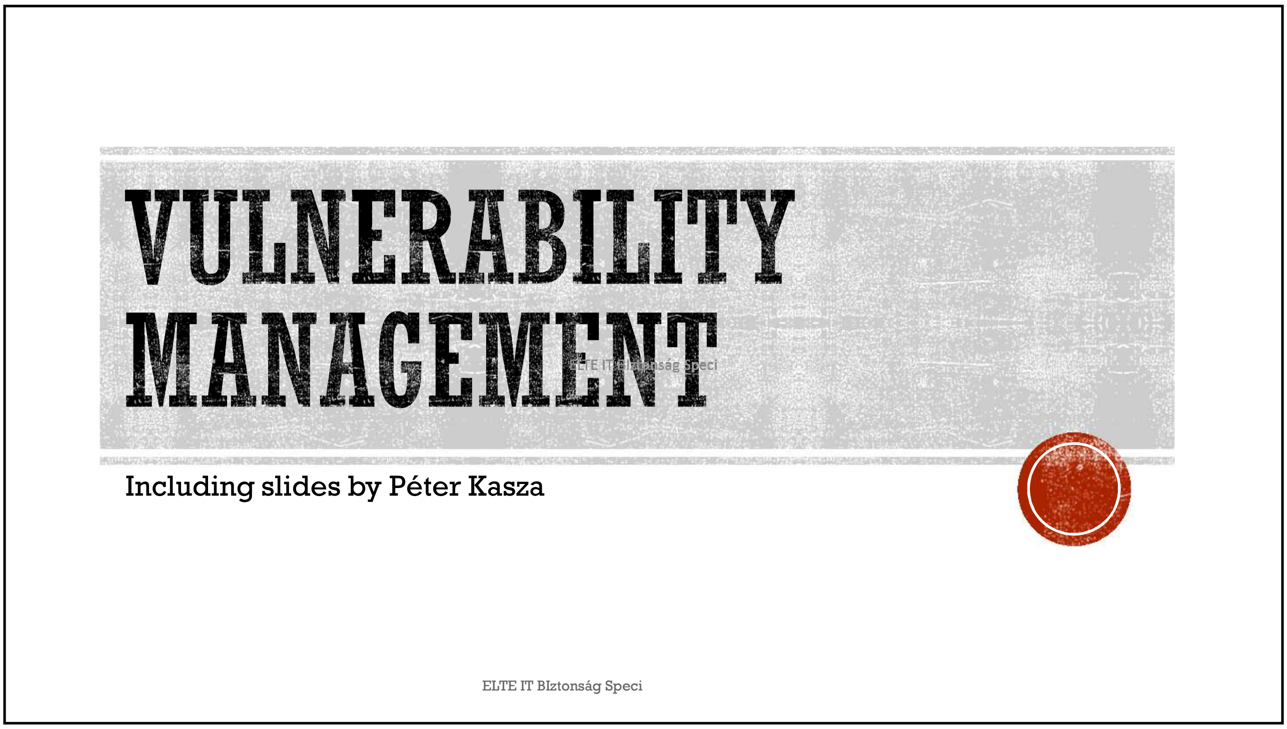
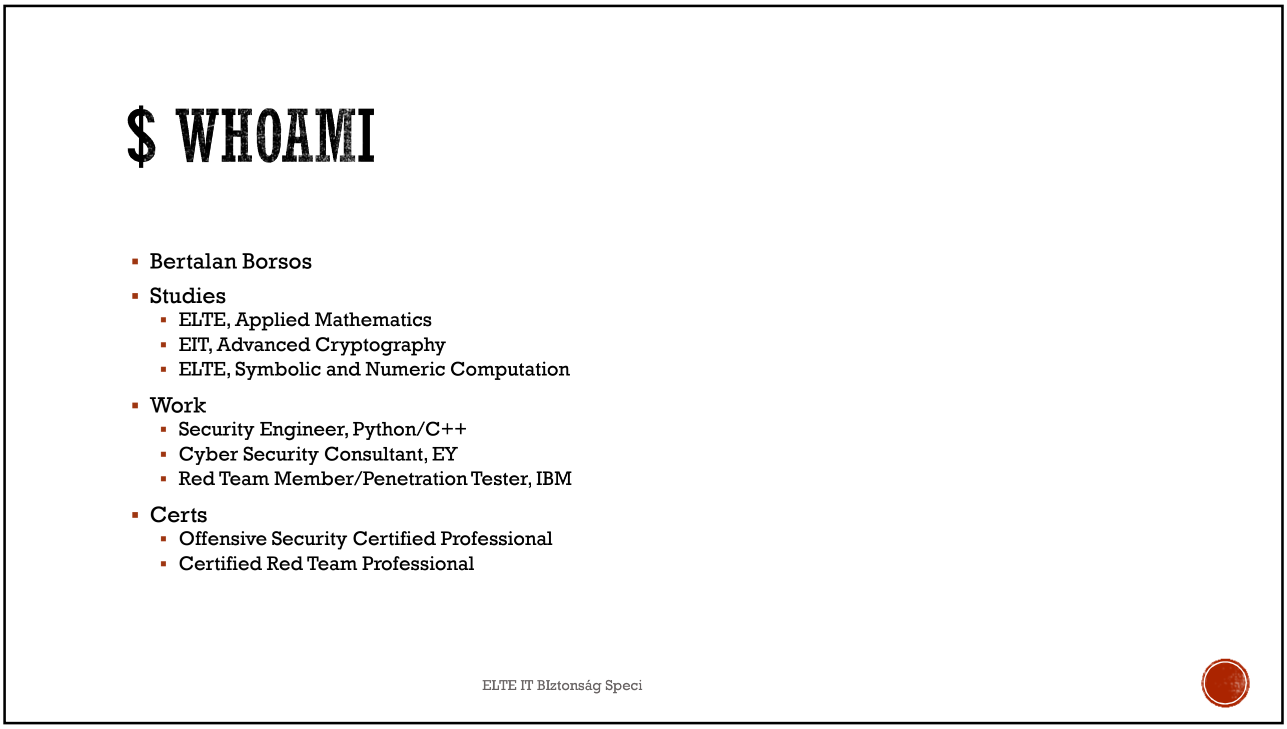


