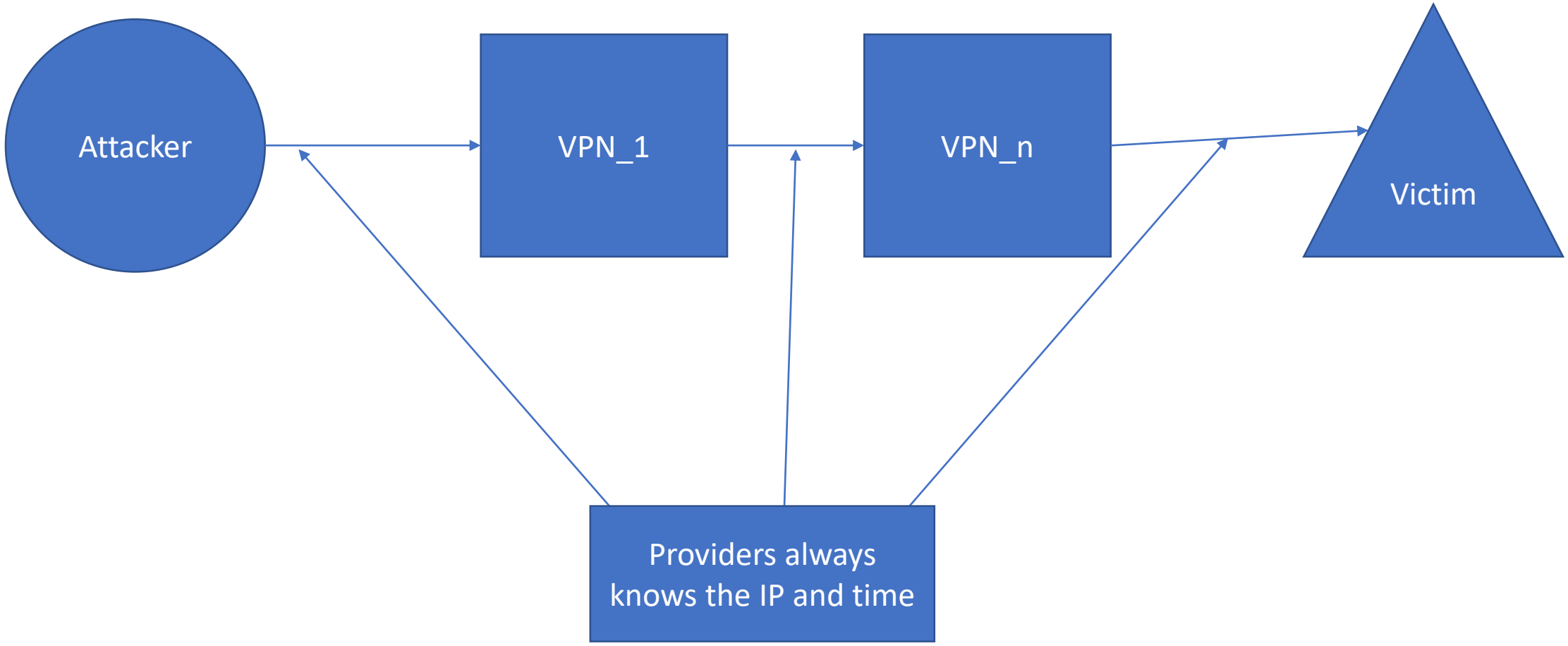
- https://en.wikipedia.org/wiki/Hacker_Manifesto

- ***The Conscience of a Hacker*** (also known as ***The Hacker Manifesto***) is a small essay written January 8, 1986 by a computer security hacker who went by the handle (or pseudonym) of The Mentor (born Loyd Blankenship), who belonged to the second generation of hacker group Legion of Doom.

# Ethics. There is always legit way

- https://www.hackerone.com/
- https://www.bugcrowd.com/
- https://bugbounty.kz/
- https://www.openbugbounty.org/
- https://www.synack.com/
- https://www.intigriti.com/
- and etc.

