Spirent™
Promise. Assured.

securitylabs

STEPPING INTO THE HACKER'S SHOES - PART TWO

Aleksander Gorkowienko

Senior Managing Consultant
Spirent Communications

Agenda

Our meeting today

1. The methodology: something similar for hackers and penetration testers
2. Reviewing the key steps in exploitation:
   a) Information discovery
   b) Target scanning
   c) Vulnerability assessment
   d) Exploiting weaknesses
   e) Privilege escalation and lateral movements
   f) Retaining access
   g) Covering tracks
3. Non-technical methods: social engineering
4. Secure SDLC
5. Q&A

Introduction

Disclamer

- This course is for educational purposes only. It is intended to provide an insight into hacking for defensive purposes.
- This course is not an endorsement to undertake illegal or malicious activity in any form, unless such activity is properly authorised and you have obtained permission to do so.
- Spirent SecurityLabs takes no responsibility for any damage sustained to computer data, software or hardware through the use or misuse of tools referenced by this course.
- At the time of writing, Spirent SecurityLabs believes all information to be correct.
- Training material is (c) Spirent SecurityLabs and is for your own personal use only. The copying, recording, transcribing or photographing of any course materials, computer programs, computer code or digital information produced or supplied as part of any course is prohibited.

Stepping Into the Hacker's Shoes - Part Two

Hackers' methodology and tools

Penetration testers and malicious hackers do similar things

1. **Information discovery** (analysis and research of the target)
2. **Scanning** (attempt to identify potential entry points)
3. **Vulnerability assessment** (looking for weaknesses)
4. **Exploitation of the weakness** (make use of the identified vulnerabilities)
5. **Privilege escalation** (increasing privileges for total access)
6. **Lateral movements** (aka “pivoting attacks”: hacking the adjacent systems, servers, workstations, etc.)
7. **Retaining access** (set up a backdoor to be able to return later)
8. **Covering tracks** (removing evidence of malicious activities)

The methodology: something similar for hackers and penetration testers

- Information discovery
- Scanning
- Vulnerability assessment
- Exploitation of the weakness
- Privilege escalation
- Lateral movements (optional)

- Information discovery
- Scanning
- Vulnerability assessment
- Exploitation of the weakness
- Privilege escalation
- Lateral movements

The methodology: something similar for hackers and penetration testers

- Information discovery
- Scanning
- Vulnerability assessment
- Exploitation of the weakness
- Privilege escalation
- Lateral movements (optional)
- **Reporting the identified vulnerabilities**

- Information discovery
- Scanning
- Vulnerability assessment
- Exploitation of the weakness
- Privilege escalation
- Lateral movements
- **Retaining access**
- **Covering tracks**

Information discovery

Analysis and research of the target. OSINT.

What:

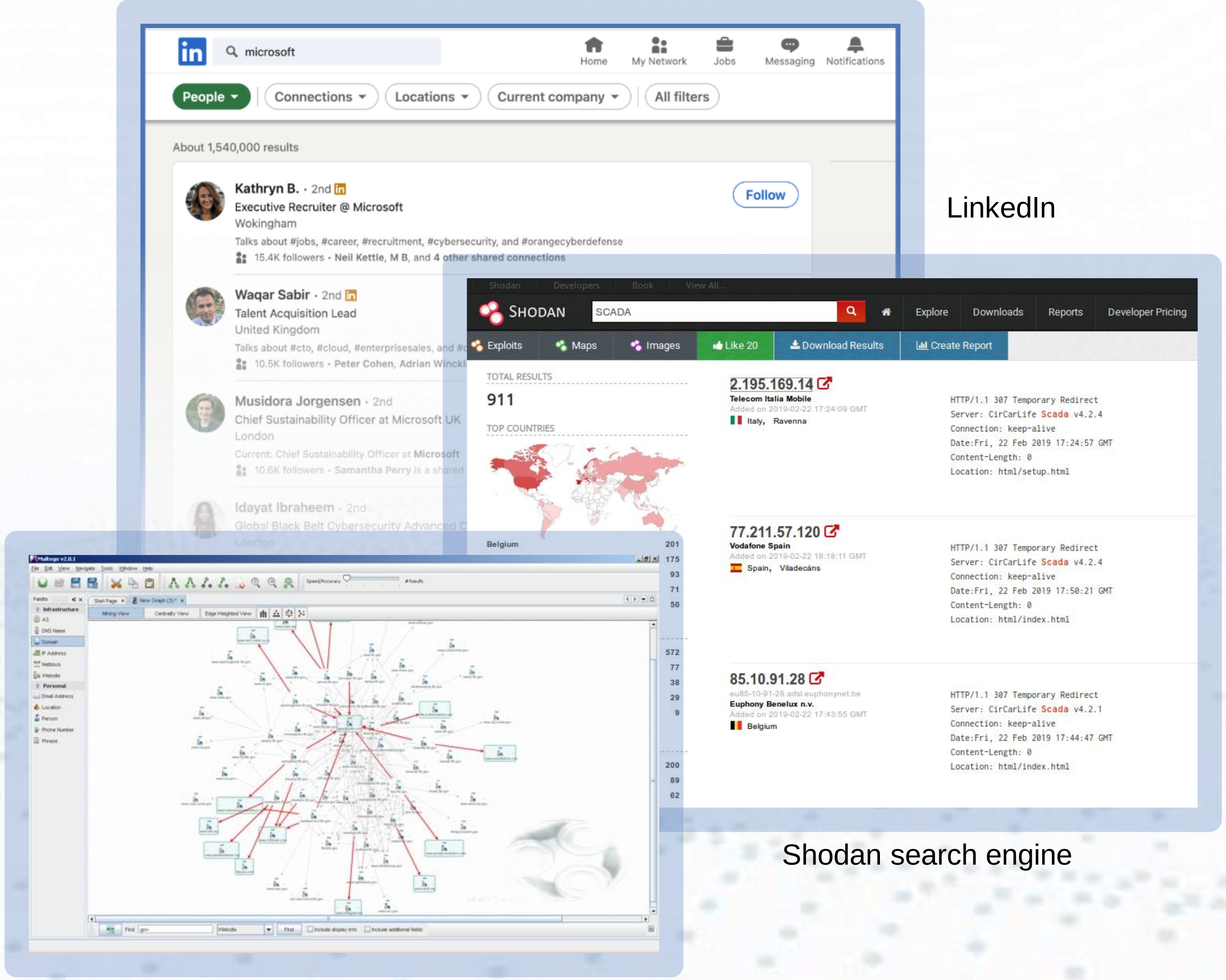
- Staff (names, positions, emails, phone nrs, etc.)
- Organisational structure (physical locations, partners, suppliers, customers, etc.)
- Business news (info about projects, acquisitions, mergers, etc.)
- Infrastructure details (ISP, domains, IP addresses, subnets, topology, equipment in use)