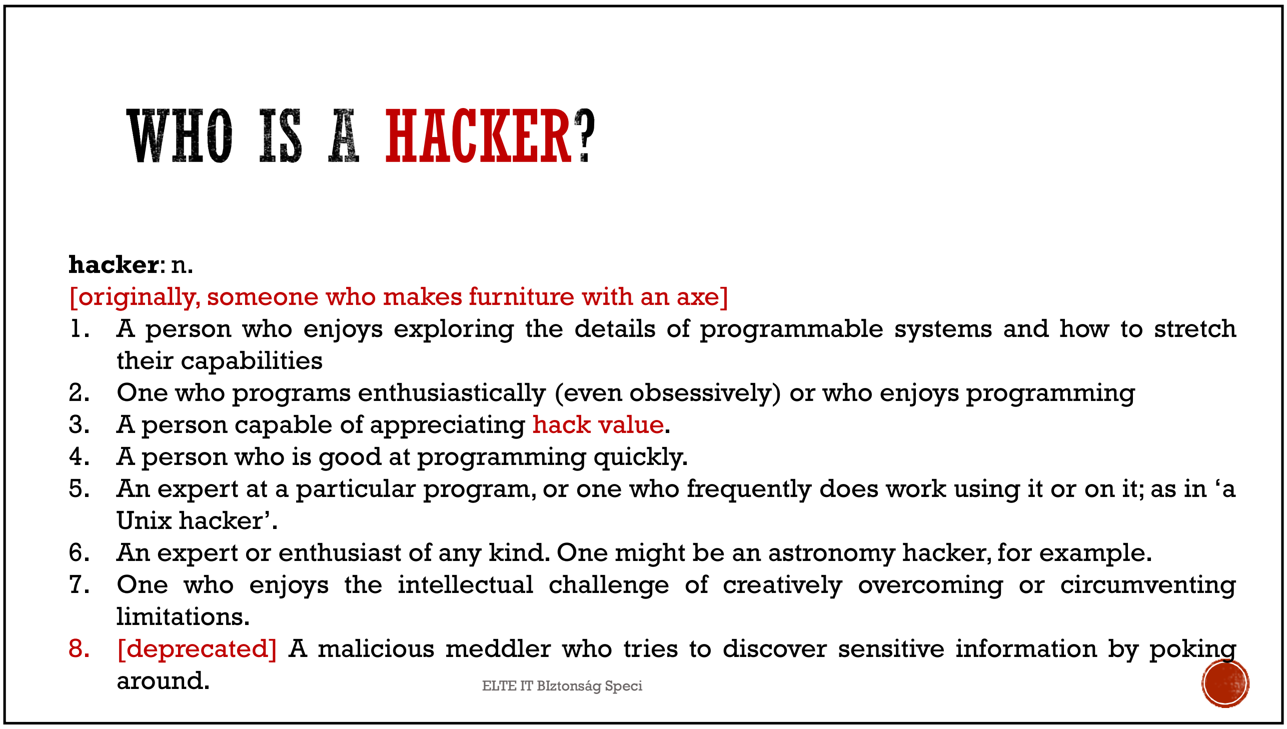
VULNERABILITY MANAGEMENT

Including slides by Péter Kasza



$ WHOAMI

- Bertalan Borsos
- Studies
  - ELTE, Applied Mathematics
  - EIT, Advanced Cryptography
  - ELTE, Symbolic and Numeric Computation
- Work
  - Security Engineer, Python/C++
  - Cyber Security Consultant, EY
  - Red Team Member/Penetration Tester, IBM
- Certs
  - Offensive Security Certified Professional
  - Certified Red Team Professional

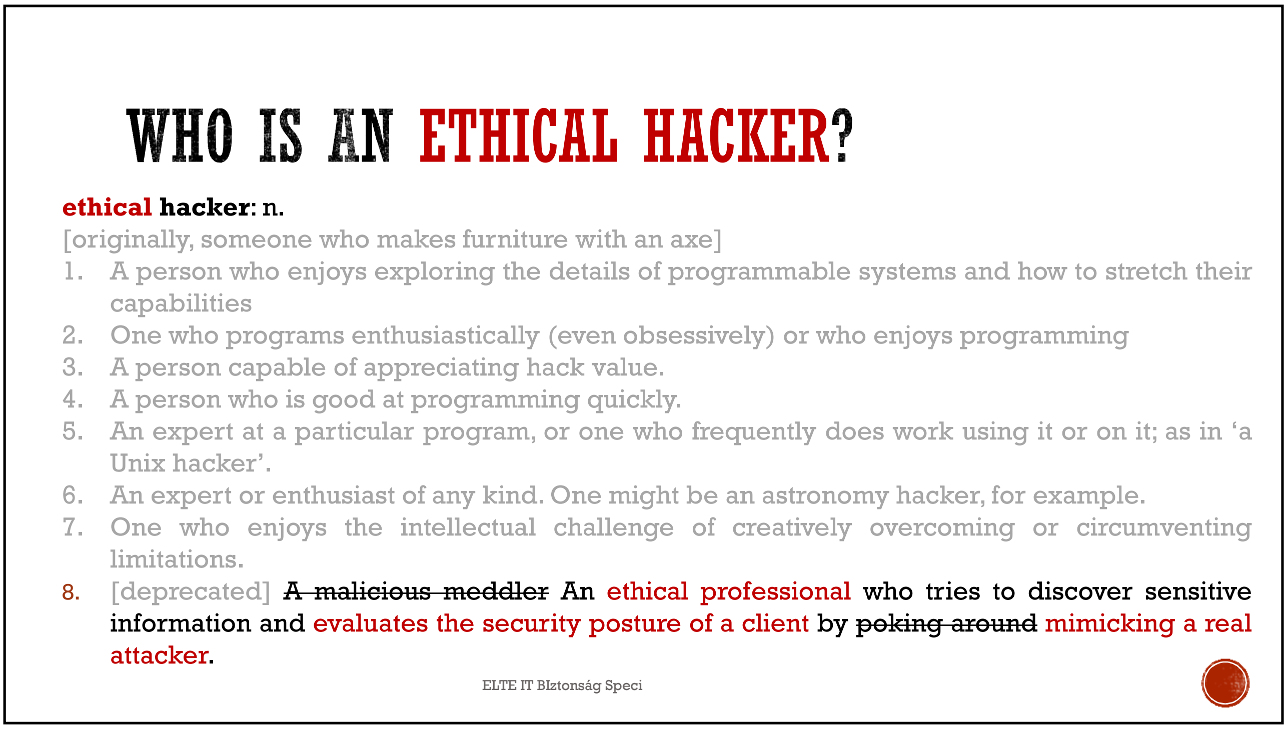


WHO IS A HACKER?

hacker: n.

[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities
2. One who programs enthusiastically (even obsessively) or who enjoys programming
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'.
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around.