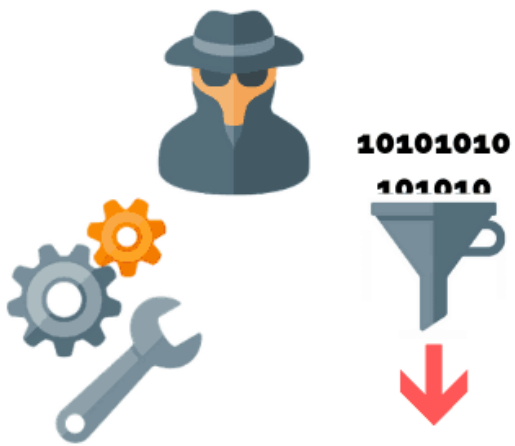
# Ethics. Why bad guys will be catched?

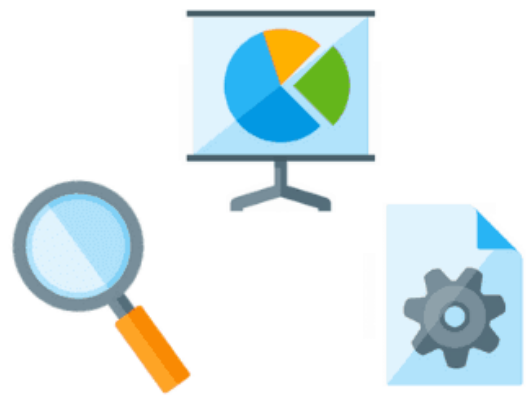


RED TEAM

PURPLE TEAM

BLUE TEAM



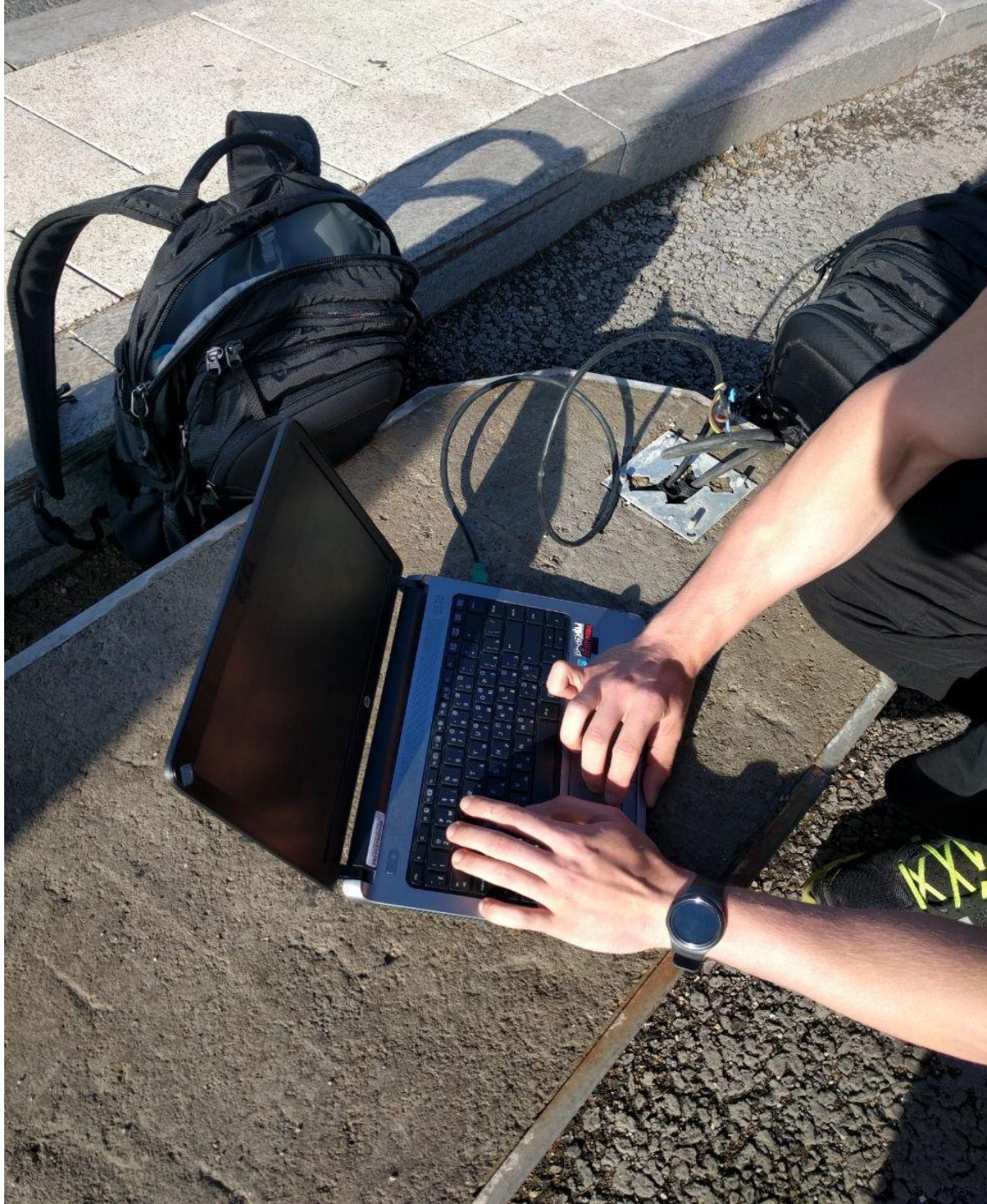




Translate:

- Stop! It is secret government object
- My mom works here
- Welcome

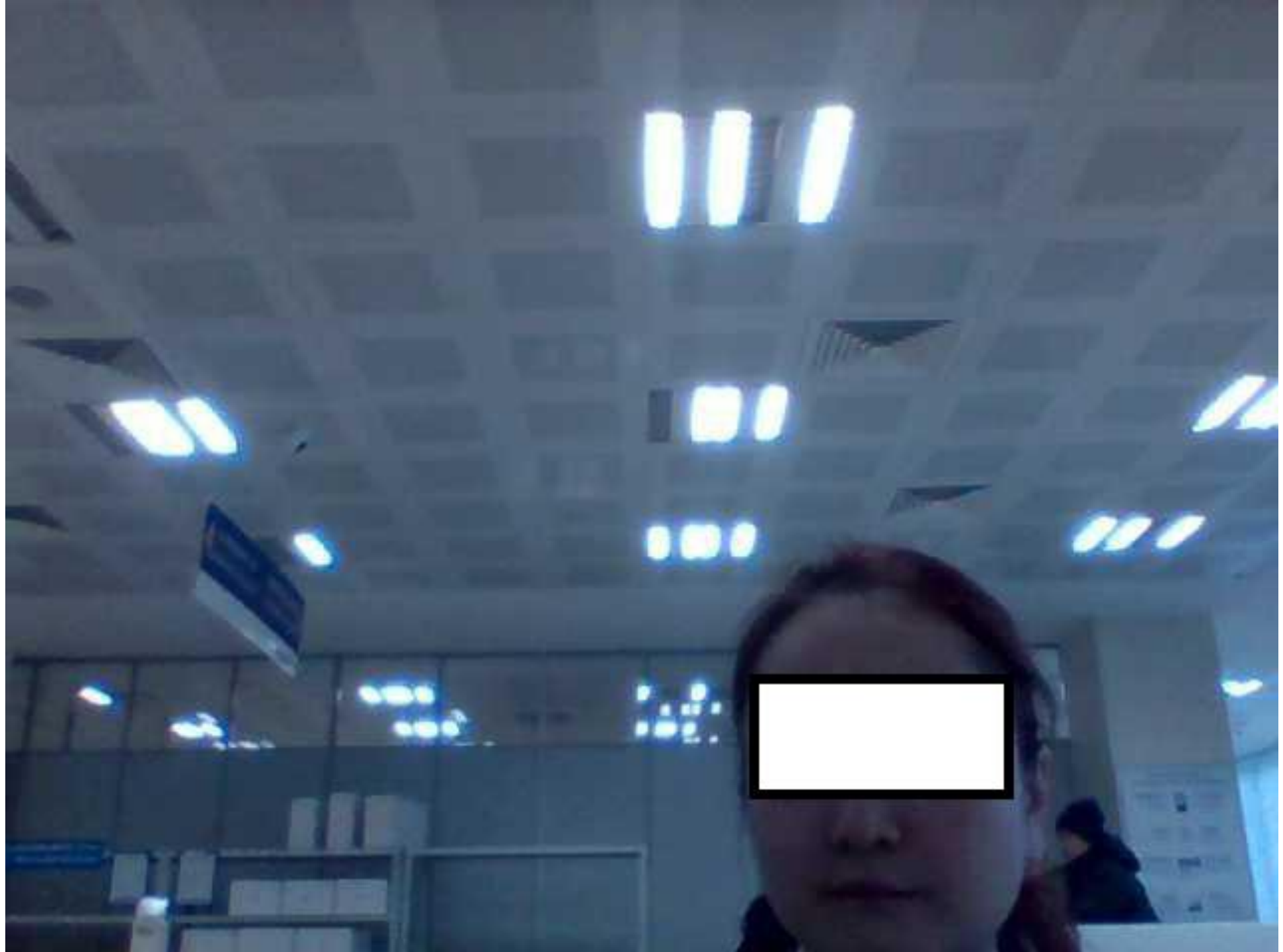
# Interesting cases in Kazakhstan


КРЕДИТТЕР
КРЕДИТЫ



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 172.16.0.1-255
rhosts => 172.16.0.1-255
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[-] 172.16.0.22:445       - An SMB Login Error occurred while connecting to the IPCs tree.
[-] 172.16.0.8:445        - Host does NOT appear vulnerable.
[-] 172.16.0.15:445       - Host does NOT appear vulnerable.
[*] 172.16.0.1-255:445    - Scanned  31 of 255 hosts (12% complete)
[-] 172.16.0.24:445       - Host does NOT appear vulnerable.
[+] 172.16.0.13:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7600 x64 (64-bit)
[+] 172.16.0.20:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[+] 172.16.0.7:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x86 (32-bit)
[+] 172.16.0.17:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64
[!] 172.16.0.7:445        - Host is likely INFECTED with DoublePulsar! - Arch: x86 (32-bit), XOR Key: 0x951FB68A
[+] 172.16.0.20:445       - Named pipe found: netlogon
[!] 172.16.0.17:445       - Host is likely INFECTED with DoublePulsar! - Arch: x64 (64-bit), XOR Key: 0x61781765
[+] 172.16.0.13:445       - Named pipe found: netlogon
[-] 172.16.0.51:445       - Host does NOT appear vulnerable.
[-] 172.16.0.62:445       - Host does NOT appear vulnerable.
[+] 172.16.0.44:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 R2 3790 Service Pack 1 x86 (32-bit)
[+] 172.16.0.44:445       - Named pipe found: netlogon
[*] 172.16.0.1-255:445    - Scanned  70 of 255 hosts (27% complete)
[*] 172.16.0.1-255:445    - Scanned  84 of 255 hosts (32% complete)
[*] 172.16.0.1-255:445    - Scanned 102 of 255 hosts (40% complete)
```



Alfa - https://www.alfa.com.tw/

Raspberry Pi connected to the printer in the hall of our customer.

The most interesting thing, the printer was moved after connecting, but nobody touched the Raspberry Pi.


# Interesting cases in the World


0
10
20
40
60
80