Where:

- Using (and abusing) public search engines
- Corporate website, job ADs, metadata
- Public forums (business or help forums)
- Public records (company register, credit ratings)

How:

- Google is your best friend ;-)
- Specialised OSINT tools
- Dumpster diving
- Eavesdropping conversations (pub, caffe)
- “Shoulder-surfing”



About 1,540,000 results

Kathryn B. · 2nd
Executive Recruiter @ Microsoft
Wokingham
Talks about #jobs, #career, #recruitment, #cybersecurity, and #orangecyberdefense
15.4K followers · Neil Kettle, M B, and 4 other shared connections

Waqar Sabir · 2nd
Talent Acquisition Lead
United Kingdom
Talks about #cto, #cloud, #enterprisesales, and #c
10.5K followers · Peter Cohen, Adrian Winckl

Musidora Jorgensen · 2nd
Chief Sustainability Officer at Microsoft UK
London
Current: Chief Sustainability Officer at Microsoft
10.6K followers · Samantha Perry is a shared

Idayat Ibraheem · 2nd
Global Black Belt Cybersecurity Advanced C
London

TOTAL RESULTS
911

TOP COUNTRIES

Belgium 201

175
93
71
50
572
77
38
29
9
200
89
62

2.195.169.14
Telecom Italia Mobile
Added on 2019-02-22 17:24:09 GMT
Italy, Ravenna

```
HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.4
Connection: keep-alive
Date:Fri, 22 Feb 2019 17:24:57 GMT
Content-Length: 0
Location: html/setup.html
```

77.211.57.120
Vodafone Spain
Added on 2019-02-22 18:18:11 GMT
Spain, Viladecáns

```
HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.4
Connection: keep-alive
Date:Fri, 22 Feb 2019 17:50:21 GMT
Content-Length: 0
Location: html/index.html
```

85.10.91.28
eu85-10-91-28.adsl.euphonynet.be
Euphony Benelux n.v.
Added on 2019-02-22 17:43:55 GMT
Belgium

```
HTTP/1.1 307 Temporary Redirect
Server: CirCarLife Scada v4.2.1
Connection: keep-alive
Date:Fri, 22 Feb 2019 17:44:47 GMT
Content-Length: 0
Location: html/index.html
```