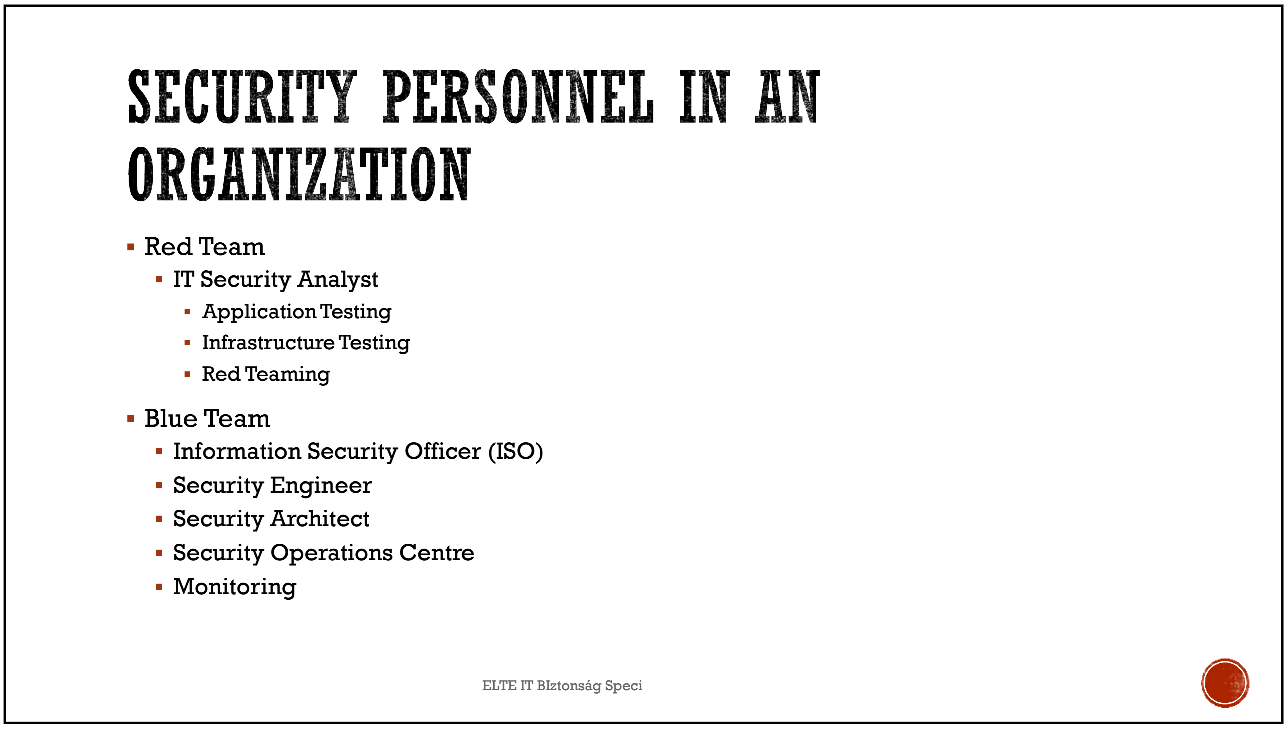


WHO IS AN ETHICAL HACKER?

ethical hacker: n.

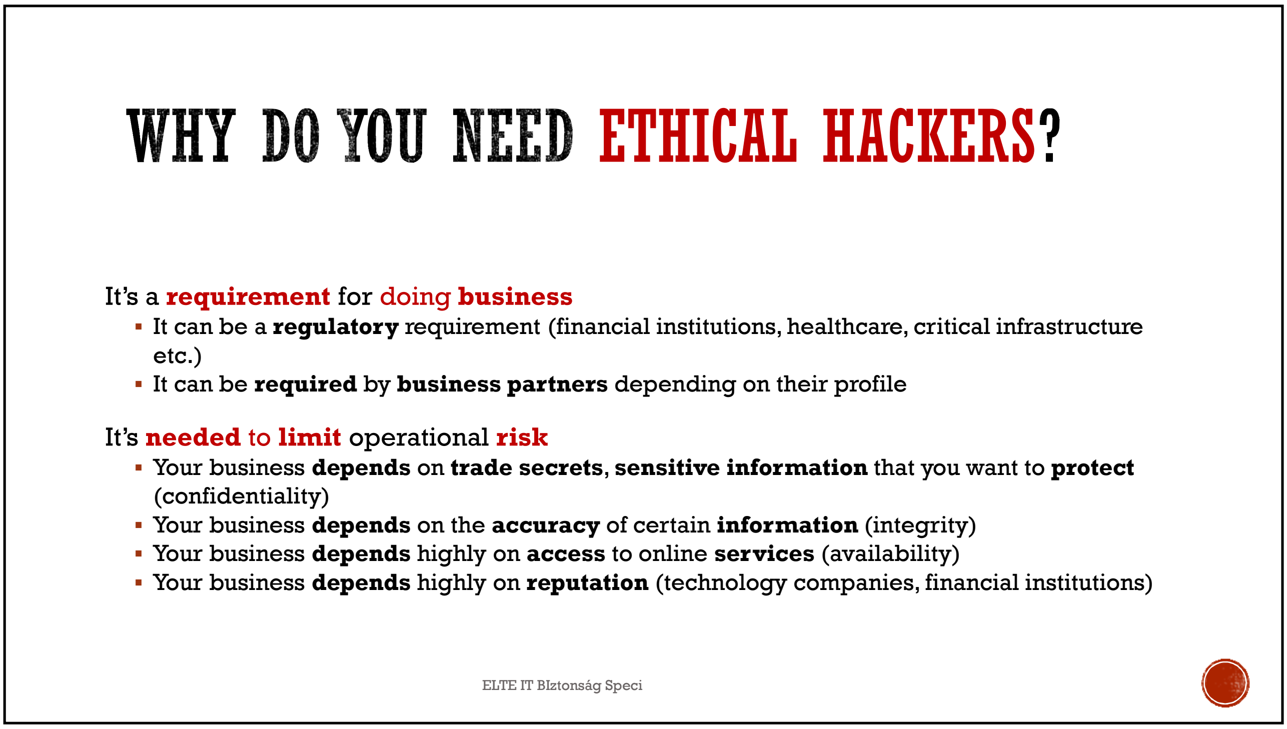
[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities
2. One who programs enthusiastically (even obsessively) or who enjoys programming
3. A person capable of appreciating hack value.
4. A person who is good at programming quickly.
5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'.
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. [deprecated] ~~A malicious meddler~~ An ethical professional who tries to discover sensitive information and evaluates the security posture of a client by ~~poking around~~ mimicking a real attacker.



SECURITY PERSONNEL IN AN ORGANIZATION

- Red Team
  - IT Security Analyst
    - Application Testing
    - Infrastructure Testing
    - Red Teaming
- Blue Team
  - Information Security Officer (ISO)
  - Security Engineer
  - Security Architect
  - Security Operations Centre
  - Monitoring



