



Advanced Cybersecurity Essentials Workshop

Dr. Amin Hasbini

Previous labs/Homework

So.. Please tell me your Linux story, any issues?

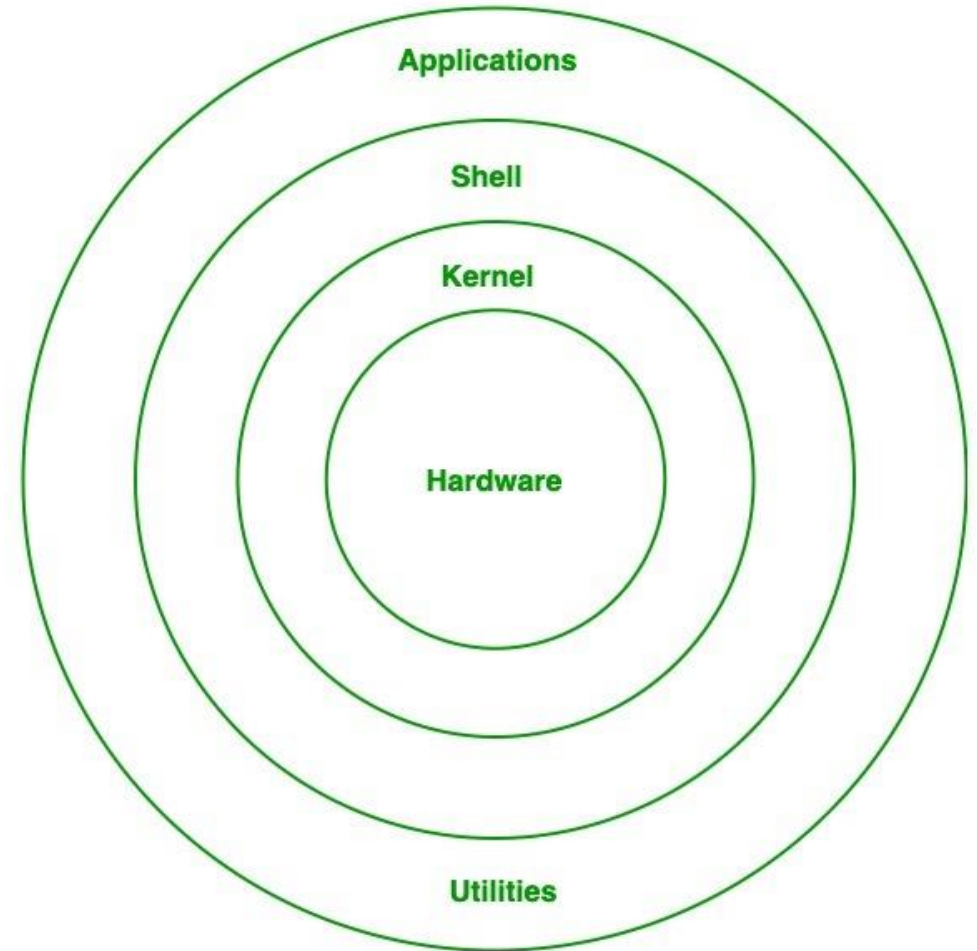
- Install Ubuntu linux, check bash terminal, gnome desktop
- Import windows 10 VM to virtualization app
- Configure virtual machines for NAT to internet
- Fully update virtual machines

Lab2 / homework

- Install Ubuntu linux in VM (using downloaded ISO image)
- Explore Linux terminal: <https://hackr.io/blog/basic-linux-commands>
- Install/play ninvaders via terminal
- Online emulators (limited)
 - <https://bellard.org/jslinux/>
 - <https://www.webminal.org/>

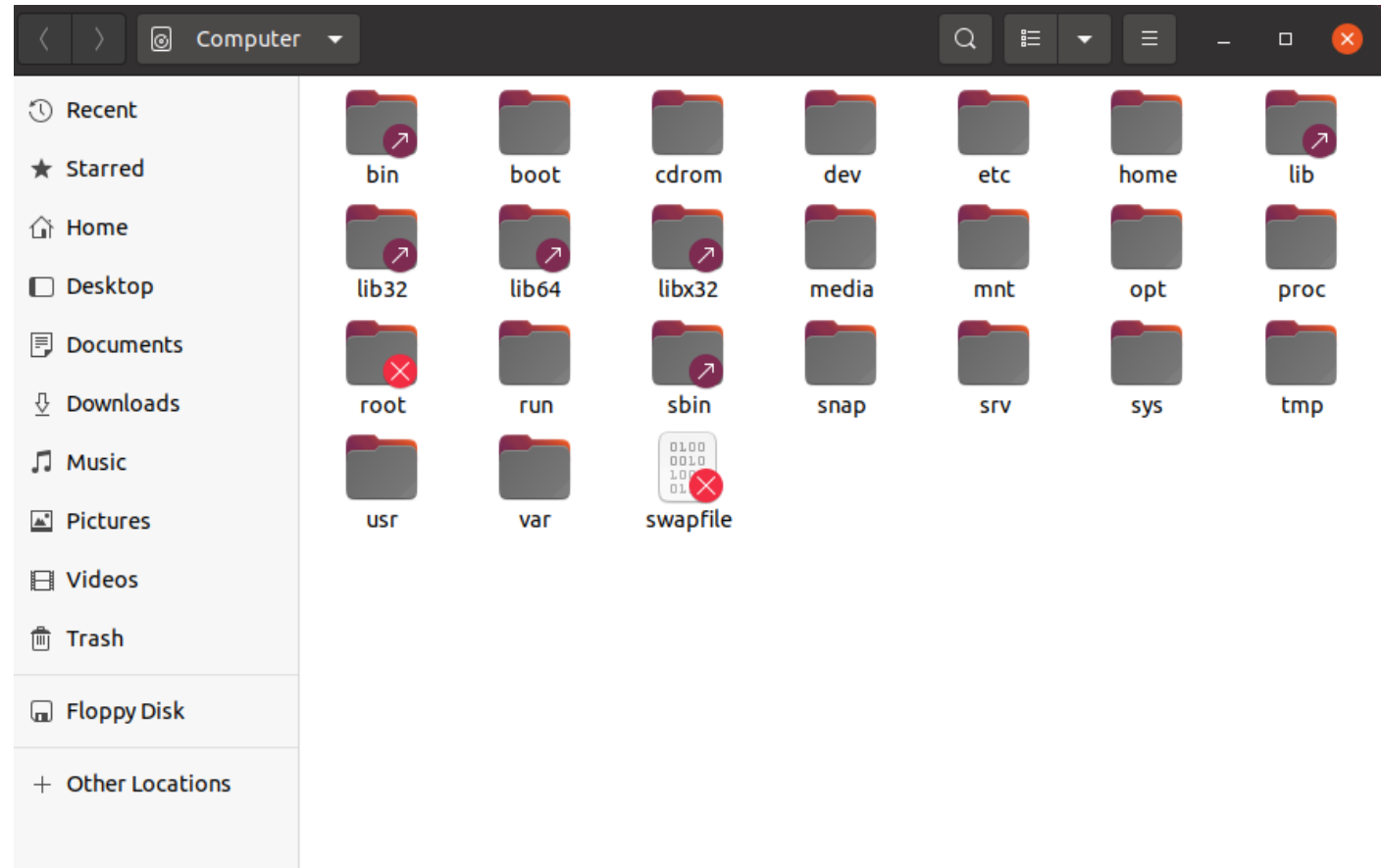
Linux introduction/demo

- Environment
- Application sources
- Advantages: opensource, community support, flexibility
- Disadvantages: not very user-friendly, support/drivers



Linux directory structure: /

- /boot: boot files
- /cdrom
- /dev
- /etc
- /home
- /lib
- /sbin: administration binaries
- /usr: user binaries
- /var: variables, logs...



Few top used tools/commands

pwd, ls, cd, touch, cat, more, sudo, apt, nano, vi, grep, find

So... Amin, how is Linux
cybersecurity?!

Module 2 Ethical hacking and penetration testing

Dr. Amin Hasbini

Disclaimer (again)

- We are whitehat ethical hackers
- Anyone can easily get in trouble
- We are focusing on the most important concepts

Important concepts for penetration testing

Kinds of hackers

- Blackhat
- Whitehat
- Greyhat
- ...
- Scriptkiddie
- State sponsored
- Hacktivist
- Insider

... ?



Types Of Hackers

**HACKER
COMBAT**
COMMUNITY

@hackercombat

Black Hat



Malicious Hackers

White Hat



Ethical Hackers

Grey Hat



Not Malicious Or
Ethical (Mix Of Both)

Green Hat



New To Hacking

Blue Hat



Vengeful Hacker

Red Hat



Vigilante Hacker

@hackercombat

@hackercombat

Types of Hackers



Black Hat



Black Hat
Hackers



Suicide
Hackers



White Hat



White Hat
Hackers



Red Hat
Hackers



National Supported
Hackers



Grey Hat



Grey Hat
Hackers



Malicious
Insider

Junior Hackers



Script
Kiddies



Green Hat
Hackers



Blue Hat
Hackers

 IpCisco.com

Kinds of attacks

- Malware
- Phishing
 - Spear Phishing (via social engineering)
 - Whaling (via executives)
 - Pharming (via DNS redirection)
- Denial of service / Distributed Dos/DDos
- Database SQL injection
- Zerodays exploit
- APT
- ...

What is social engineering?

- 5 min search

Social engineering

- Online
- Offline (freebies!)

If there are problems with how this message is displayed, click here to view it in a web browser.

From: Wells Fargo Online <atmarin@calpoly.edu>
To: Recipients
Cc:
Subject: Your Account Has Been Compromised.

WELLS FARGO [wellsfargo.com](https://www.wellsfargo.com)

Your Account has been restricted, unlock

Your account has been limited for security reason to keep your account safe note all your transaction will be monitored to enhance your security.

To Unlock click on the below link and follow the security check Questions:

Go to <http://www.wellsfargo.com/secure>
Answer the security questions carefully and correctly.
After you answer all the security question has been answer you dont have to do anything.

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements online, Wells Fargo Customer Service is available 24 hours a day, 7 days a week. Call 1-800-368-2211 or sign on to https://www.wellsfargo.com/privacy_security/fraud Click to follow link

[wellsfargo.com](https://www.wellsfargo.com) | [Fraud Information Center](#)

Please do not reply to this email directly. To ensure a prompt and secure response, sign on to email us.

213405-168-a5ed-117d3a1aa2-b28b65a2_5716fc7a_131b0-721

Important Notice- Fix Incoming Email issues - Message (HTML)

File Message Help

Ignore Delete Archive Reply Reply Forward Move Mark Categorize Follow Unread Translate

Important Notice- Fix Incoming Email issues

To: [Redacted]

exchange

Incoming messages for [Redacted] couldn't be delivered.

Action Required Confirmation

Fix Email issues below

This message was sent in response to multiple incoming messages being rejected consistently from 2:00 AM, Wednesday, August 19, 2020.

To fix, recover and prevent further rejection of emails by our server, connect to your Company-Assigned OWA portal securely below.

[https://portal.\[Redacted\].lwa](https://portal.[Redacted].lwa)

naked security by SOPHOS

Bank Of America <noreply@isp.org>
To: [Redacted]
Account Update

TechTerms.com

Bank of America

Dear Valued Customer :

As part of our security measures, we regularly screen activity in the Bank of America Online Banking system.

We recently contacted you after noticing an issue on your account .

We requested information from you for the following reason:

Our system requires further account verification.

To restore your account, please [Sign in to Online Banking.](#)

Always hover over the URL to make sure it is legitimate before clicking it.

[http://tinyurl.com/\[Redacted\]](http://tinyurl.com/[Redacted])

Dear user, congratulations!

We want to thank you for being a loyal Google India user! Your IP address [Redacted] has been randomly selected to receive a **FREE Apple iPhone X.**

From time to time we select a handful of Google users to give them the opportunity to receive valuable gifts from our partners and sponsors. This is our way of thanking you for choosing Google as your preferred search engine.