LinkedIn

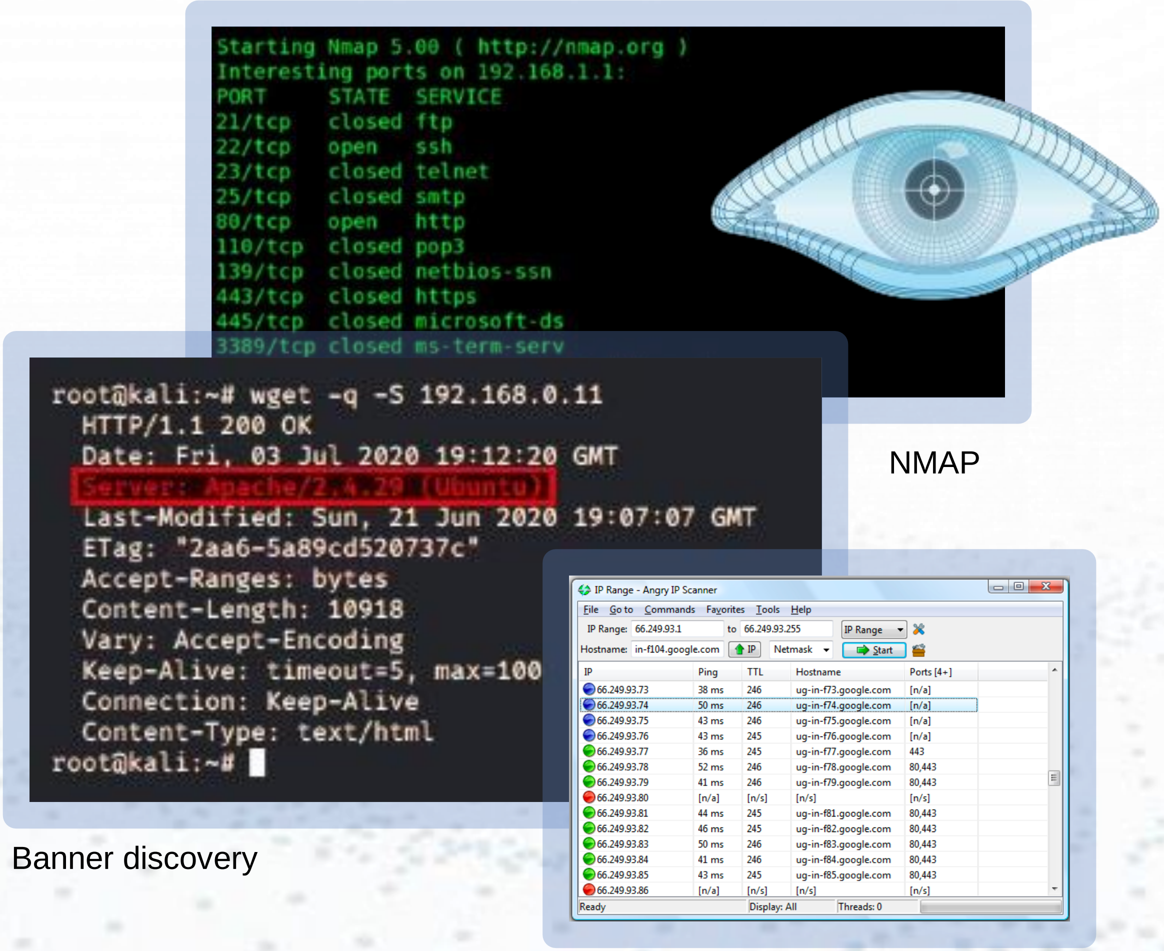
Shodan search engine

Maltego

Target scanning

An attempt to identify potential entry points

- Internet-facing **hosts** have various **ports** open
- Servers can run multiple **services**. Each service has its own port (like a radio channel).
- Software version on the server can often be discovered by “banner grabbing” technique
- Hosts, ports and services can be discovered by using special tools: scanners
- A well-known tool: NMAP (Swiss army knife in the world of scanners), but also *Zenmap, Angry IP Scanner, Masscan, Advanced IP Scanner, NetCrunch tools, Cain & Abel*, etc.



```
Starting Nmap 5.00 ( http://nmap.org )
Interesting ports on 192.168.1.1:
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
```

NMAP

```
root@kali:~# wget -q -S 192.168.0.11
  HTTP/1.1 200 OK
  Date: Fri, 03 Jul 2020 19:12:20 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Last-Modified: Sun, 21 Jun 2020 19:07:07 GMT
  ETag: "2aa6-5a89cd520737c"
  Accept-Ranges: bytes
  Content-Length: 10918
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html
root@kali:~#
```

Banner discovery

IP Range - Angry IP Scanner
File Go to Commands Favorites Tools Help
IP Start

IP Range: 66.249.93.1 to 66.249.93.255 IP Range
Hostname: in-f104.google.com Netmask

IP	Ping	TTL	Hostname	Ports [4+]
66.249.93.73	38 ms	246	ug-in-f73.google.com	[n/a]
66.249.93.74	50 ms	246	ug-in-f74.google.com	[n/a]
66.249.93.75	43 ms	246	ug-in-f75.google.com	[n/a]
66.249.93.76	43 ms	245	ug-in-f76.google.com	[n/a]
66.249.93.77	36 ms	245	ug-in-f77.google.com	443
66.249.93.78	52 ms	246	ug-in-f78.google.com	80,443
66.249.93.79	41 ms	246	ug-in-f79.google.com	80,443
66.249.93.80	[n/a]	[n/s]	[n/s]	[n/s]
66.249.93.81	44 ms	245	ug-in-f81.google.com	80,443
66.249.93.82	46 ms	245	ug-in-f82.google.com	80,443
66.249.93.83	50 ms	246	ug-in-f83.google.com	80,443
66.249.93.84	41 ms	246	ug-in-f84.google.com	80,443
66.249.93.85	43 ms	245	ug-in-f85.google.com	80,443
66.249.93.86	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display: All Threads: 0

Angry IP Scanner

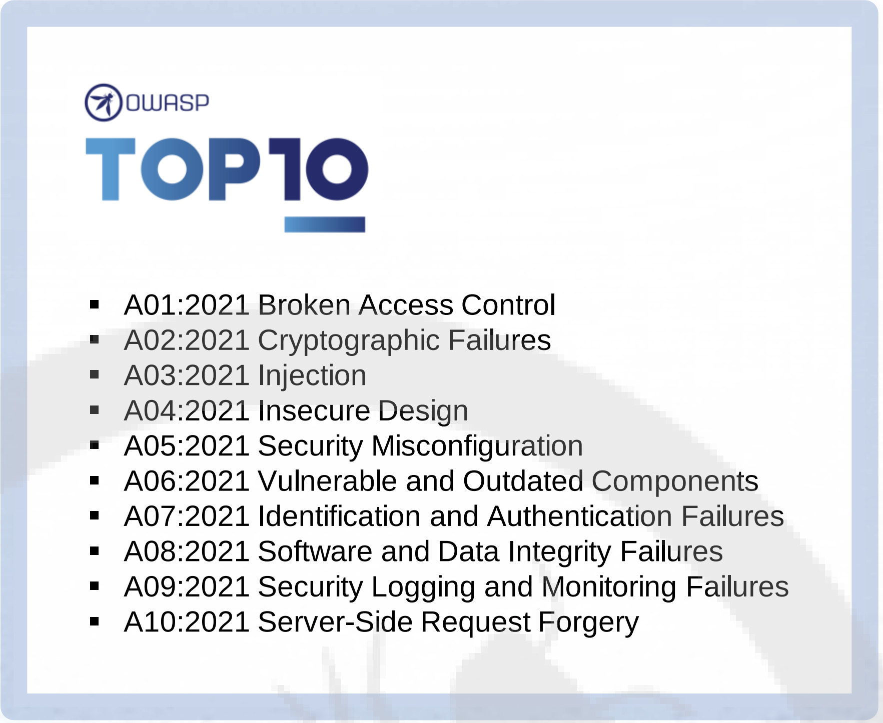
Vulnerability assessment

Looking for weaknesses

Vulnerability: weakness that affects the security posture of the IT asset (web application, mobile app, server, IoT device, industrial microcontroller, cloud service, etc.)

- **Client-side vulnerabilities** ("thin" and "thick" client applications)
- **Server-side vulnerabilities**

Vulnerability detection/scanning on the server side by specialised tools (vulnerability scanners): like *Nessus, Acunetix, Burp, Nexpose, Open VAS, Core Impact,* etc.