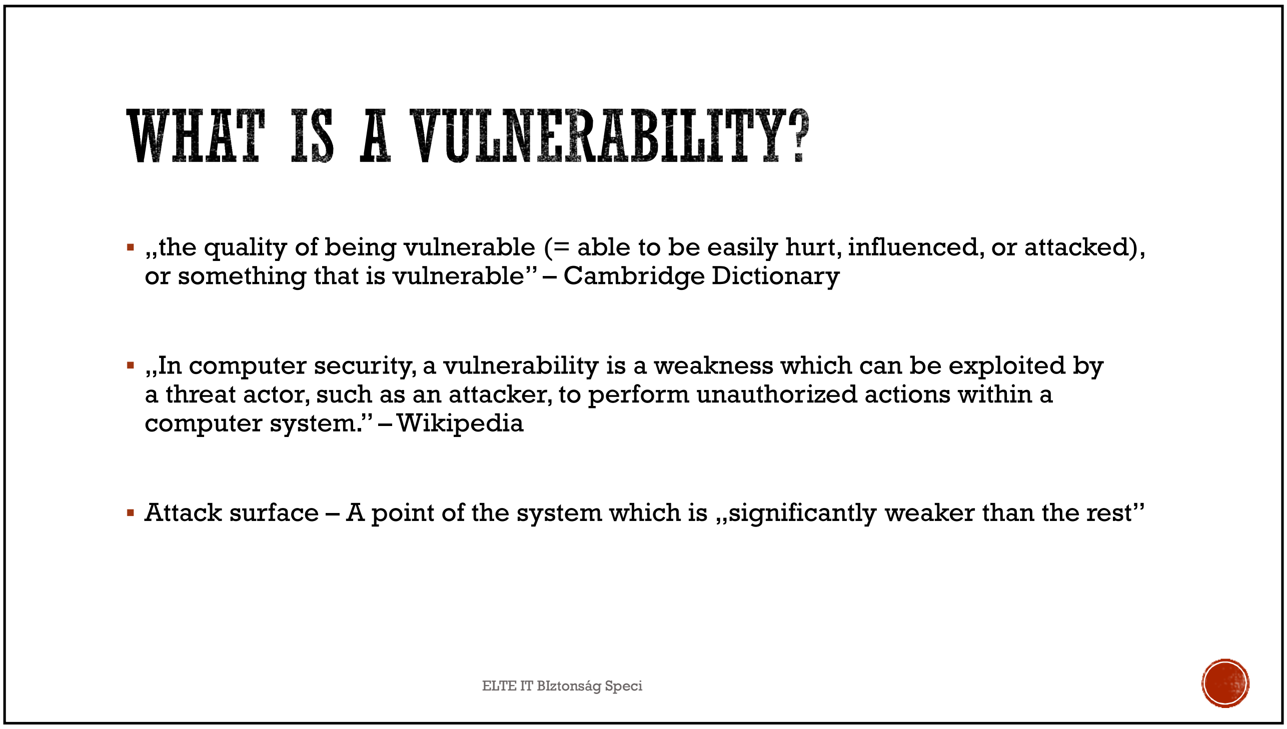
WHY DO YOU NEED ETHICAL HACKERS?

It's a **requirement** for doing **business**

- It can be a **regulatory** requirement (financial institutions, healthcare, critical infrastructure etc.)
- It can be **required** by **business partners** depending on their profile

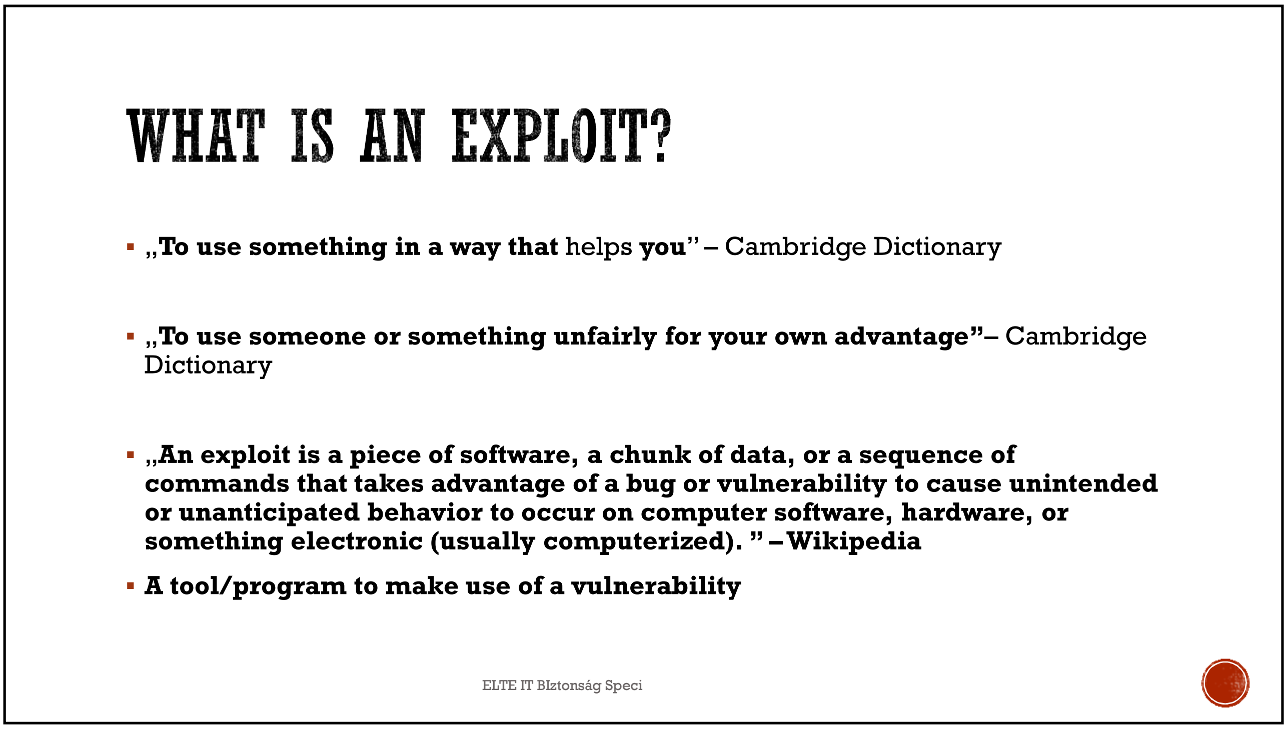
It's **needed** to **limit** operational **risk**

- Your business **depends** on **trade secrets**, **sensitive information** that you want to **protect** (confidentiality)
- Your business **depends** on the **accuracy** of certain **information** (integrity)
- Your business **depends** highly on **access** to online **services** (availability)
- Your business **depends** highly on **reputation** (technology companies, financial institutions)