Today is your lucky day! You are one of the 10 randomly selected users who will receive this gift.

To receive your gift, you simply have to complete our short and anonymous survey. But hurry! There are only a few gifts available today!

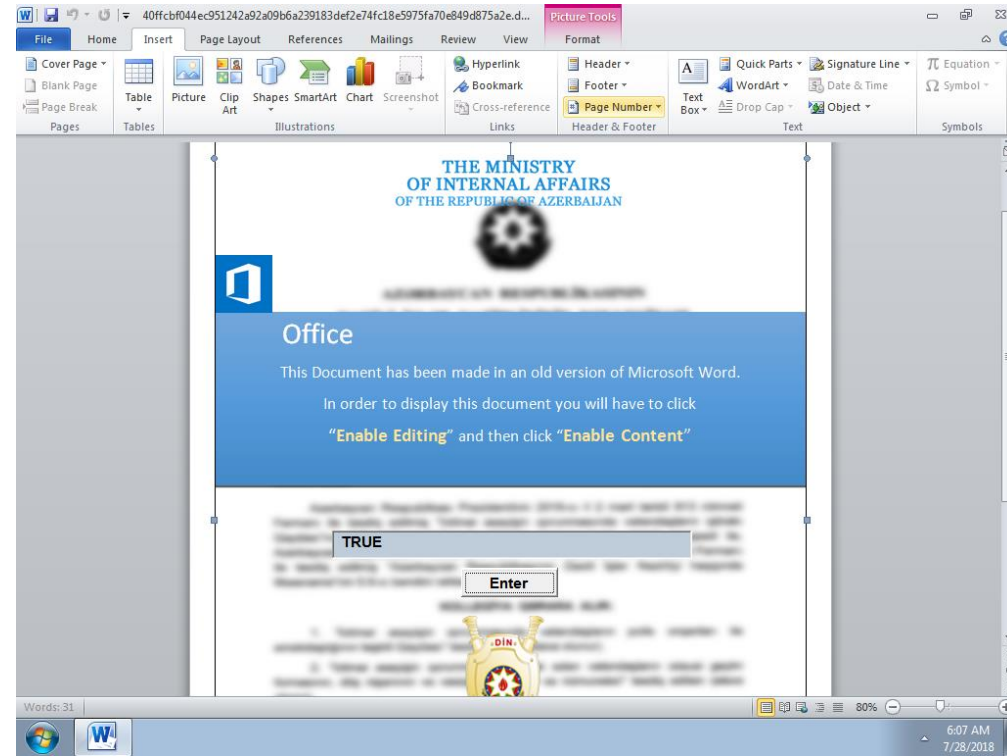
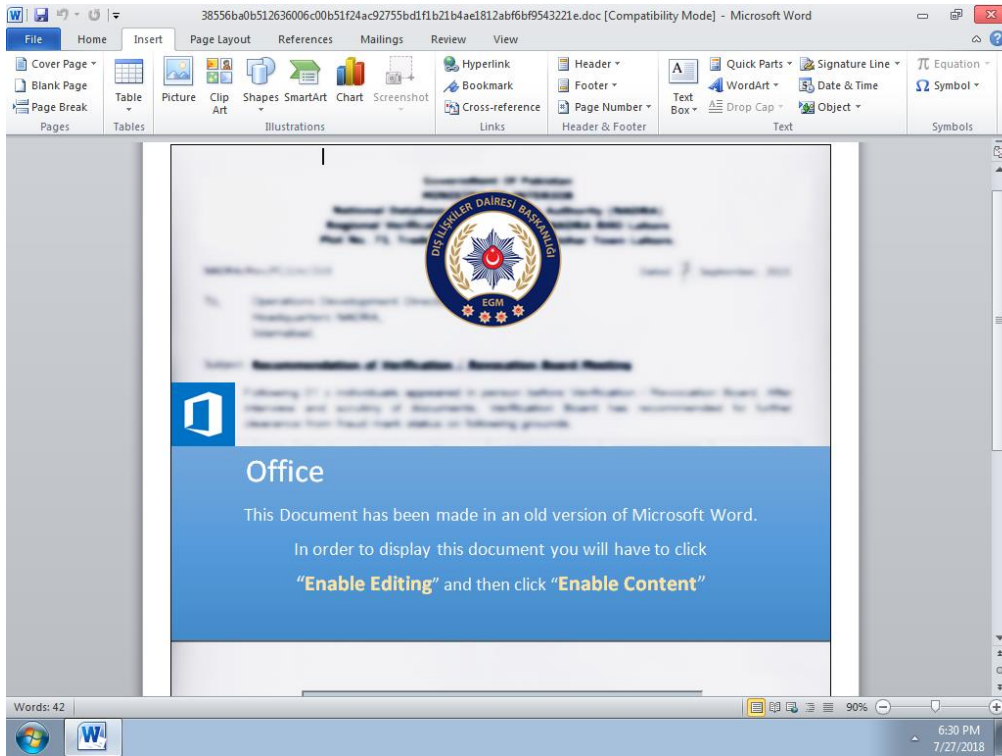
How satisfied are you with Google?

Very Satisfied

Satisfied

Unsatisfied

Social engineering: malicious macro scripts



<https://securelist.com/muddywater/88059/>

This document is TLP RED

Social engineering file tricks

- Zerodays (office docs, zip, pdf, chm, swf, browser, imessage, whatsapp)
- Office/Macros, VBS...
- .exe
- .bat
- .scr
- .lnk
- .url
- ...

Phishing

- Spear phishing
- Whaling (senior execs)
- Pharming (DNS poisoning)



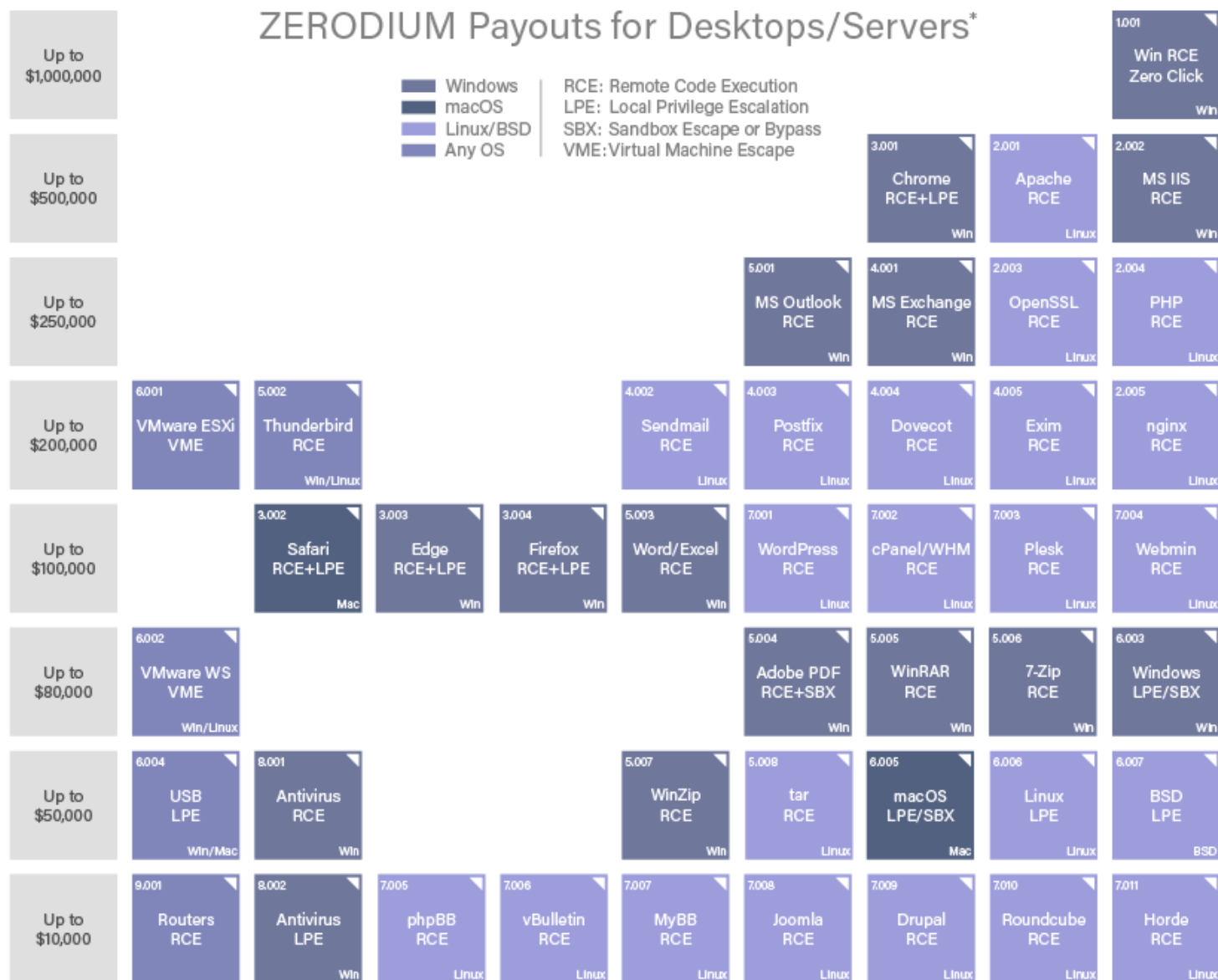
<https://www.funinformatique.com/cours/quest-ce-que-le-phishing-et-comment-sen-proteger/>

What is a zeroday?

- 5 min search

Zerodays

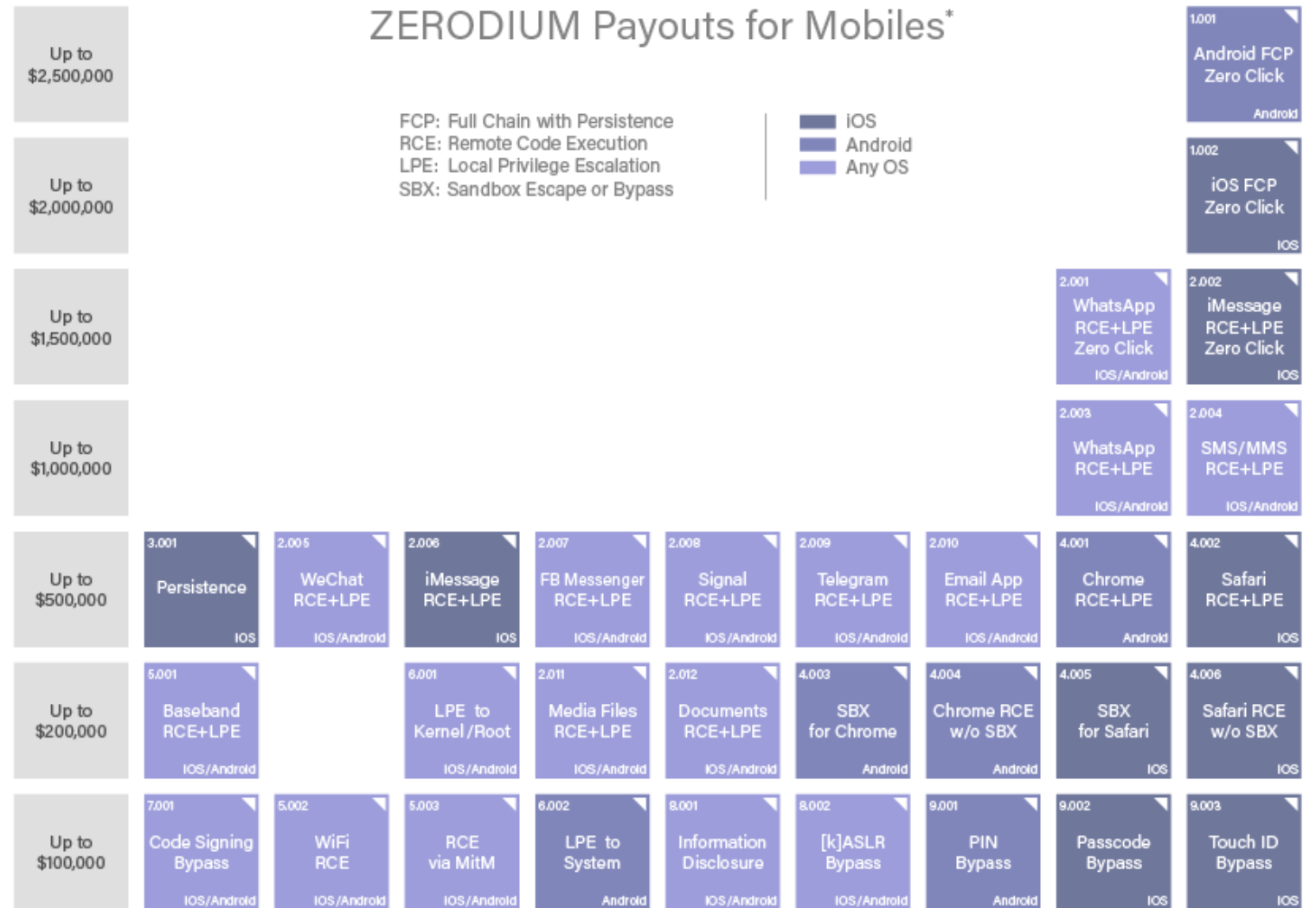
- Fresh exploits
- Previously unknown weaknesses



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

Zerodays



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

But Amin, aren't zerodays illegal?