According to a 2018 Business Insider report, cybersecurity executive Nicole Eagan of security firm Darktrace told the story while addressing a conference.

“The attackers used that (a fish-tank thermometer) to get a foothold in the network,” she recounted. “They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud.”

Source: https://www.entrepreneur.com/article/368943

# HIRE ME, DON'T HIRE ME

If F-Secure's red team gets nothing from the garbage, they may try a different approach: applying for a job.

"We have some CVs that will knock your socks off," he says.

The goal here is not to get the job; in fact the team member in question will work quite hard not to get it once they are inside the building. Instead they are trying to get an interview.

"You're inside the building and you say: 'Look my wife is pregnant, it's the doctor, do you mind if I just stay in the meeting room for five minutes?' And they'll leave you," he says.

"You log in with the computer that you've brought and then you call your colleagues saying: 'Did you get in?' and they say: 'Yep we have persistent access', because that little boxy thingy connects out to the network and then climbs back in and we're in."

# Fingerprint is not secure

- https://tjournal.ru/tech/480202-specialisty-oboshli-skaner-otpechatkov-palcev-v-macbook-i-ipad-s-pomoshchyu-plenki-i-kleya
- https://blog.kraken.com/post/11905/your-fingerprint-can-be-hacked-for-5-heres-how/
- https://www.youtube.com/watch?v=VYI9XNO4XzU

# Don’t play with bad USB

- https://en.wikipedia.org/wiki/BadUSB
- https://www.youtube.com/watch?v=e_f9p-_JWZw

# Bonus (offtop)

- https://cs9.pikabu.ru/post_img/2016/12/13/9/1481643187166124581.webm

# List of security hacking incidents from 1903

- https://en.wikipedia.org/wiki/List_of_security_hacking_incidents

## 1900 [ edit ]

### 1903 [ edit ]

- Magician and inventor Nevil Maskelyne disrupts John Ambrose Fleming's public demonstration of Guglielmo Marconi's pur wireless telegraphy technology, sending insulting Morse code messages through the auditorium's projector.[1]