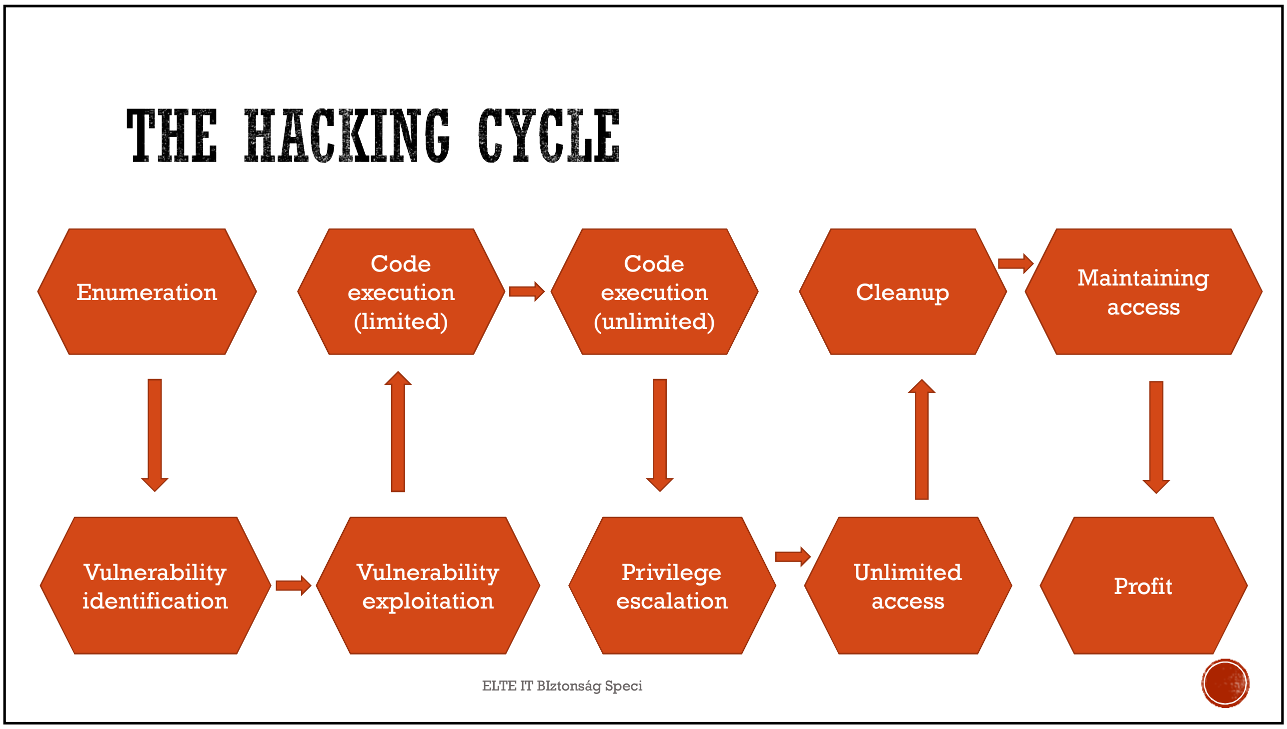
WHAT IS A VULNERABILITY?

- „the quality of being vulnerable (= able to be easily hurt, influenced, or attacked), or something that is vulnerable" – Cambridge Dictionary
- „In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system." – Wikipedia
- Attack surface – A point of the system which is „significantly weaker than the rest"



WHAT IS AN EXPLOIT?

- „**To use something in a way that** helps **you**" – Cambridge Dictionary
- „**To use someone or something unfairly for your own advantage"**– Cambridge Dictionary
- „**An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). " – Wikipedia**
- **A tool/program to make use of a vulnerability**



THE HACKING CYCLE

Enumeration

Code execution (limited)

Code execution (unlimited)

Cleanup

Maintaining access

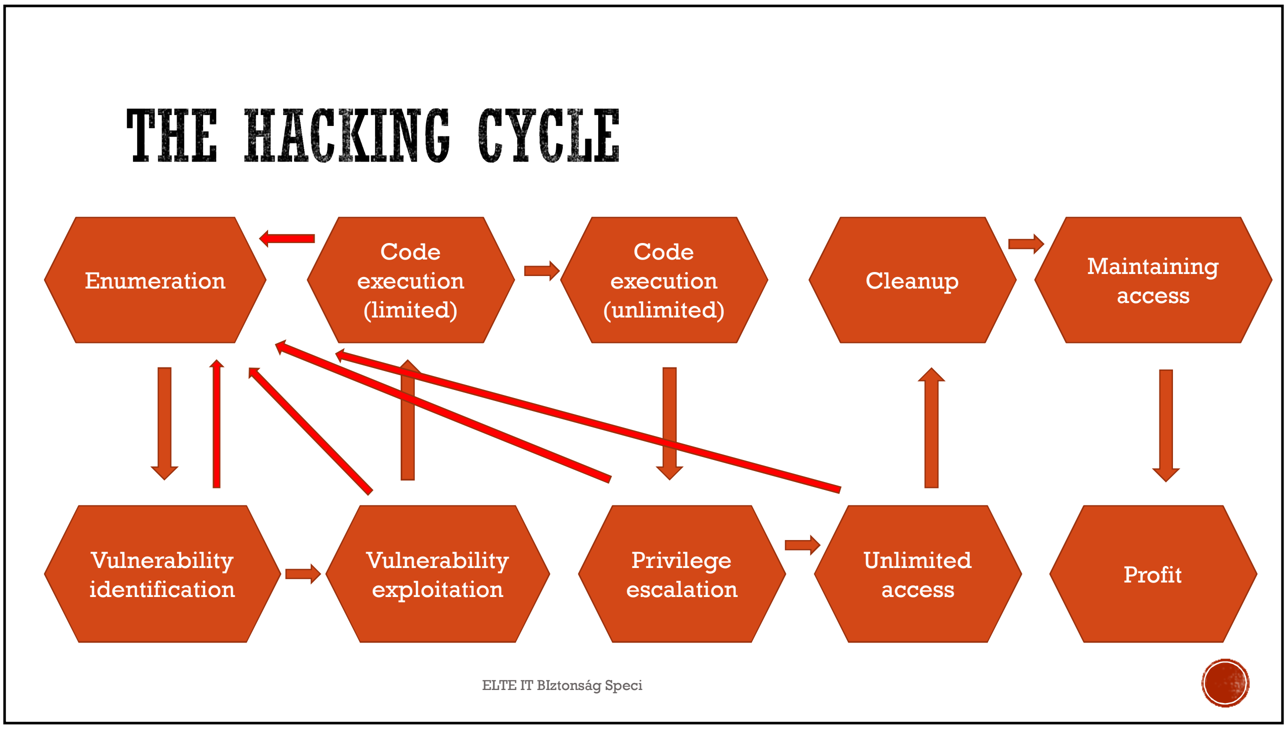
Vulnerability identification

Vulnerability exploitation

Privilege escalation

Unlimited access

Profit



THE HACKING CYCLE

Enumeration

Code execution (limited)

Code execution (unlimited)

Cleanup

Maintaining access

Vulnerability identification

Vulnerability exploitation

Privilege escalation

Unlimited access

Profit

WHAT IS VULNERABILITY ASSESSMENT (VA)?

- **Vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- Vulnerability assessment is a well (well, better) defined process, but often confused with **penetration testing**, which is goal oriented, i.e., a pentester makes an effort to control critical systems and acquire access to sensitive data.