What is an APT?

- 5 min search

APT Advanced persistent threats

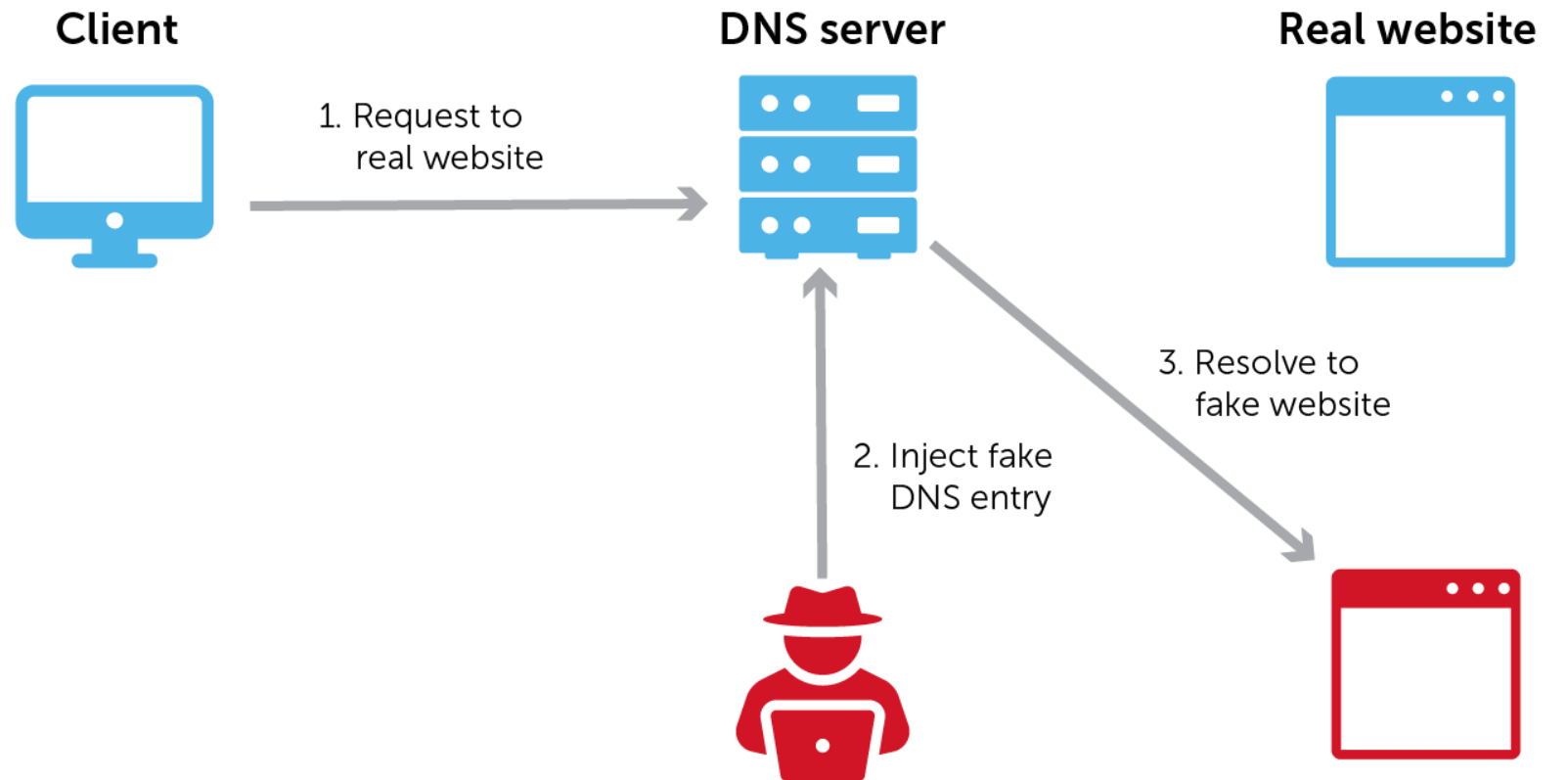
APT	Malware
The APT is well funded, organized groups that are systematically developed to compromise government and commercial entities.	Malware is any malicious software or program designed to damage or disable computers or networks.
APT is a broad term used to describe a prolonged, more strategic and targeted attack.	Most malware attacks are target-specific, quick damaging attacks.
APTs can stay undetected for a prolonged period.	Anti-malware can detect and eradicate malware.
APTs are targeted attack on sensitive, corporate, banking networks to maintain access to their networks and infiltrate intellectual property data.	Most malware attacks are aimed at a specific user, company, or organization to gain access to their sensitive or personal data in a stealthy manner. 

What are the most common DNS attacks?

- What is DNS?
- 5 min search

DNS attacks

- DNS compromise
- DNS poisoning
- ...



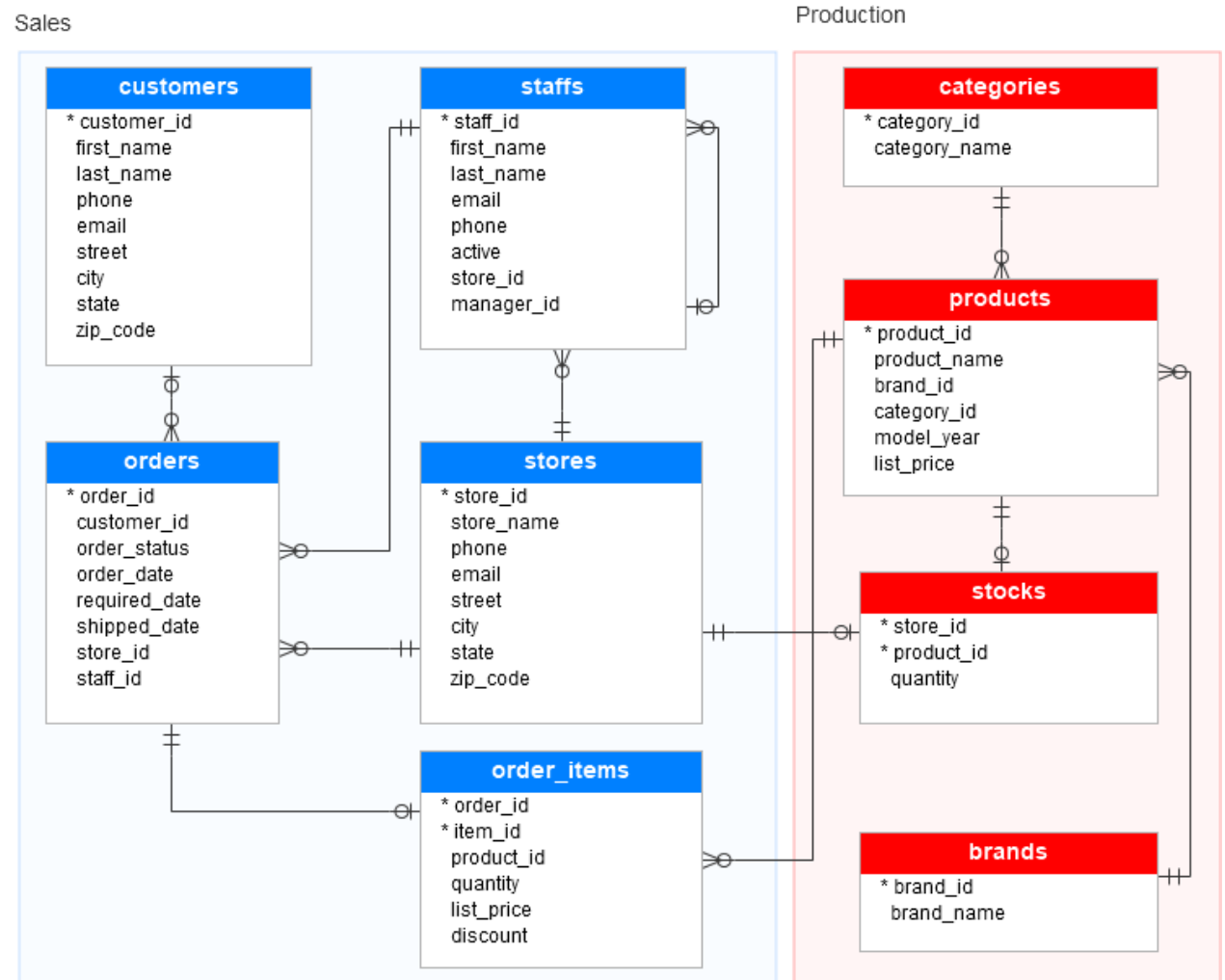
What is SQL injection?