## 1930s [ edit ]

### 1932 [ edit ]

- Polish cryptologists Marian Rejewski, Henryk Zygalski and Jerzy Różycki broke the Enigma machine code.[2]

### 1939 [ edit ]

- Alan Turing, Gordon Welchman and Harold Keen worked together to develop the Bombe (on the basis of Rejewski's works Enigma machine's use of a reliably small key space makes it vulnerable to brute force.

# Pentest models

- PTES - http://www.pentest-standard.org/
- OSSTMM - https://www.isecom.org/OSSTMM.3.pdf
- ISSAF - https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521
- NIST-800–115 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

- Reviewing models - https://www.vumetric.com/blog/top-penetration-testing-methodologies/

# PTES

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

# PTES. Pre-engagement Interactions

- This step is carried out to verify the customer's need, scope of tests and the mapping of parameters to perform vulnerability tests.

- Remember, a penetration test should not be confrontational. It should not be an activity to see if the tester can "hack" you. It should be about identifying the business risk associated with and attack.

# PTES. Intelligence Gathering

- Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.

# PTES. Threat Modeling

- With the information collected, the attacker will determine the impact he can have with what he has in hand, thus developing methods to try to compromise the target system.

# PTES. Vulnerability Analysis

- In this phase, pentester looks for security holes that can lead to exploitation, discovering holes in the implementation or application code.

# PTES. Exploitation

- It is one of the crucial phases, as the exploitation of the vulnerabilities found will be carried out, either using a public or private exploit to try to invade or compromise a target.

# PTES. Post-exploitation

- After compromising your target, the post-exploitation phase ensures that you get persistent access to the target, escalate privileges to have an administrative-level user, perform lateral movements and pivoting to try to compromise other machines on the same network or in an internal subnet