VULNERABILITY CLASSIFICATION

🟦 Informational

🟩 Low

🟨 Medium

🟥 High

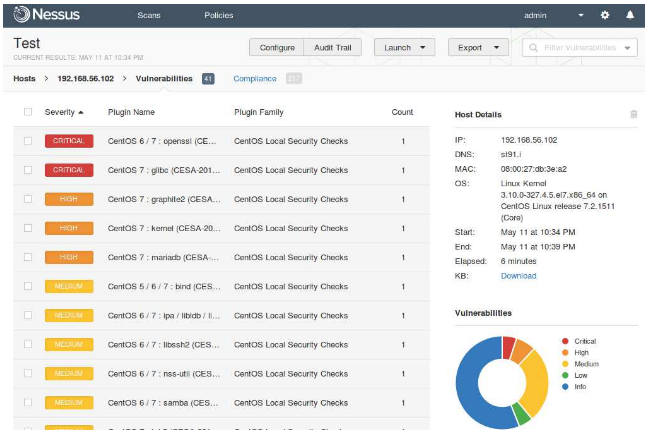
🟥 Critical

CVSS 3.0

THE VULNERABILITY DISCOVERY PROCESS

- Automated Tools
  - Qualys
  - Nessus
  - OpenVAS
- Manual
  - Vendor publications, CVEs
  - Service discovery (Nmap)

THE VULNERABILITY DISCOVERY PROCESS (NESSUS)



Test

CURRENT RESULTS: MAY 11 AT 10:34 PM

Hosts > 192.168.56.102 > Vulnerabilities 41

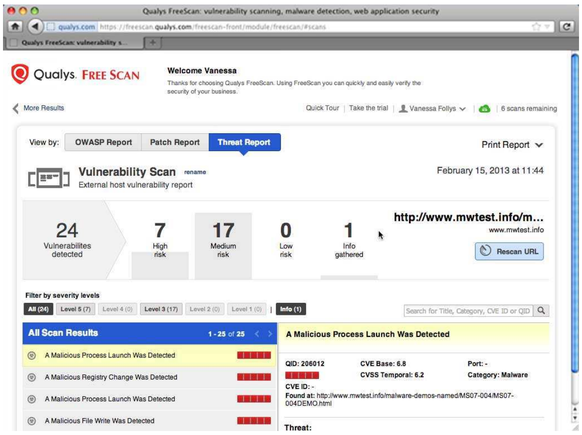
Severity	Plugin Name	Plugin Family	Count
CRITICAL	CentOS 6 / 7 : openssl (CE…	CentOS Local Security Checks	1
CRITICAL	CentOS 7 : glibc (CESA-201…	CentOS Local Security Checks	1
HIGH	CentOS 7 : graphite2 (CESA…	CentOS Local Security Checks	1
HIGH	CentOS 7 : kernel (CESA-20…	CentOS Local Security Checks	1
HIGH	CentOS 7 : mariadb (CESA-…	CentOS Local Security Checks	1
MEDIUM	CentOS 5 / 6 / 7 : bind (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : ipa / libldb / li…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : libssh2 (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : nss-util (CES…	CentOS Local Security Checks	1
MEDIUM	CentOS 6 / 7 : samba (CES…	CentOS Local Security Checks	1

Host Details

IP:	192.168.56.102
DNS:	st91.i
MAC:	08:00:27:db:3e:a2
OS:	Linux Kernel 3.10.0-327.4.5.el7.x86_64 on CentOS Linux release 7.2.1511 (Core)
Start:	May 11 at 10:34 PM
End:	May 11 at 10:39 PM
Elapsed:	6 minutes
KB:	Download

Vulnerabilities

THE VULNERABILITY DISCOVERY PROCESS (QUALYS)



Qualys FreeScan: vulnerability scanning, malware detection, web application security

https://freescan.qualys.com/freescan-front/module/freescan/#scans

Qualys. FREE SCAN

Welcome Vanessa

Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

< More Results | Quick Tour | Take the trial | Vanessa Follys | 6 scans remaining

View by: OWASP Report | Patch Report | **Threat Report** | Print Report

Vulnerability Scan rename
External host vulnerability report

February 15, 2013 at 11:44

24	7	17	0	1
Vulnerabilites detected	High risk	Medium risk	Low risk	Info gathered

http://www.mwtest.info/m...
www.mwtest.info
Rescan URL

Filter by severity levels

All (24) | Level 5 (7) | Level 4 (0) | Level 3 (17) | Level 2 (0) | Level 1 (0) | Info (1)

Search for Title, Category, CVE ID or QID

All Scan Results 1 - 25 of 25

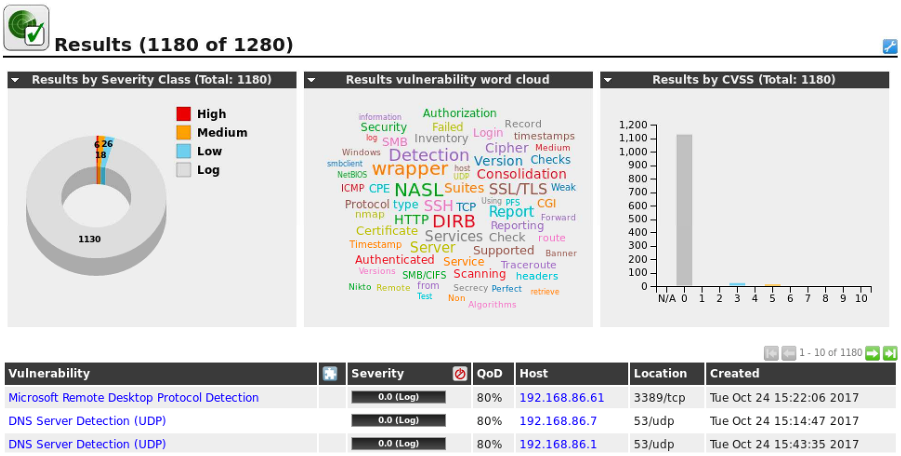
- A Malicious Process Launch Was Detected
- A Malicious Registry Change Was Detected
- A Malicious Process Launch Was Detected
- A Malicious File Write Was Detected

A Malicious Process Launch Was Detected

QID: 206012 | CVE Base: 6.8 | Port: -
CVSS Temporal: 6.2 | Category: Malware
CVE ID: -
Found at: http://www.mwtest.info/malware-demos-named/MS07-004/MS07-004DEMO.html

Threat:

THE VULNERABILITY DISCOVERY PROCESS (OPENVAS)



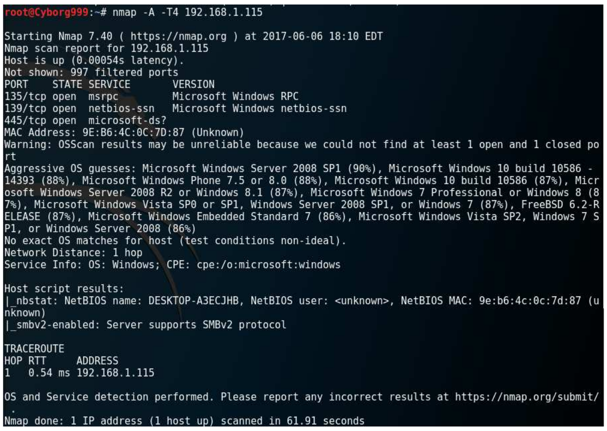
Results (1180 of 1280)