OWASP

TOP 10

- A01:2021 Broken Access Control
- A02:2021 Cryptographic Failures
- A03:2021 Injection
- A04:2021 Insecure Design
- A05:2021 Security Misconfiguration
- A06:2021 Vulnerable and Outdated Components
- A07:2021 Identification and Authentication Failures
- A08:2021 Software and Data Integrity Failures
- A09:2021 Security Logging and Monitoring Failures
- A10:2021 Server-Side Request Forgery

Typical vulnerabilities:

- Loss of CIA (confidentiality, integrity and availability)
- Denial of service (DoS and DDoS)
- Privilege escalation
- SQL injection
- Cross-site scripting
- Local File inclusion (LFI)
- …

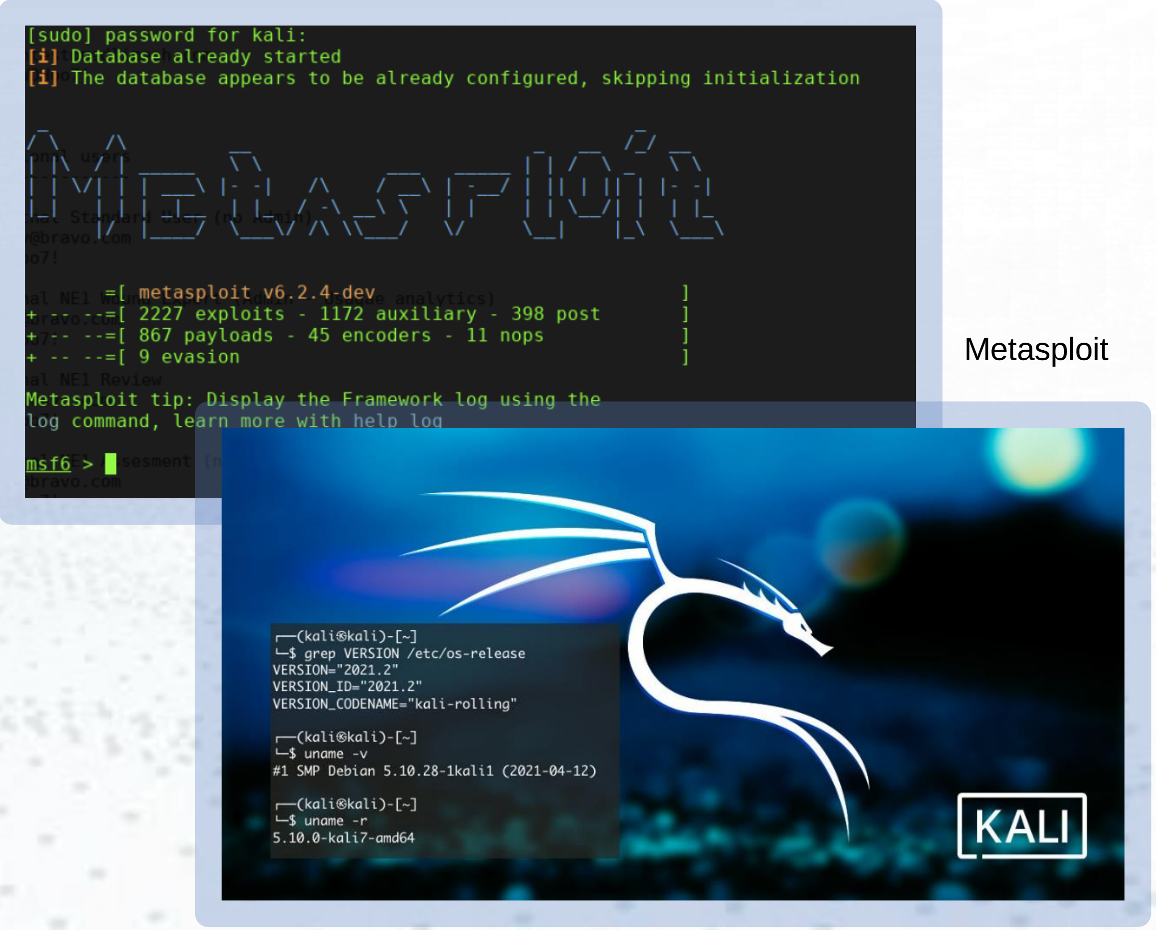
Exploitation of the weakness

Make use of the identified vulnerabilities for fun and profit

- **Exploit:** use the specific security weakness
- **Payload:** doing something useful, e.g., running remote shell
- Massive collection of exploits and payloads in **Metasploit**

(Btw: there is no guarantee that the exploit will always work – all systems are different!)

- **Zero-day:** vulnerability found and can be exploited, but there is no patch available. The attacker has a short “window of opportunity”.
- **Kali Linux:** free Linux distro with hundreds of exploitation tools
- Internet is full of free exploits and examples of malicious code



```
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization


       =[ metasploit v6.2.4-dev                           ]
+ -- --=[ 2227 exploits - 1172 auxiliary - 398 post       ]
+ -- --=[ 867 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log

msf6 >
```