- What is a database?
- 5 min search

Databases and SQL

- Store organized records of data
- Easily access/search stored data
- Example SQL query:

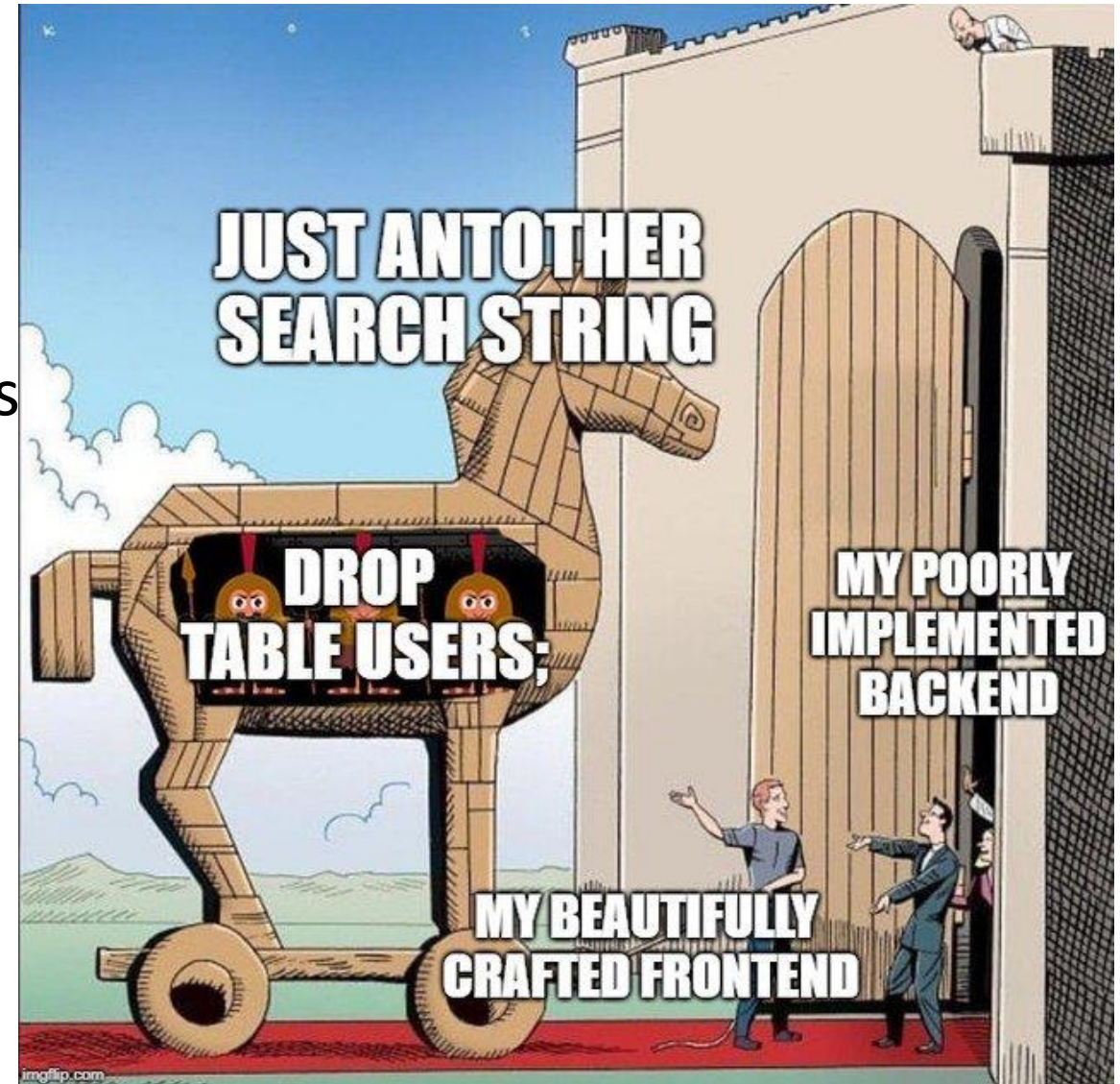
***SELECT order_status from orders
where customer_id = 12022 and
where order_id=128397***



Example shopping store DB

SQL injection

1. A database stores data records
2. A SQL query returns one/few record/s
3. Can we extract/steal records?
4. Can we execute commands?



The magic of 'or 1=1



Authentication Error: Bad user name or password

Please sign-in

Name

Password

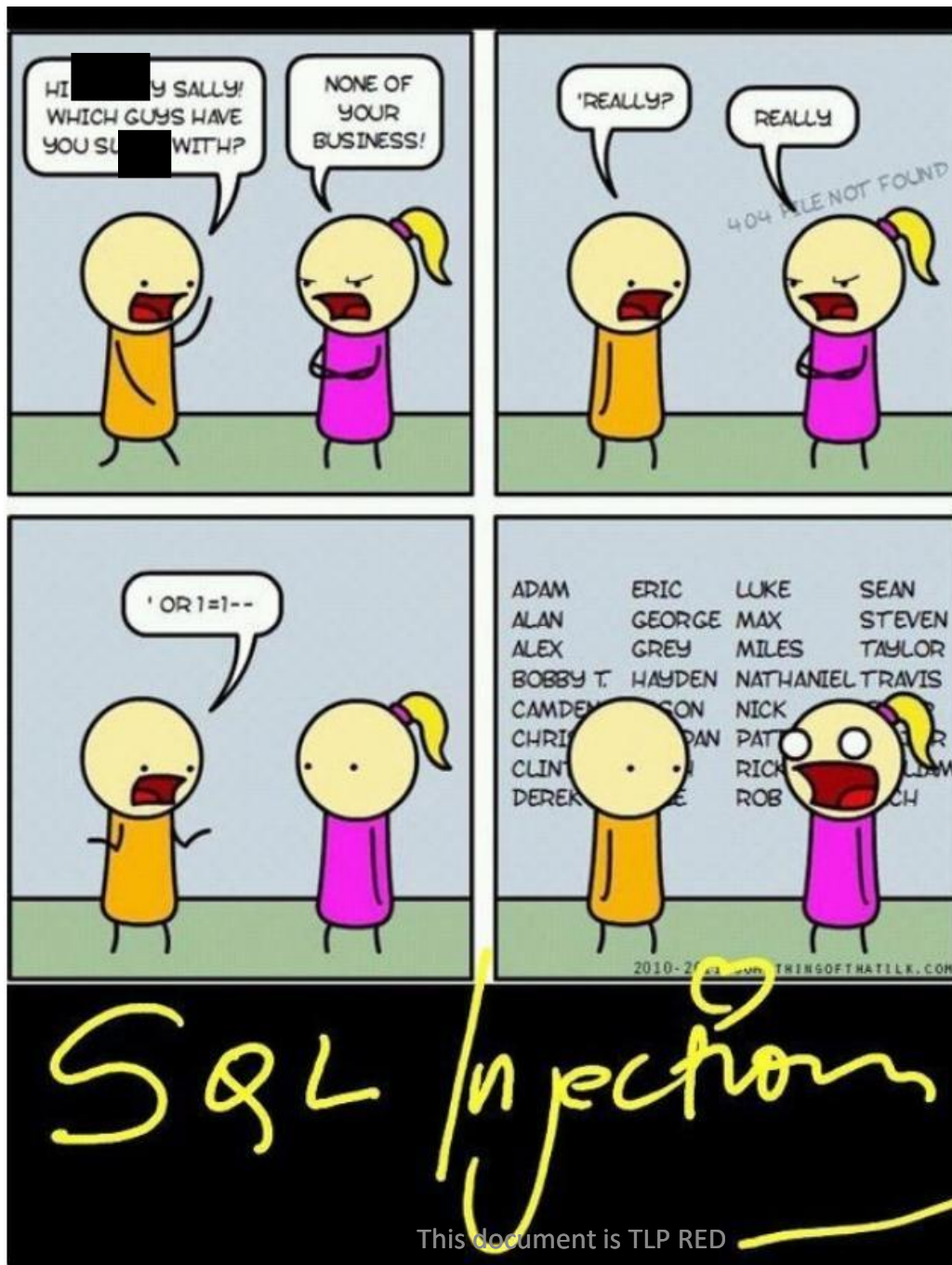
Login

Don't have an account? [Please register here](#)

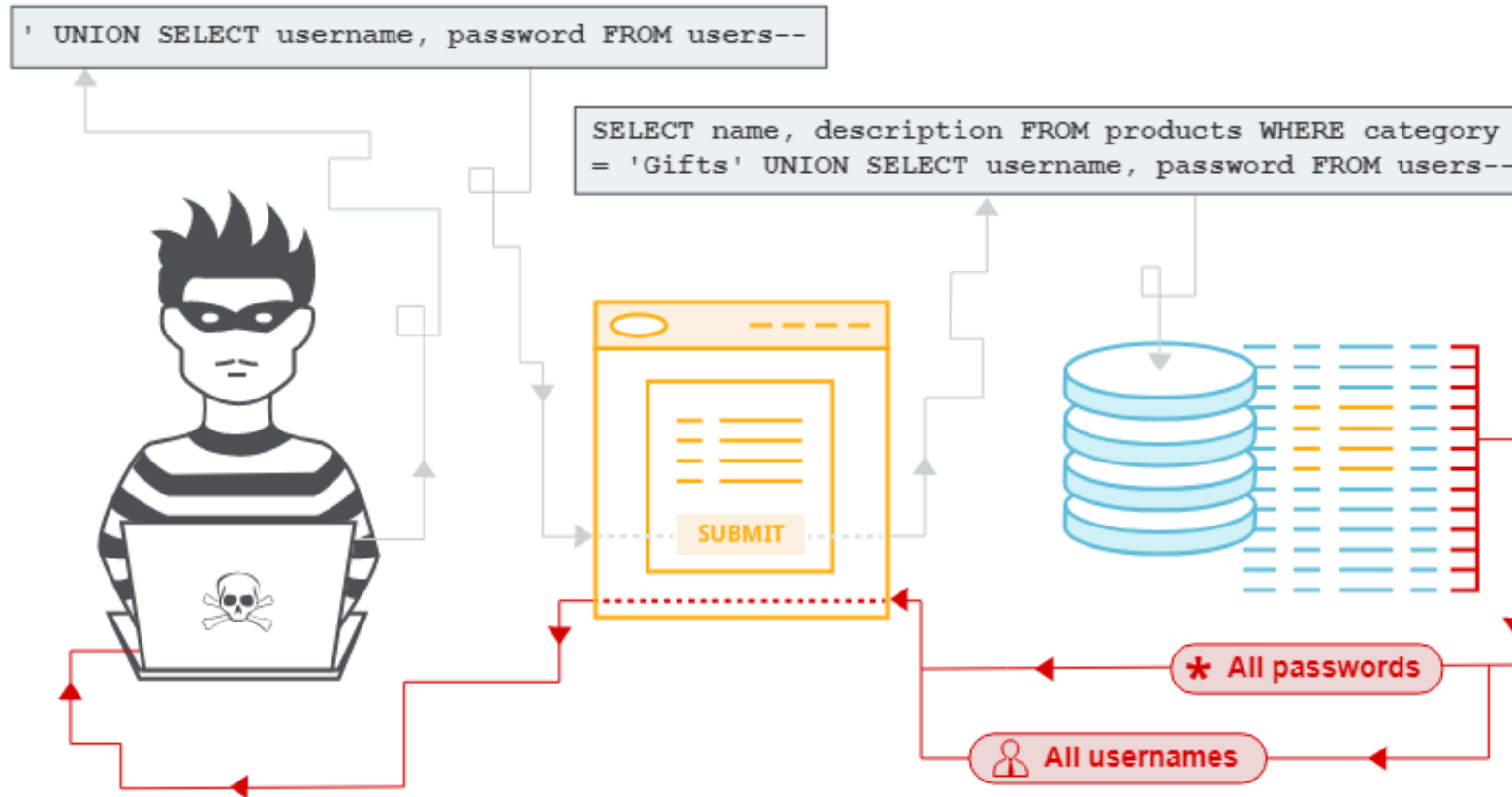


***SELECT order_status from orders
where customer_id = 12022 and
where order_id=128397 'or 1=1***

- ⇒ Query is always true
- ⇒ valid for all DB entries
- ⇒ will then return all table entries as the query result