Results by Severity Class (Total: 1180)
High
Medium
Low
Log
6
26
18
1130
Results vulnerability word cloud
information Authorization Security Failed Record Login timestamps log SMB Inventory Cipher Medium Windows Detection Version Checks smbclient wrapper host NetBIOS UDP Consolidation ICMP CPE NASL Suites SSL/TLS Weak Protocol type SSH TCP Using PFS CGI nmap Report Forward HTTP DIRB Reporting Certificate Services Check route Timestamp Server Supported Banner Authenticated Service Traceroute Versions SMB/CIFS Scanning headers Nikto Remote from Secrecy Perfect retrieve Test Non Algorithms
Results by CVSS (Total: 1180)
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
N/A
0
1
2
3
4
5
6
7
8
9
10

1 - 10 of 1180

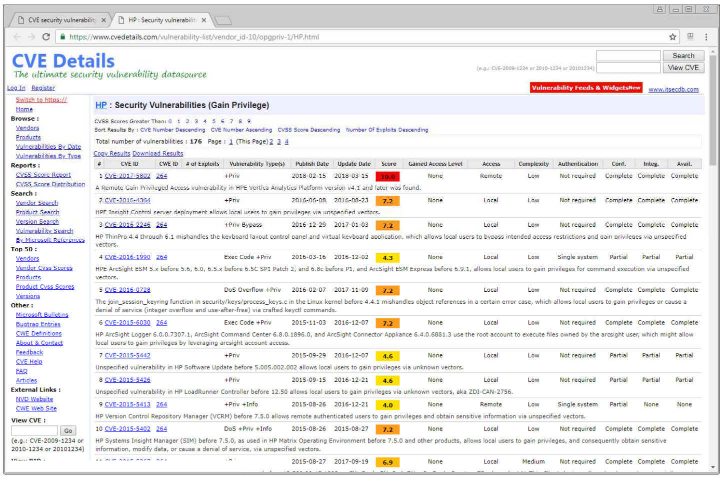
Vulnerability		Severity	QoD	Host	Location	Created
Microsoft Remote Desktop Protocol Detection		0.0 (Log)	80%	192.168.86.61	3389/tcp	Tue Oct 24 15:22:06 2017
DNS Server Detection (UDP)		0.0 (Log)	80%	192.168.86.7	53/udp	Tue Oct 24 15:14:47 2017
DNS Server Detection (UDP)		0.0 (Log)	80%	192.168.86.1	53/udp	Tue Oct 24 15:43:35 2017

THE VULNERABILITY DISCOVERY PROCESS (NMAP)



```
root@Cyborg999:~# nmap -A -T4 192.168.1.115

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-06 18:10 EDT
Nmap scan report for 192.168.1.115
Host is up (0.00054s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 9E:B6:4C:0C:7D:87 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed po
rt
Aggressive OS guesses: Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 build 10586 -
14393 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 build 10586 (87%), Micr
osoft Windows Server 2008 R2 or Windows 8.1 (87%), Microsoft Windows 7 Professional or Windows 8 (8
7%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), FreeBSD 6.2-R
ELEASE (87%), Microsoft Windows Embedded Standard 7 (86%), Microsoft Windows Vista SP2, Windows 7 S
P1, or Windows Server 2008 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-A3ECJHB, NetBIOS user: <unknown>, NetBIOS MAC: 9e:b6:4c:0c:7d:87 (u
nknown)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.54 ms 192.168.1.115

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 61.91 seconds
```

THE VULNERABILITY DISCOVERY PROCESS



CVE Details
The ultimate security vulnerability datasource

HP : Security Vulnerabilities (Gain Privilege)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

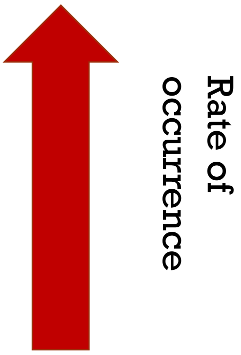
Total number of vulnerabilities : **176** Page : 1 (This Page) 2 3 4

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-5802	264		+Priv	2018-02-15	2018-03-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A Remote Gain Privileged Access vulnerability in HPE Vertica Analytics Platform version v4.1 and later was found.														
2	CVE-2016-4364			+Priv	2016-06-08	2016-08-23	7.2	None	Local	Low	Not required	Complete	Complete	Complete
HPE Insight Control server deployment allows local users to gain privileges via unspecified vectors.														
3	CVE-2016-2246	264		+Priv Bypass	2016-12-29	2017-01-03	7.2	None	Local	Low	Not required	Complete	Complete	Complete
HP ThinPro 4.4 through 6.1 mishandles the keyboard layout control panel and virtual keyboard application, which allows local users to bypass intended access restrictions and gain privileges via unspecified vectors.														
4	CVE-2016-1990	264		Exec Code +Priv	2016-03-16	2016-12-02	4.3	None	Local	Low	Single system	Partial	Partial	Partial
HPE ArcSight ESM 5.x before 5.6, 6.0, 6.5.x before 6.5C SP1 Patch 2, and 6.8c before P1, and ArcSight ESM Express before 6.9.1, allows local users to gain privileges for command execution via unspecified vectors.														
5	CVE-2016-0728			DoS Overflow +Priv	2016-02-07	2017-11-09	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.														
6	CVE-2015-6030	264		Exec Code +Priv	2015-11-03	2016-12-07	7.2	None	Local	Low	Not required	Complete	Complete	Complete
HP ArcSight Logger 6.0.0.7307.1, ArcSight Command Center 6.8.0.1896.0, and ArcSight Connector Appliance 6.4.0.6881.3 use the root account to execute files owned by the arcsight user, which might allow local users to gain privileges by leveraging arcsight account access.														
7	CVE-2015-5442			+Priv	2015-09-29	2016-12-07	4.6	None	Local	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in HP Software Update before 5.005.002.002 allows local users to gain privileges via unknown vectors.														
8	CVE-2015-5426			+Priv	2015-09-15	2016-12-21	4.6	None	Local	Low	Not required	Partial	Partial	Partial
Unspecified vulnerability in HP LoadRunner Controller before 12.50 allows local users to gain privileges via unknown vectors, aka ZDI-CAN-2756.														
9	CVE-2015-5413	264		+Priv +Info	2015-08-26	2016-12-21	4.0	None	Remote	Low	Single system	Partial	None	None
HP Version Control Repository Manager (VCRM) before 7.5.0 allows remote authenticated users to gain privileges and obtain sensitive information via unspecified vectors.														
10	CVE-2015-5402	264		DoS +Priv +Info	2015-08-26	2015-08-27	7.2	None	Local	Low	Not required	Complete	Complete	Complete
HP Systems Insight Manager (SIM) before 7.5.0, as used in HP Matrix Operating Environment before 7.5.0 and other products, allows local users to gain privileges, and consequently obtain sensitive information, modify data, or cause a denial of service, via unspecified vectors.														
[illegible]	[illegible]	[illegible]		[illegible]	2015-08-27	2017-09-19	6.9	None	Local	Medium	Not required	Complete	Complete	Complete