Metasploit

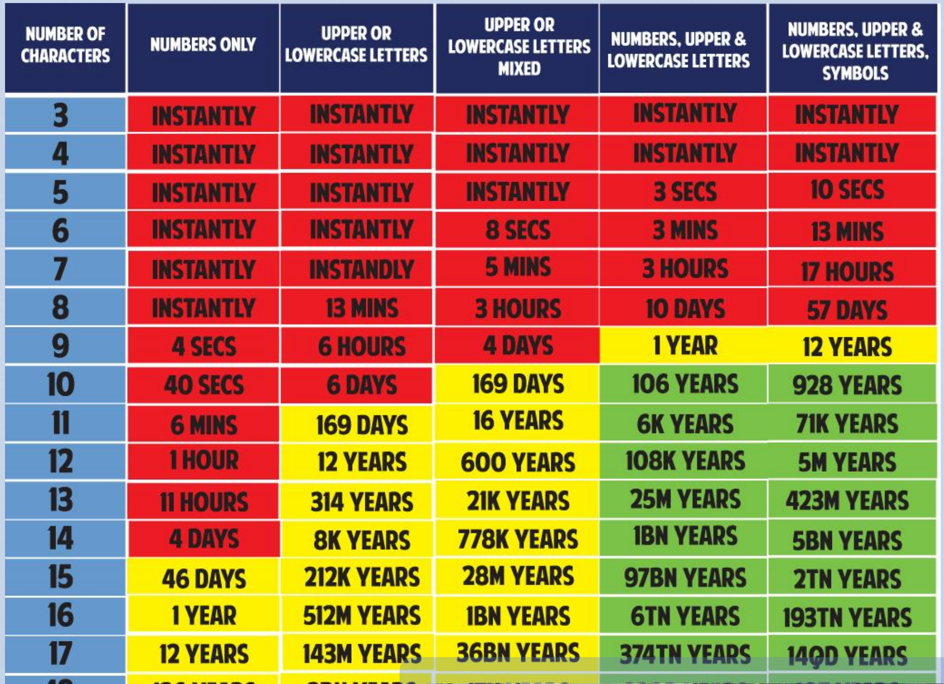
```
┌──(kali㉿kali)-[~]
└─$ grep VERSION /etc/os-release
VERSION="2021.2"
VERSION_ID="2021.2"
VERSION_CODENAME="kali-rolling"

┌──(kali㉿kali)-[~]
└─$ uname -v
#1 SMP Debian 5.10.28-1kali1 (2021-04-12)

┌──(kali㉿kali)-[~]
└─$ uname -r
5.10.0-kali7-amd64
```

Kali Linux

Privilege escalation

Increasing privileges for total access

- Leveraging privileges in the system that was exploited
- Privilege escalation is not always required and is dependent on the attacker's objectives
- Privilege escalation sometimes require *password cracking*



NUMBER OF CHARACTERS	NUMBERS ONLY	UPPER OR LOWERCASE LETTERS	UPPER OR LOWERCASE LETTERS MIXED	NUMBERS, UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS, SYMBOLS
3	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
4	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
5	INSTANTLY	INSTANTLY	INSTANTLY	3 SECS	10 SECS
6	INSTANTLY	INSTANTLY	8 SECS	3 MINS	13 MINS
7	INSTANTLY	INSTANDLY	5 MINS	3 HOURS	17 HOURS
8	INSTANTLY	13 MINS	3 HOURS	10 DAYS	57 DAYS
9	4 SECS	6 HOURS	4 DAYS	1 YEAR	12 YEARS
10	40 SECS	6 DAYS	169 DAYS	106 YEARS	928 YEARS
11	6 MINS	169 DAYS	16 YEARS	6K YEARS	71K YEARS
12	1 HOUR	12 YEARS	600 YEARS	108K YEARS	5M YEARS
13	11 HOURS	314 YEARS	21K YEARS	25M YEARS	423M YEARS
14	4 DAYS	8K YEARS	778K YEARS	1BN YEARS	5BN YEARS
15	46 DAYS	212K YEARS	28M YEARS	97BN YEARS	2TN YEARS
16	1 YEAR	512M YEARS	1BN YEARS	6TN YEARS	193TN YEARS
17	12 YEARS	143M YEARS	36BN YEARS	374TN YEARS	14QD YEARS
18	126 YEARS	3BN YEARS	[illegible]	[illegible]	[illegible]

Password cracking:

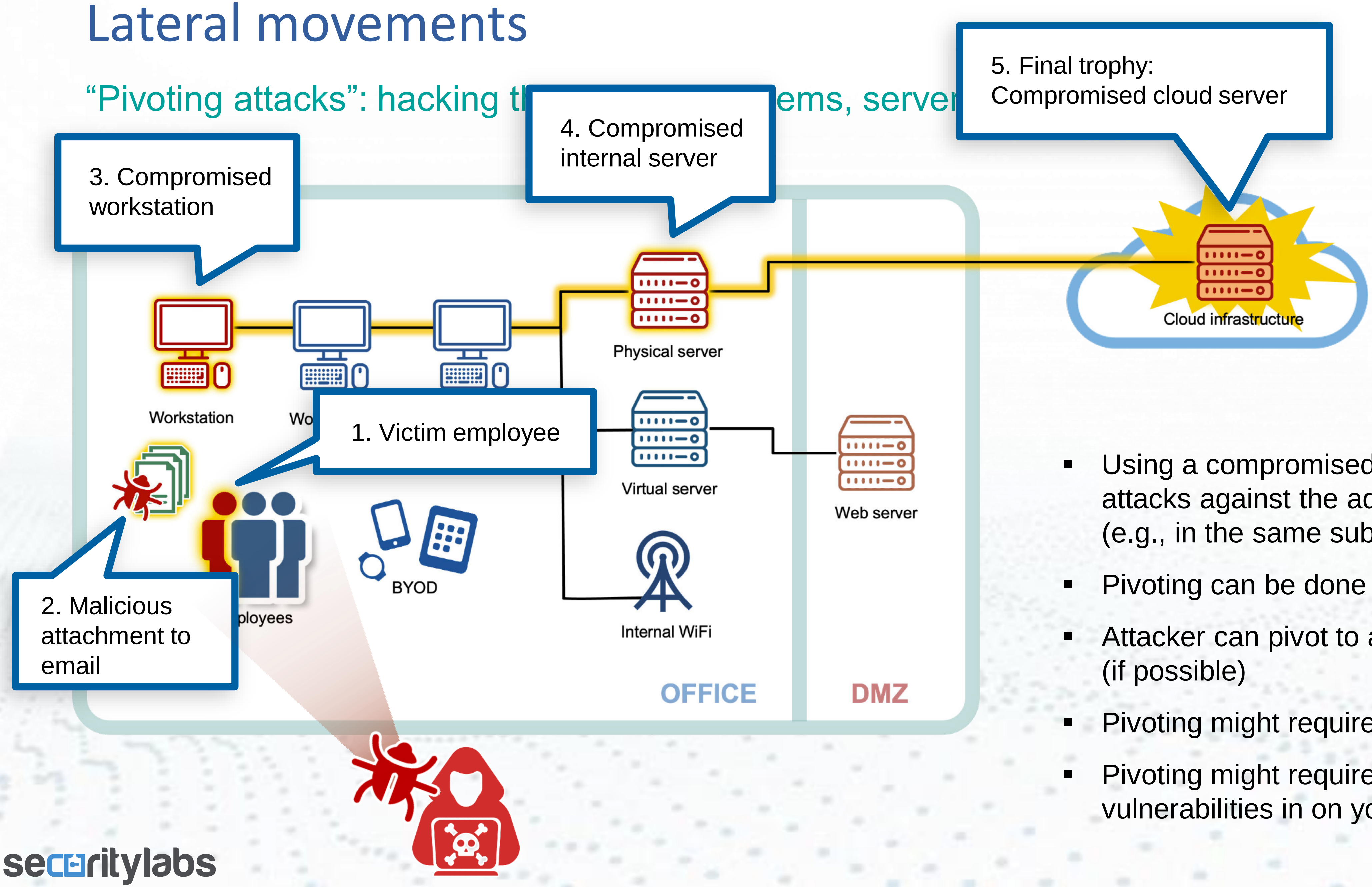
- Stealing passwords by **keyloggers**
- **Bruteforcing** passwords
- Cracking password hashes: online and offline
- Use pre-compiled databases of hashes ("**Rainbow tables**")
- Use password cracking GPU-based rig. Tools of the trade: *Hashcat, John the Ripper*.
- Password hashes in the wild (6.5M LinkedIn, Yahoo, etc.)