SQL injection – a more elaborate example

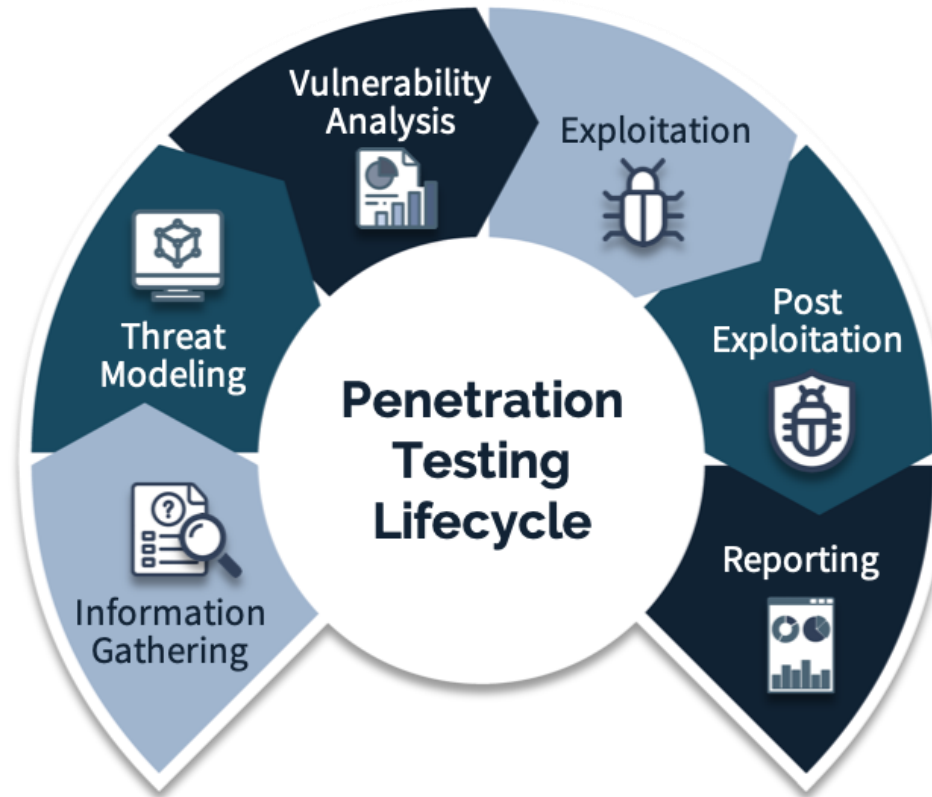


Penetration testing lifecycle

There are multiple representations of the penetration testing lifecycle

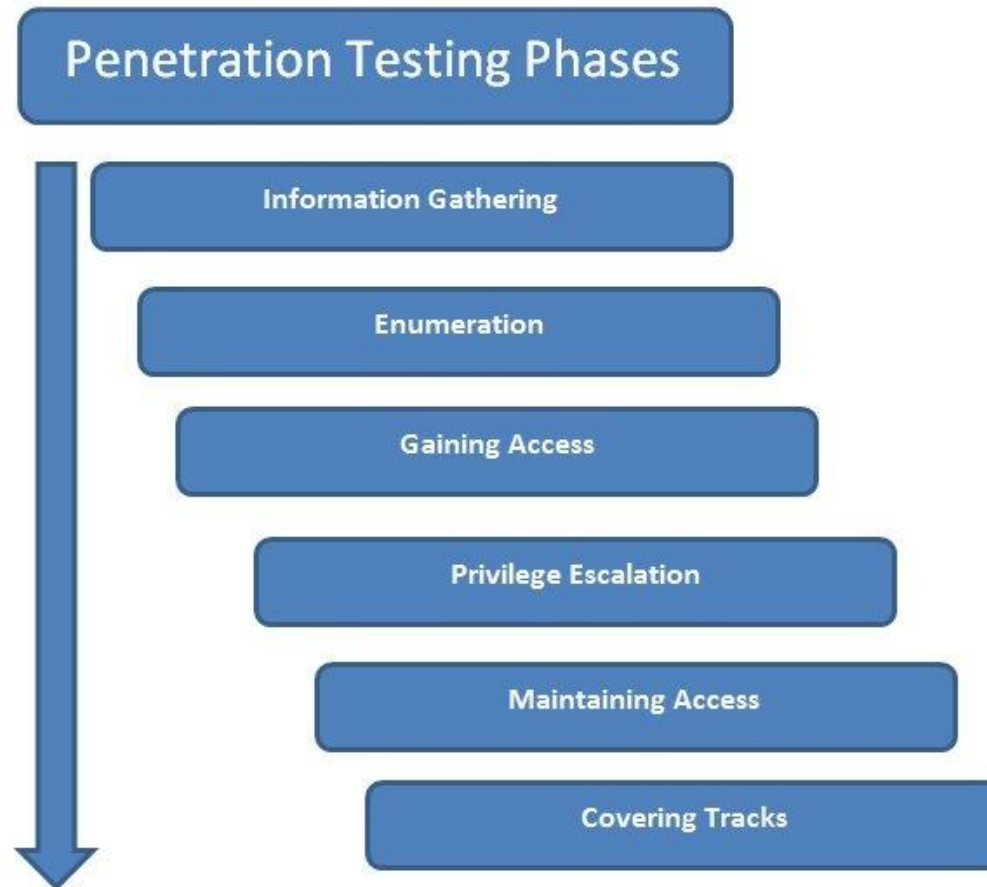
- EcCouncil, IBM, ISS, Mcafee foundstone, OSSTMM, ISSAF, NIST, OWASP, MITRE...

Penetration testing / traditional controlled process

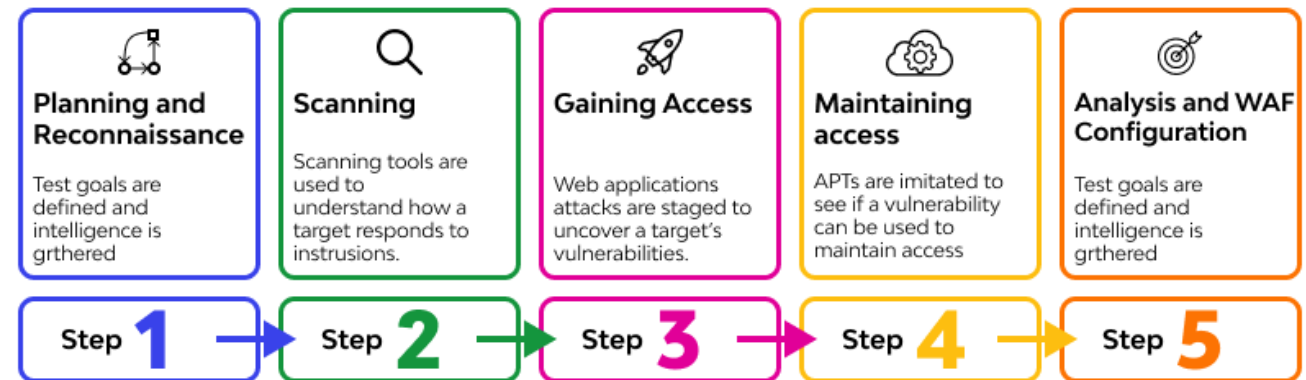


https://www.secornite.com/index.php/onepress_service/penetration-and-red-team-testing/

Penetration testing / Red teaming / cyberattack simulation



And some more...



<https://www.wallarm.com/what/what-is-penetration-testing>

• • •



MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Cyber Kill Chain

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/
Anti-forensics
- Denial of Service
- Exfiltration

<https://www.varonis.com/blog/mitre-attck-framework-complete-guide>

1-Get approvals!

- On scope
- On exploitation and actions allowed

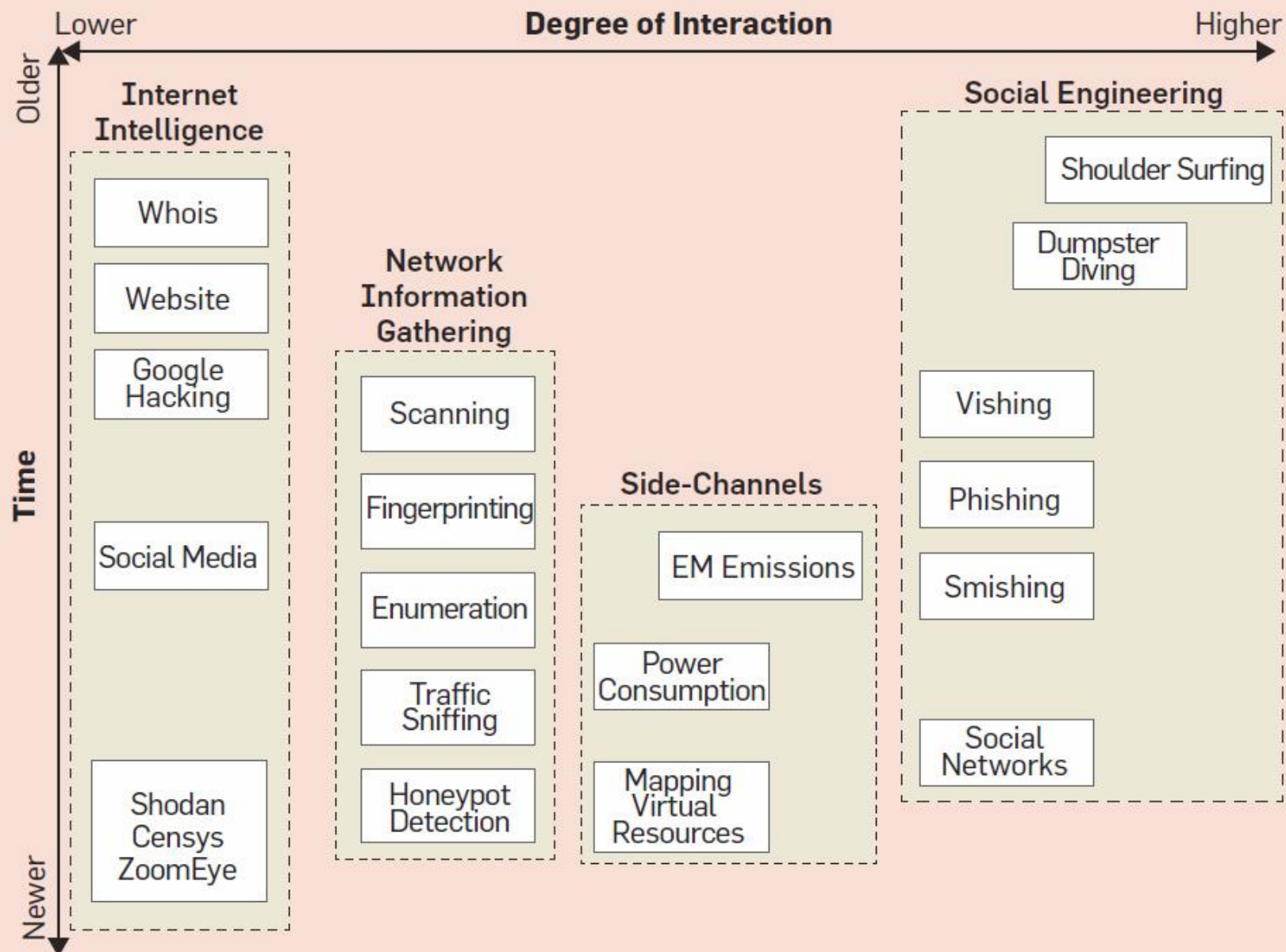
2- Specify and stay within the scope of work

- Kind of pen test (blackbox, greybox, whitebox)
- Subnet, domains, systems
- Attack options, damage risk extent
- Evidence collection extent
- Stakeholders