- *We will try Covenant C2 or Merlin.*

# PTES. Reporting

- It is the final phase, but it must also be the beginning, because each step taken during the tests must be properly documented and detailed, my recommendation is that you have 2 reports. The first is the production report, that is, the tests that you carry out and document, even work it as a timeline report. The second is the final report, which you will present to Management and your chosen technical team.

# Pentest types

- Black box
- Gray box
- White box

# Attack preventing frameworks

- Cyber Kill Chain - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- MITRE ATT&CK - https://attack.mitre.org/

- Example, APT (Advanced persistent threat) list - https://attack.mitre.org/groups/

# Pentest checklists

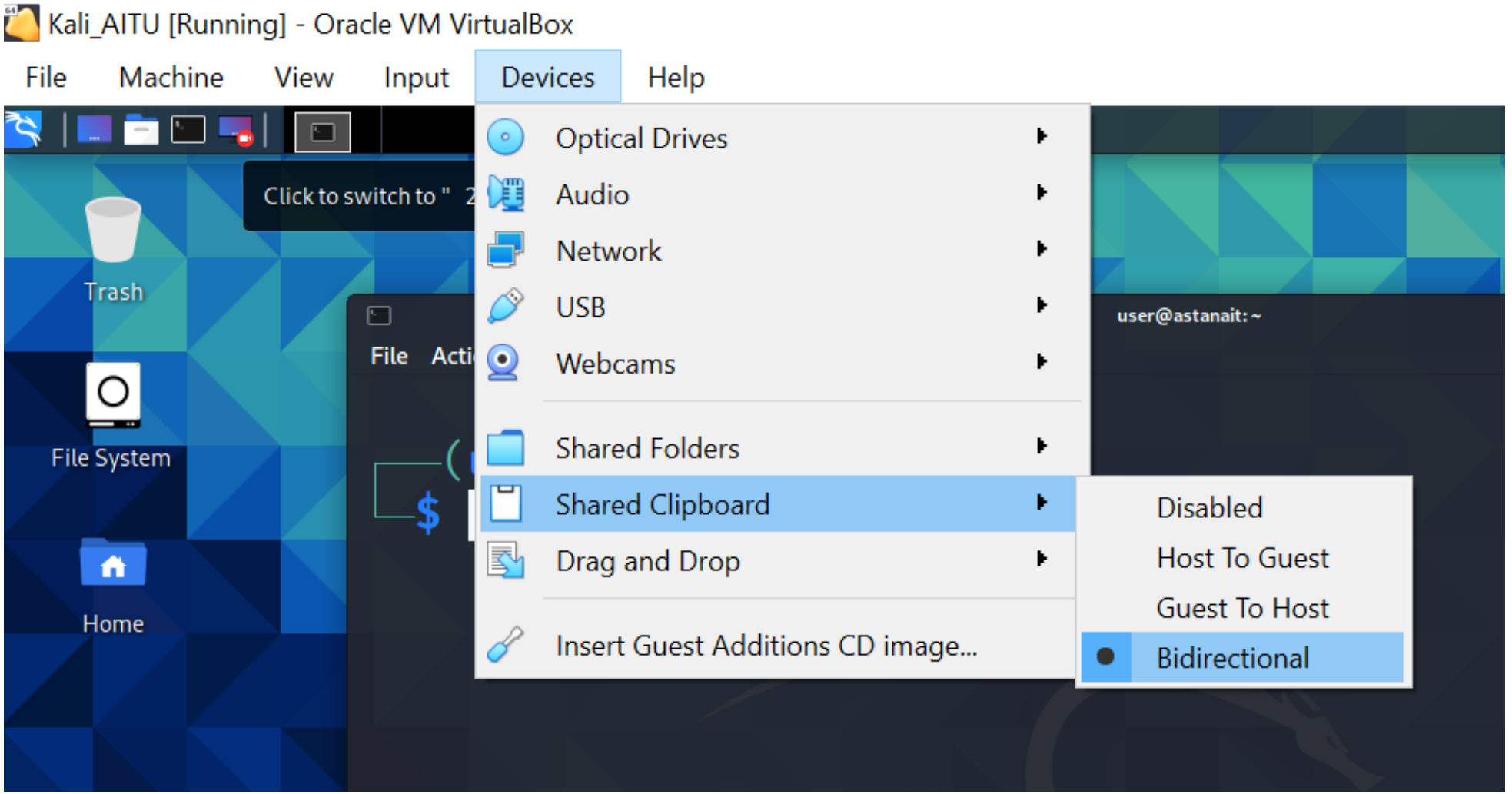
- https://github.com/0xRadi/OWASP-Web-Checklist
- https://pentestbook.six2dez.com/others/web-checklist

# Building workspace

# Installing Kali Linux on VirtualBox

- https://kali.download/virtual-images/kali-2021.4a/

# Insert Guest Additions, then turn on clipboard



# Installing Metasploitable

- https://sourceforge.net/projects/metasploitable/

# Installing OWASP Juice Shop

- https://github.com/juice-shop/juice-shop

# Installing WebGoat

- https://github.com/WebGoat/WebGoat

# Additional environments

- https://www.vulnhub.com/
- https://github.com/vulhub/vulhub

Any questions?

# Homework for the next lesson

- Install Kali Linux, WebGoat, Juicy Shop, Metasploitable
- Sign up at Tryhackme, Hackthebox, PriviaHub

# Useful links

- https://purplesec.us/red-team-vs-blue-team-cyber-security/
- https://blog.kraken.com/post/11905/your-fingerprint-can-be-hacked-for-5-heres-how/
- https://nitroteam.kz
- https://murat.one
- https://verdict-encrypt.nridigital.com/verdict_encrypt_summer18/a_day_in_the_life_of_a_cybersecurity_red_team
- https://en.wikipedia.org/wiki/Advanced_persistent_threat
- https://owasp.org