GPU password cracking rig

Hardware keylogger

Lateral movements

“Pivoting attacks”: hacking th ems, server



1. Victim employee

2. Malicious attachment to email

3. Compromised workstation

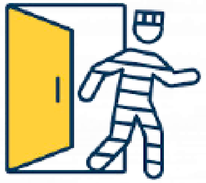
4. Compromised internal server

5. Final trophy: Compromised cloud server

- Using a compromised machine for new attacks against the adjacent infrastructure (e.g., in the same subnet)
- Pivoting can be done in multiple steps
- Attacker can pivot to another subnets (if possible)
- Pivoting might require escalated privileges
- Pivoting might require exploiting multiple vulnerabilities in on your way

Retaining access

Set up a backdoor to be able to return later



Backdoor: a hidden stealthy entry point to the exploited system, aimed to retain access. Typically achieved by using special software or changing the system configuration.

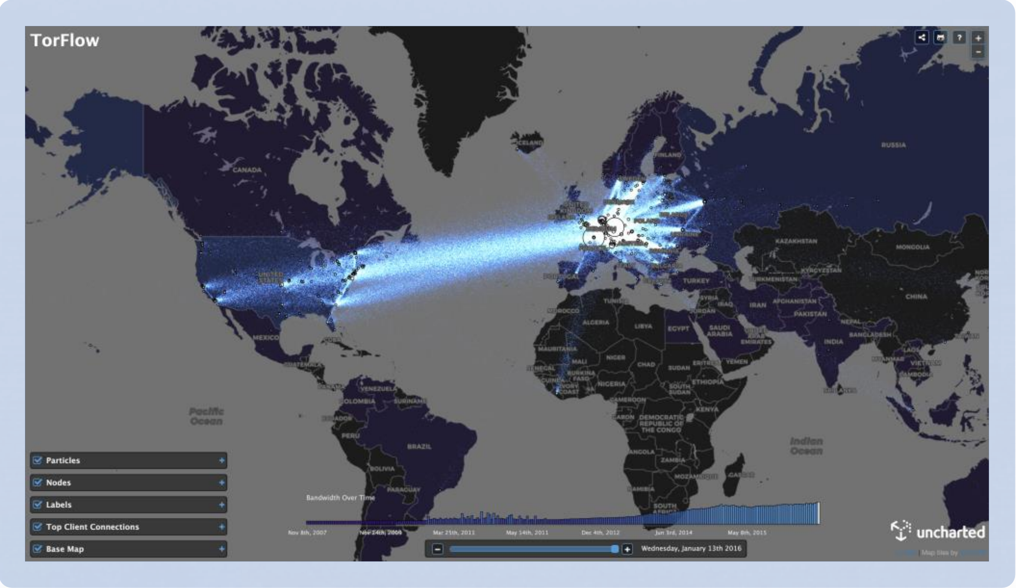
- **RAT:** Remote Administration Tool
- **RAT installation:** manual, by malware, trojan horses, etc.

- **Trojan horse:** a malware that was packaged to look benign
- **Trojan horse installation:**
  - Downloaded as “warez” (free Windows software in P2P networks). *Ergo: Do NOT download warez!*
  - Malicious email attachments
  - Malicious documents (MS Office, PDF, etc.)
  - Using social engineering techniques

Covering tracks

Removing evidence of malicious activities

- It is in the best interest of the attacker **staying unnoticed as long as possible**
- There could be **weeks or months** between getting remote access and exploiting the system
- Modification of the system logs, removing files
- Connecting to the victim through intermediate points (another vulnerable machines, Onion Router TOR network, etc.)
- Installing **rootkits**



https://torflow.uncharted.software

Rootkit: a collection of many post-exploitation tools in one binary

- Well-written rootkit costs $$$ (literally: fortune)
- Main objective: staying totally stealth
- Typically include backdoor, advanced mechanisms preventing detection by AV, remote access functionality and much more.