3-Reconnaissance passive and active

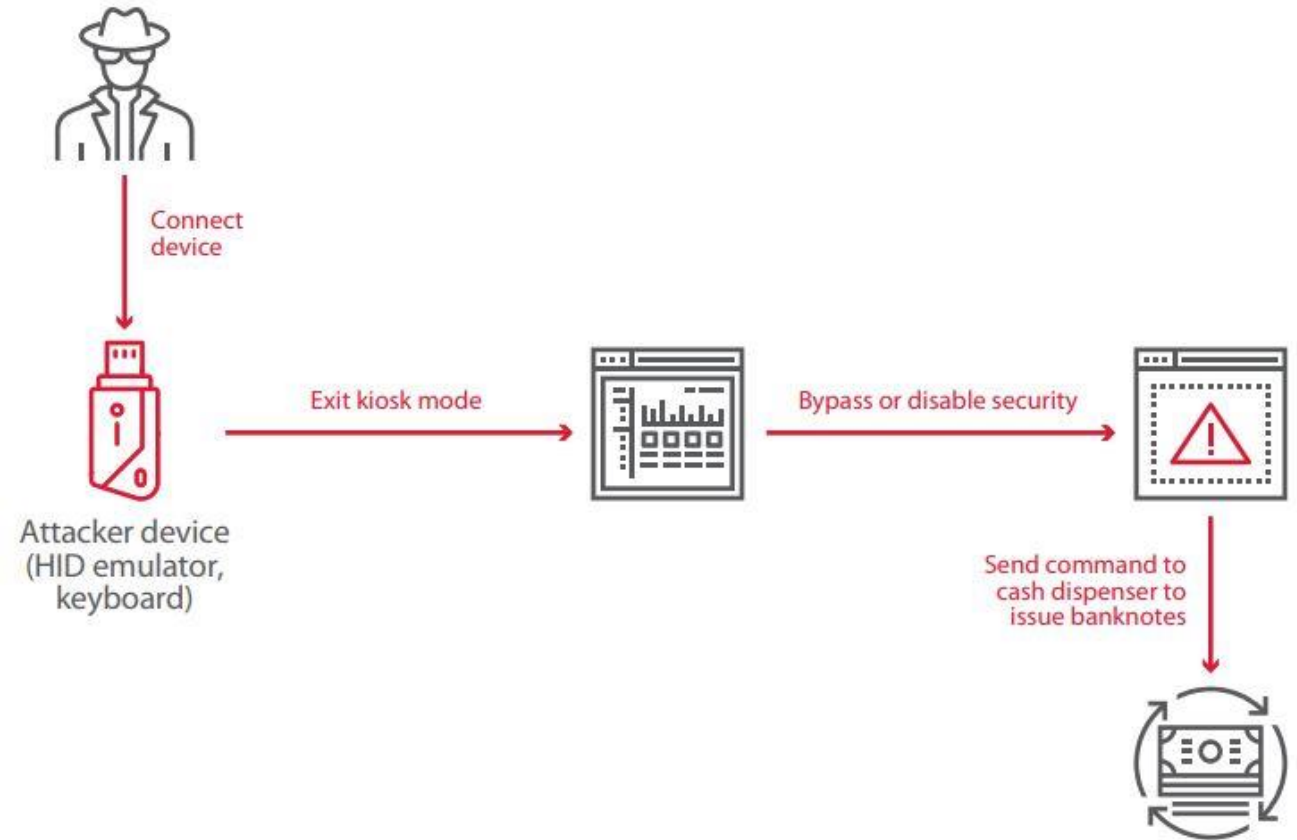
- Target identification
 - Target profiling
 - Target validation
-
- Passive / no interaction with target
 - Active / interaction with target systems

e.g. Shodan.io



4-Identify potential vulnerabilities and attack scenarios

- CVE (Common Vulnerabilities and Exposures)
- Cvedetails.com



<https://github.com/jakejarvis/awesome-shodan-queries>
<https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/>



This document is TLP RED

Exploitation

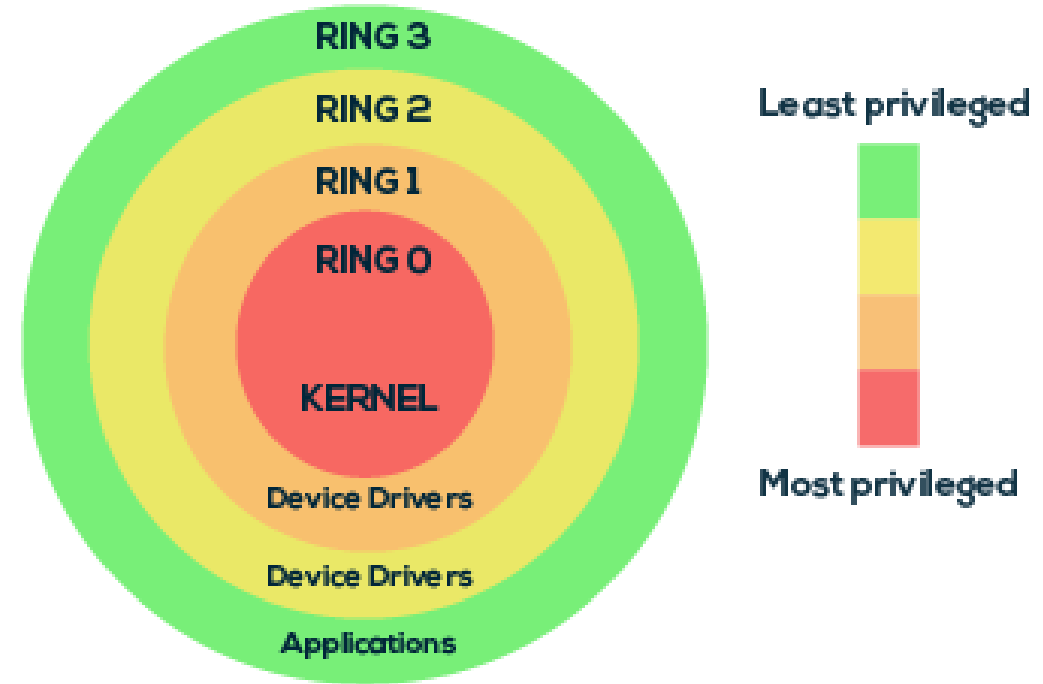
5-Exploitation

- Execute attack scenario
- Getting hold of access

Post-exploitation

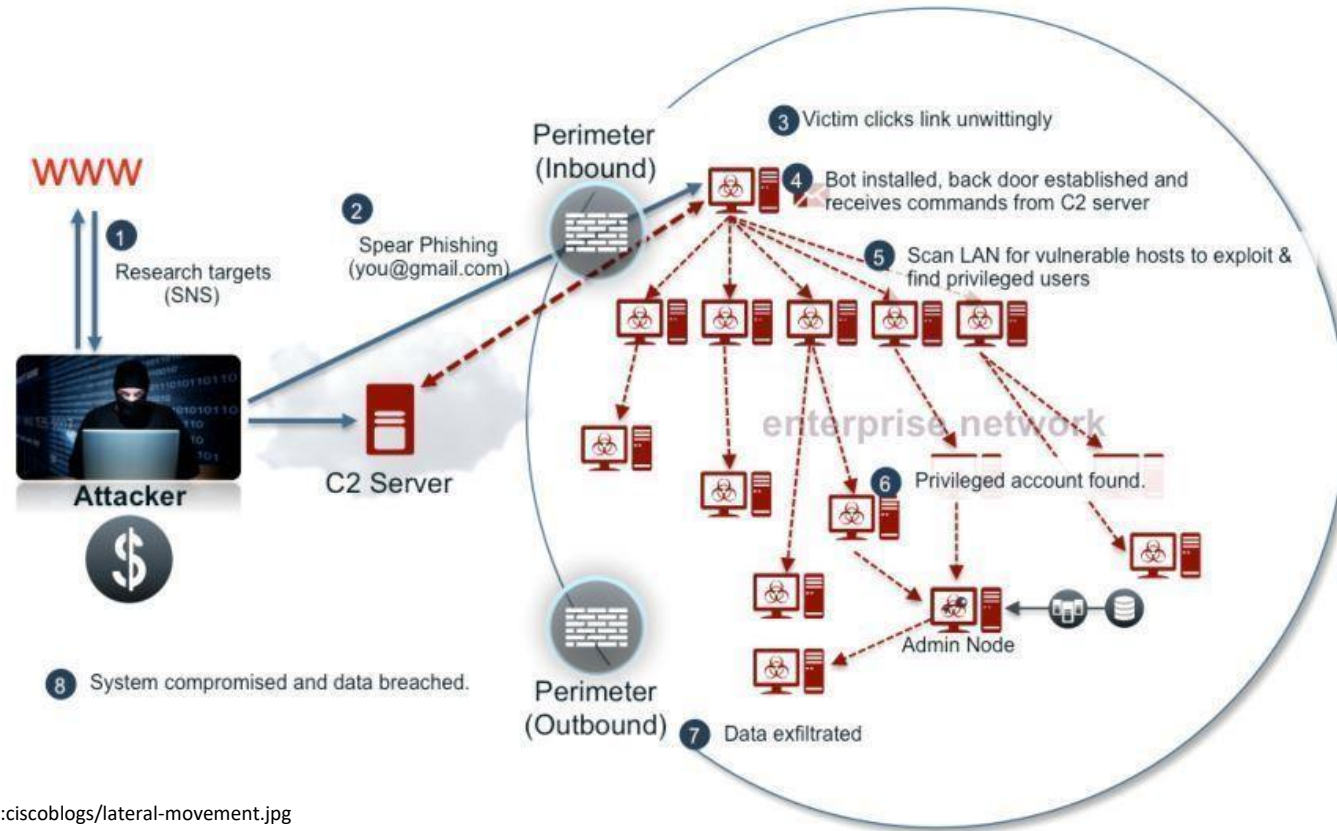
6-Post exploitation

- Maintaining access
- Expanding access
- Lateral movement
- Privilege escalation
- Stealthy persistence

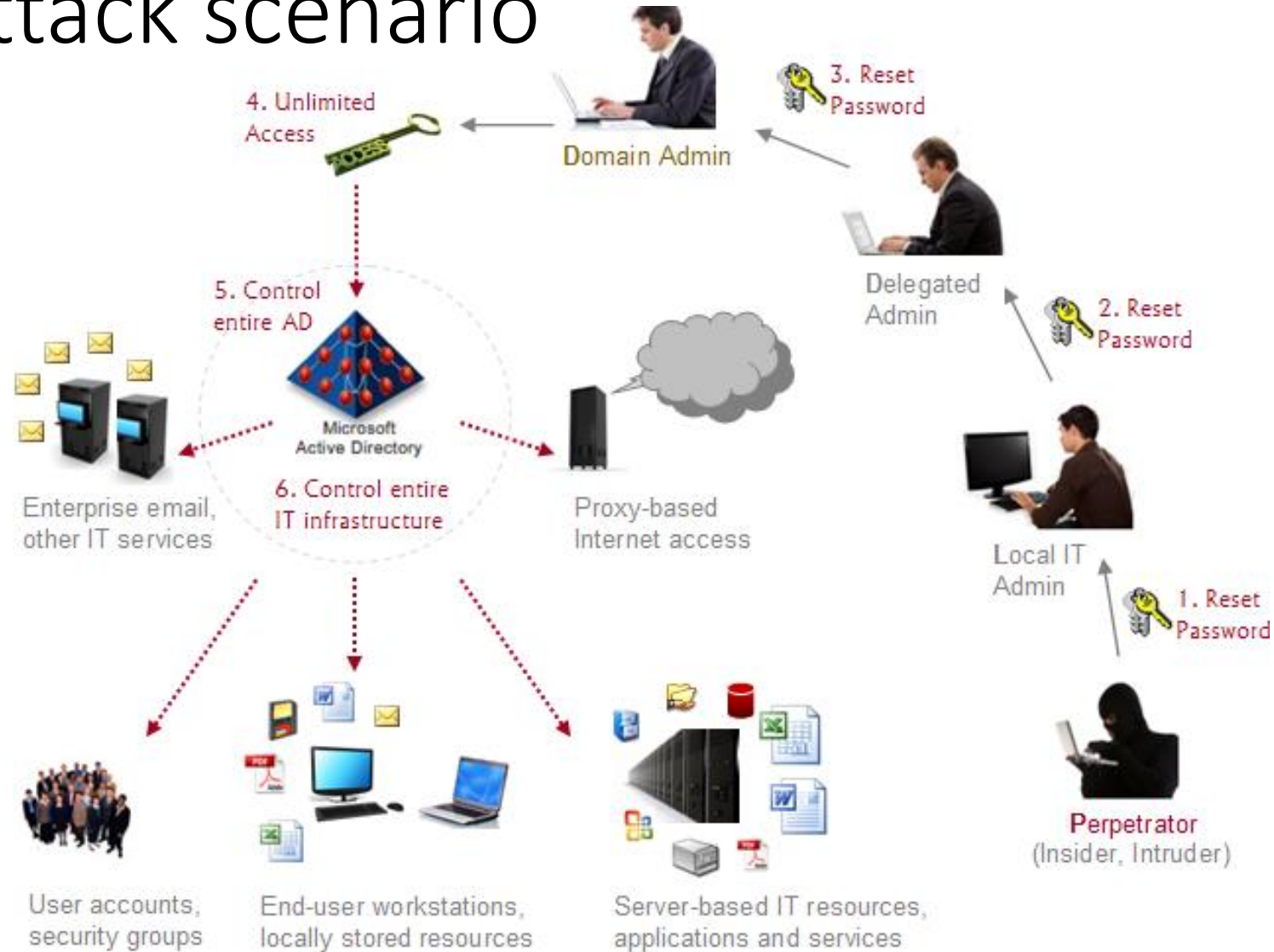


<https://blog.convisoappsec.com/en/privilege-escalation-how-it-can-affect-application-security/>