Non-technical methods: social engineering

Hacking humans

Gaining and misusing human trust by using psychological manipulative techniques (often in multiple small steps).

- Impersonation
- Staged fake friendliness
- Social engineering combined with technical hacking
- Remote (email, phone)
- Local (shared office space, company's smoking zone, reception)

Read about Kevin Mitnick – it's fun! (and very educational)

From the 1970s up until his last arrest in 1995 Kevin Mitnick eluded and bypassed corporate security, penetrating some of the most well-guarded systems, including (amongst countless others) **Sun Microsystems, Motorola, Netcom**, and **Nokia**. He has even had to go on record and deny hacking into the **Department of Defense's North American Aerospace Defense Command (NORAD)** and wiretapping the **Federal Bureau of Investigation**.

Types of social engineering:

- Phishing (luring to disclose sensitive info)
- Pretexting (fabricating a fake scenario)
- Baiting (promise of an item or good)
- Quid Pro Quo (give something in exchange)
- Tailgating (following to restricted area)

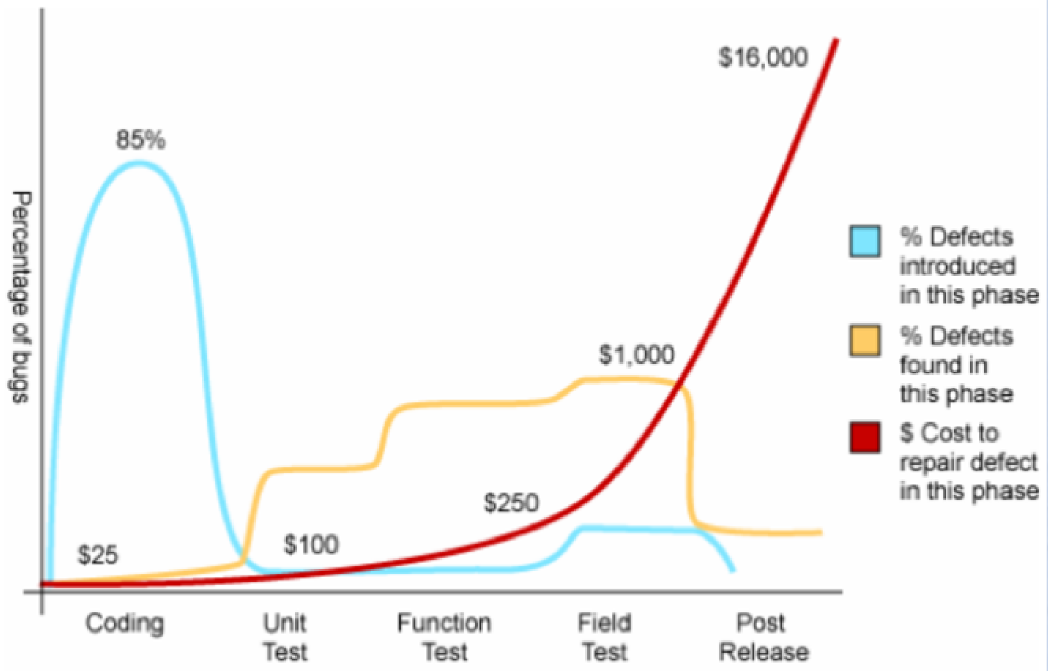
Secure SDLC

A secure SDLC involves **integrating security testing and other security-related activities into an existing development process**.

Examples:

- Creating general security policies for the product
- Developing security requirements alongside functional requirements
- Performing an architecture risk analysis during the design phase
- Following secure coding standards and best practices

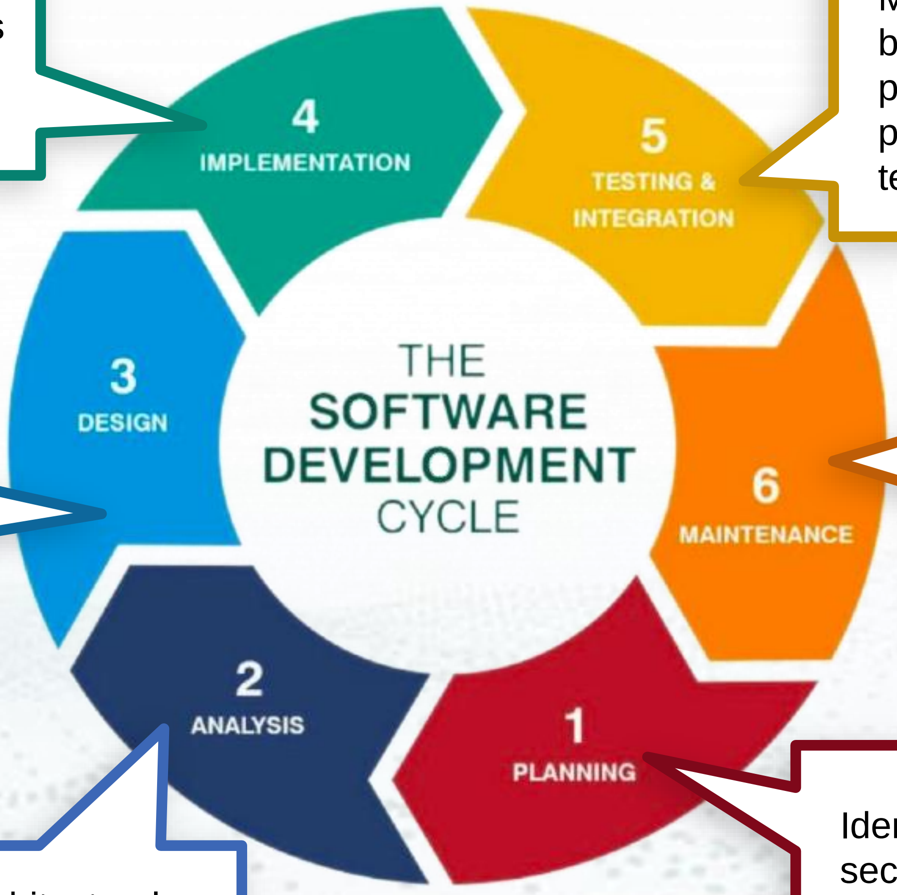
The Cost of Software Bugs



Source: Applied Software Measurement, Capers Jones, 1996

Eoin Keary & Jim Manico

Secure SDLC



Identify and/or define relevant security policies and pick those applicable to the software.