Lateral movement



Typical attack scenario



7-Covering tracks, anti-forensics

- Delete logs, history files, backup files
 - Event logs
 - Application logs
 - USB device logs
 - Timestamps
 - System restore, Wipe drive

9-Collecting evidence

- Screenshots
- Small non-sensitive data or files (approved?), directory listings

10-Reporting, remediation

- Conclusion of exercises
- Lessons learned and changes required/applied
- Accountability

11-Retesting

- Periodic security audits
- Periodic testing
- Compliance

Tools

Tools1

- Scripting with powershell or shell/Bash
- Nmap / Zmap / Zenmap: network scan
- Xray network mapping
- SimplyEmail: email harvesting

Tools2

- Wireshark: network sniffer and protocol analyzer
- Hashcat/ John the ripper / Hydra: password “recovery”
- Aircrack-ng: wireless penetration testing

Tools3

- Nessus: vulnerability management
- Burpsuite: web application penetration testing
- Metasploit: vulnerability scanning/exploitation
- Nikto: web/network scanner
- Sqlmap: sql injection penetration testing

Tools4

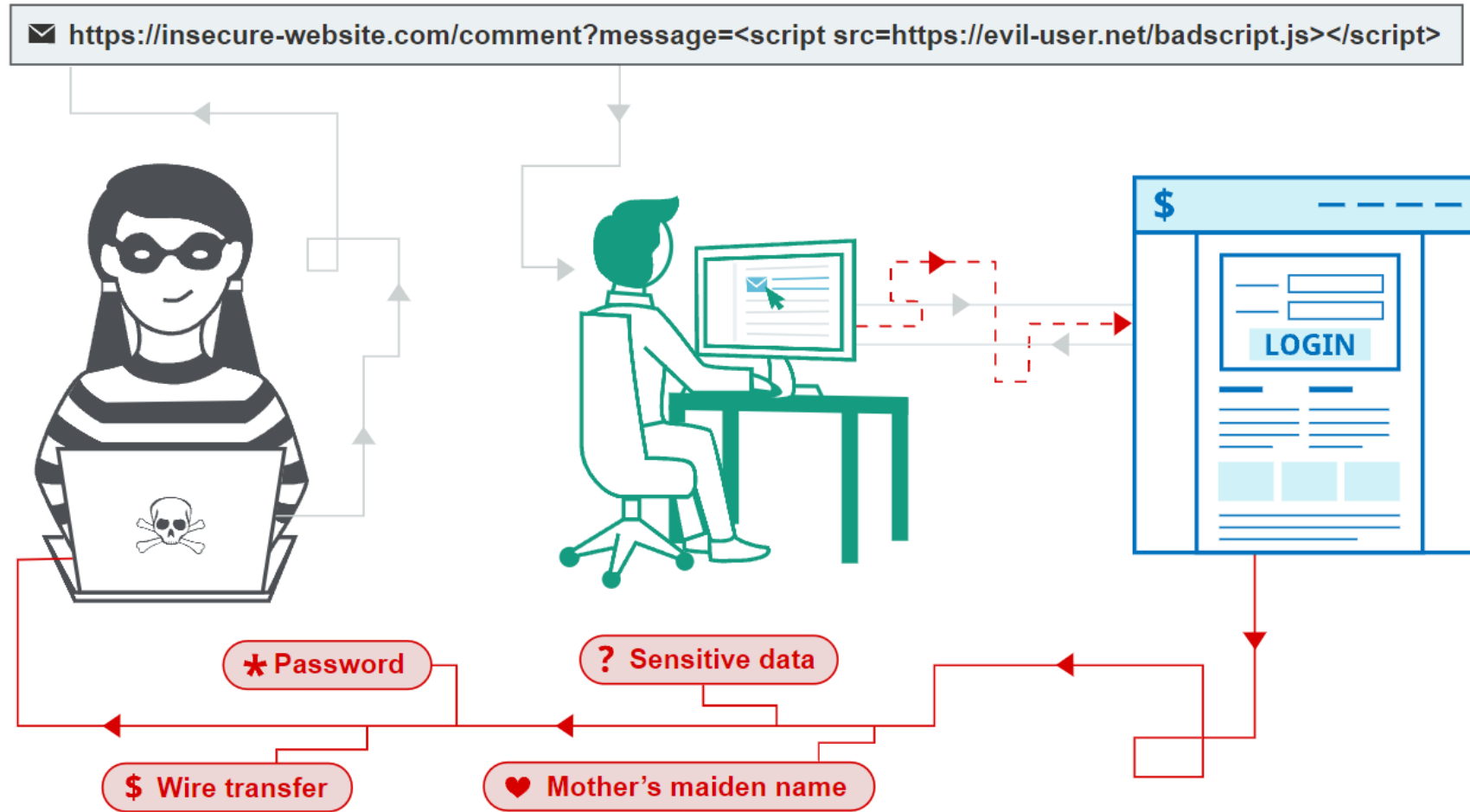
- Apktool: reversing android applications
- Resource hacker: decompile/extract windows files
- IDA/Radare/Ghidra: reverse engineering

Tools5

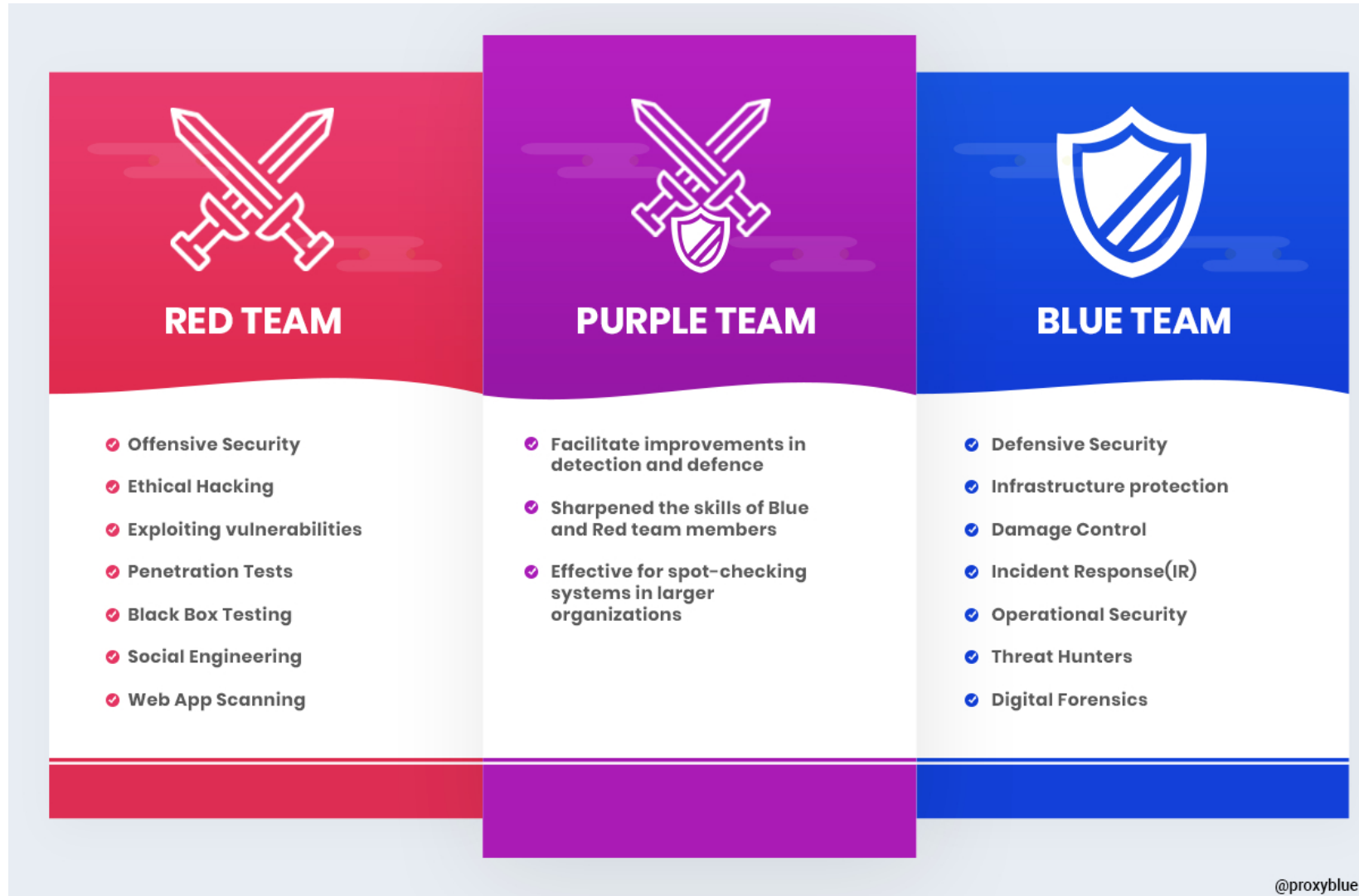
- And few thousands more
- Still not enough sometimes