Conduct architectural risk analysis that identifies security flaws in the very early stage.

Develop guidelines to address risks evaluated during previous phases. A comprehensive Product Security Risk Assessment ("Static Assessment").

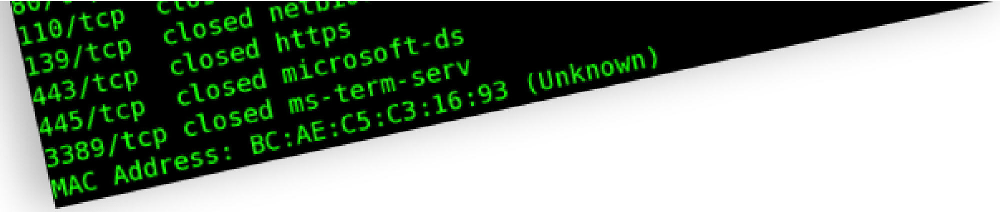
Developers follow the robust secure coding practices. Security guidelines are set and awareness campaigns are conducted regularly.

Monitoring of the product is carried out both in its production and post-production environment. Under production, the developed software is tested/re-tested again.

Continuous attempts to identify new, recently discovered and published, vulnerabilities.

LC requires its own set of security too
eams' IDEs, code repositories, build servers, and
o gauge any scope of risk and to address them.

Takeaways



```
80/
110/tcp  clo
139/tcp  closed netbi
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)
```

- Security is a **continuous process**, where an organization is learning and improving their processes and the security posture all the time.
- A system can be called “secure” only in a specific moment in time. It cannot be “always secure”, therefore **regular testing is imperative**.
- Security is a **system property**, not a feature.
- Security is a **continual process**, not a product.
- The cybersecurity landscape is changing rapidly. Learning something new about cybersecurity every day is very important **for cyber-safety of you, your family and your business.**

People

Humans remain one of the weakest links in security chain. Ensure you have a strong security awareness training program.

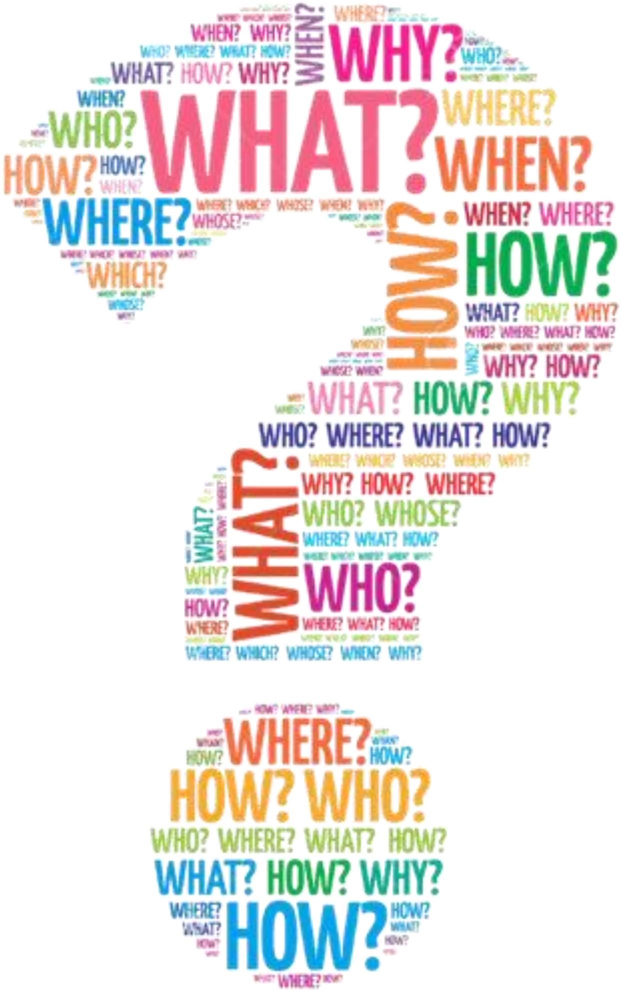
Processes

It is important to ensure that best practice processes and associated management frameworks are in place. Regular audits and reviews are important.

Technology

The continuously increasing sophistication and rate of attacks means that constant upkeep and tracking of technology changes is essential.

Questions


WHEN? WHY?
WHEN?
WHY?
WHERE?
WHO? WHERE? WHAT? HOW?
WHO?
WHAT? HOW? WHY?
WHEN?
WHAT?
WHERE?
WHO?
HOW? HOW?
WHEN?
WHEN?
WHERE?
WHEN? WHERE?
WHOSE?
HOW?
HOW?
WHICH?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHY? HOW?
WHAT? HOW? WHY?
WHO? WHERE? WHAT? HOW?
WHAT?
WHY? HOW? WHERE?
WHO? WHOSE?
WHERE? WHAT? HOW?
WHAT?
WHY?
WHO?
HOW?
WHERE? WHAT? HOW?
WHERE?
WHERE? WHICH? WHOSE? WHEN? WHY?
WHERE?
HOW?
HOW? WHO?
WHO? WHERE? WHAT? HOW?
WHAT? HOW? WHY?
WHERE?
HOW?
HOW?
WHAT?
WHERE?

Thank you!

https://www.spirent.com/Products/SecurityLabs

securityLabs@spirent.com

securitylabs

Aleksander Gorkowienko
e: aleksander.gorkowienko@spirent.com
m: +44 (0) 7974431025