Other main ethical hacking concepts

Cross site scripting XSS

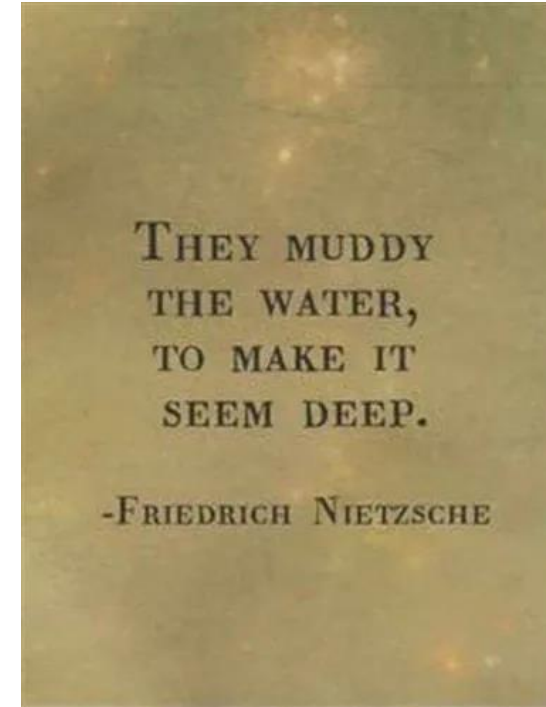


Types of security teams involved in a Pentest



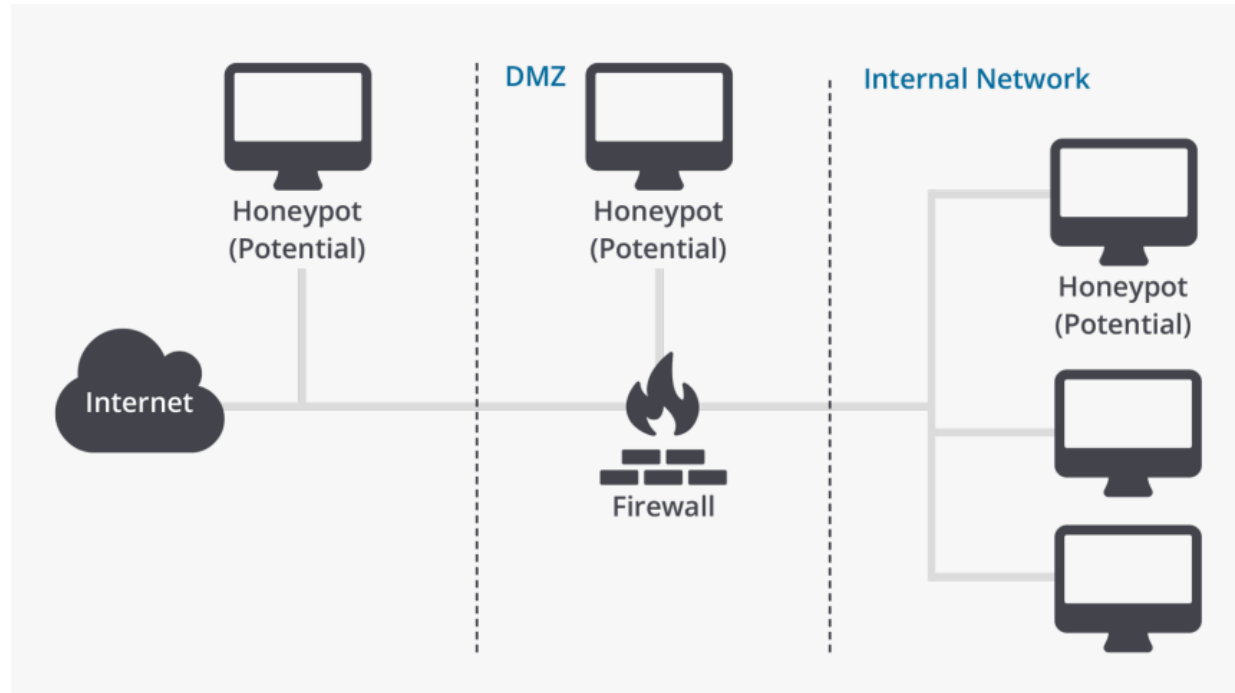
Deception in cyber offense

- DDoS
- Physical security, call centers



Deception for defense - low maturity

- Honeypots
- Virtual/physical



https://www.kindpng.com/imgv/iJTtTbo_server-honeypots-png-download-cyber-honeypot-transparent-png/

Goal of deception-defense

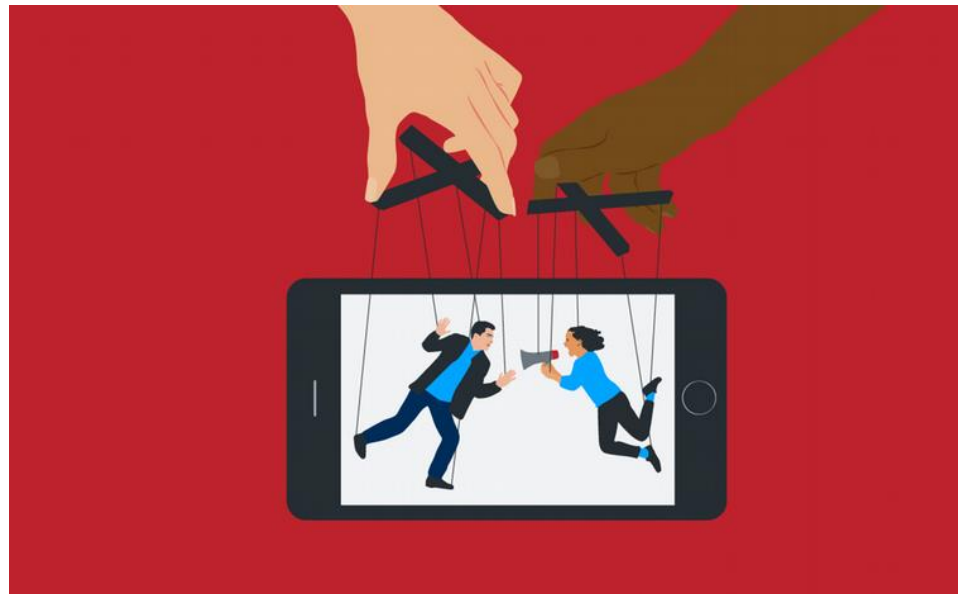


Propaganda - Information operations

- Influencing public opinion
- Fake news



Unknown maturity



<https://www.dw.com/en/fact-check-how-do-i-spot-state-sponsored-propaganda/a-60245403>

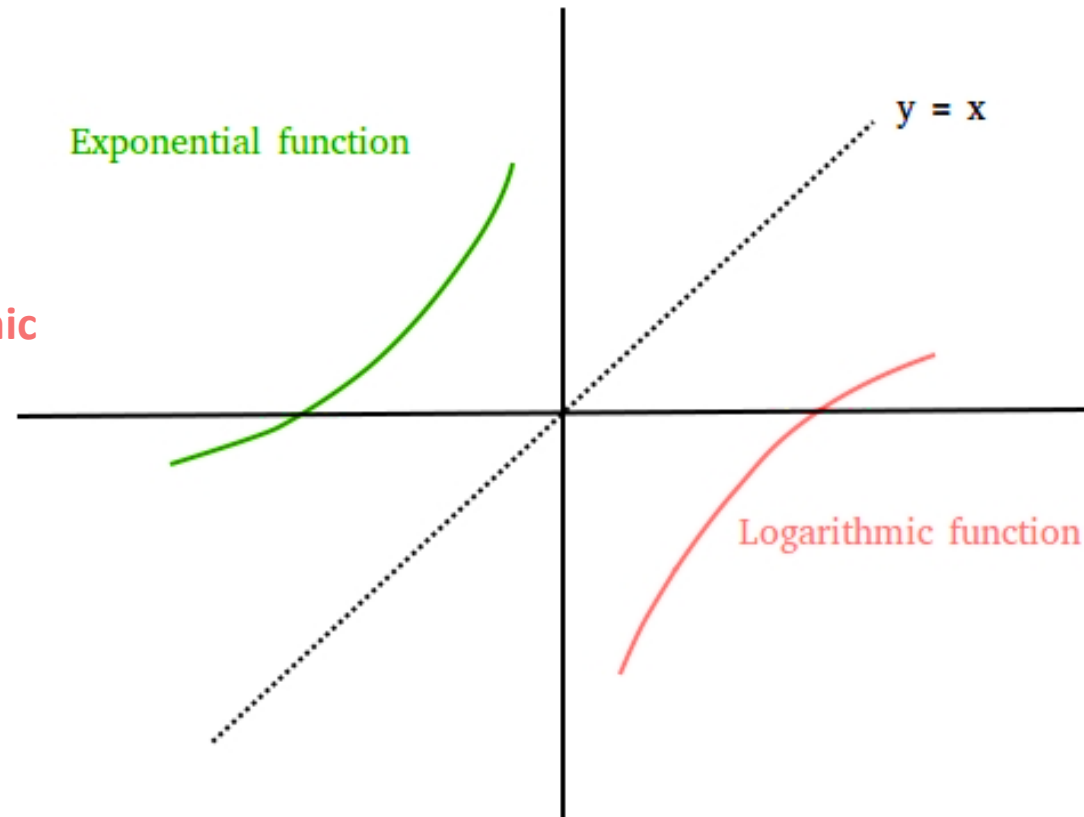
Few last thoughts on penetration testing

Some reflection – domain/certifications

Overall technology evolution => exponential

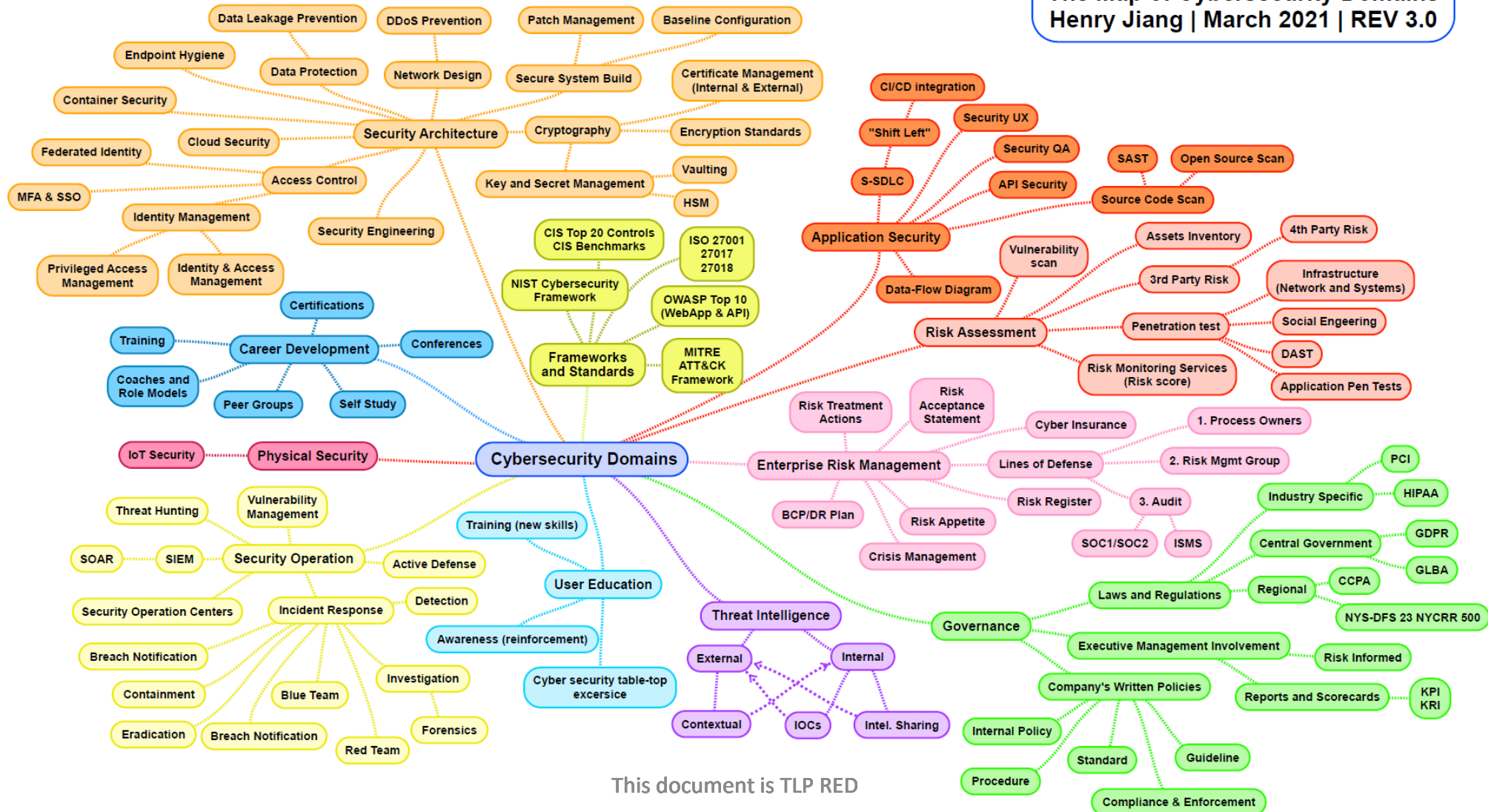
Vs

Specific technology domain evolution => logarithmic



The cybersecurity domains map

The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0



[illegible]

73

So Amin... Why are we installing stuff on Ubuntu when it's already there on Kali Linux?

Lab/homework

- Exercise on linux Ubuntu VM 20min: install nmap and run a quick port scan on your personal LAN network/gateway IP
- Exercise on linux Ubuntu VM: install Nikto and scan vulnerable VM
- Exercise on Kali linux: what exploitation attacks can you execute on vulnerable VM?
 - Information disclosure?
 - Misconfigurations?
 - Exploitation with Metasploit?
 - SQL injection?
- Research: what is Turla APT? earliest traces? List of campaigns? (10min)

Hints

- Mutillidae for SQL injection
- You need to repair database access under `/var/www/mutillidae/config.inc`



End of Module 2 Ethical hacking and penetration testing

Dr. Amin Hasbini