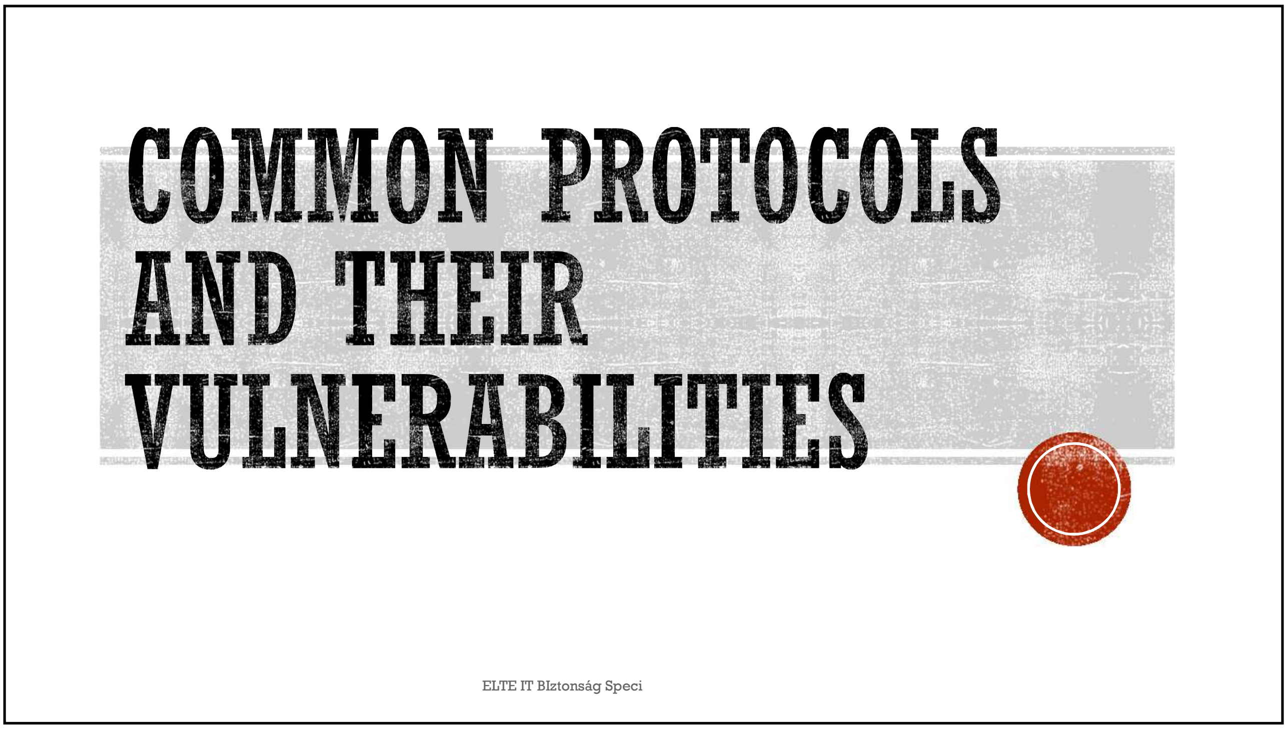
COMMON TYPES OF SECURITY ISSUES

- Configuration issues
  - Default username and password
  - Exposed admin interface
  - Forgotten features
- Implementation errors
  - High-level errors
    - Improper authorization
    - Race conditions
    - Logic bugs
  - Low level implementation issues
    - Buffer overflow
    - Heap overflow

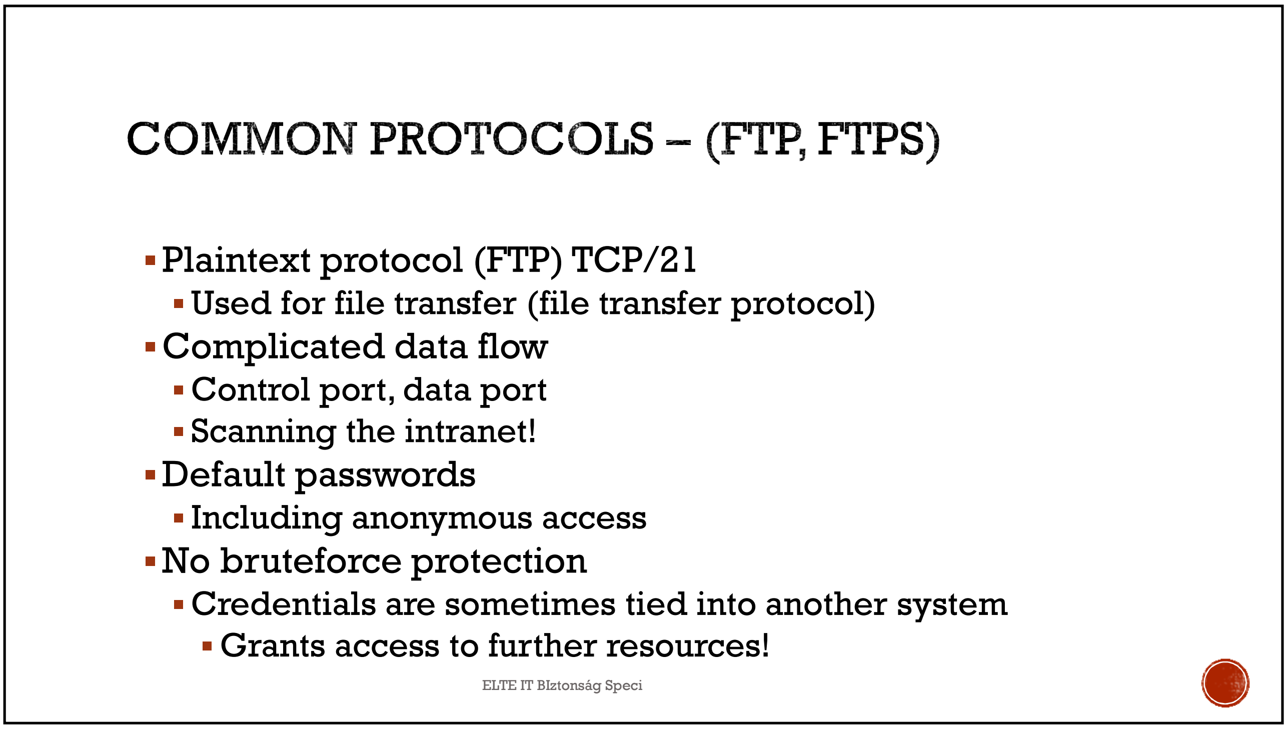


MITIGATING RISK

- Vulnerabilities are discovered, what do we do?
- **Ideally → Fix everything!**
- **Reality → Mitigate risk**
- **How? → Patches, configuration changes, policy updates, personnel training, extreme measures (rare, but should be more frequent)**
- **A cycle rather than a linear process**

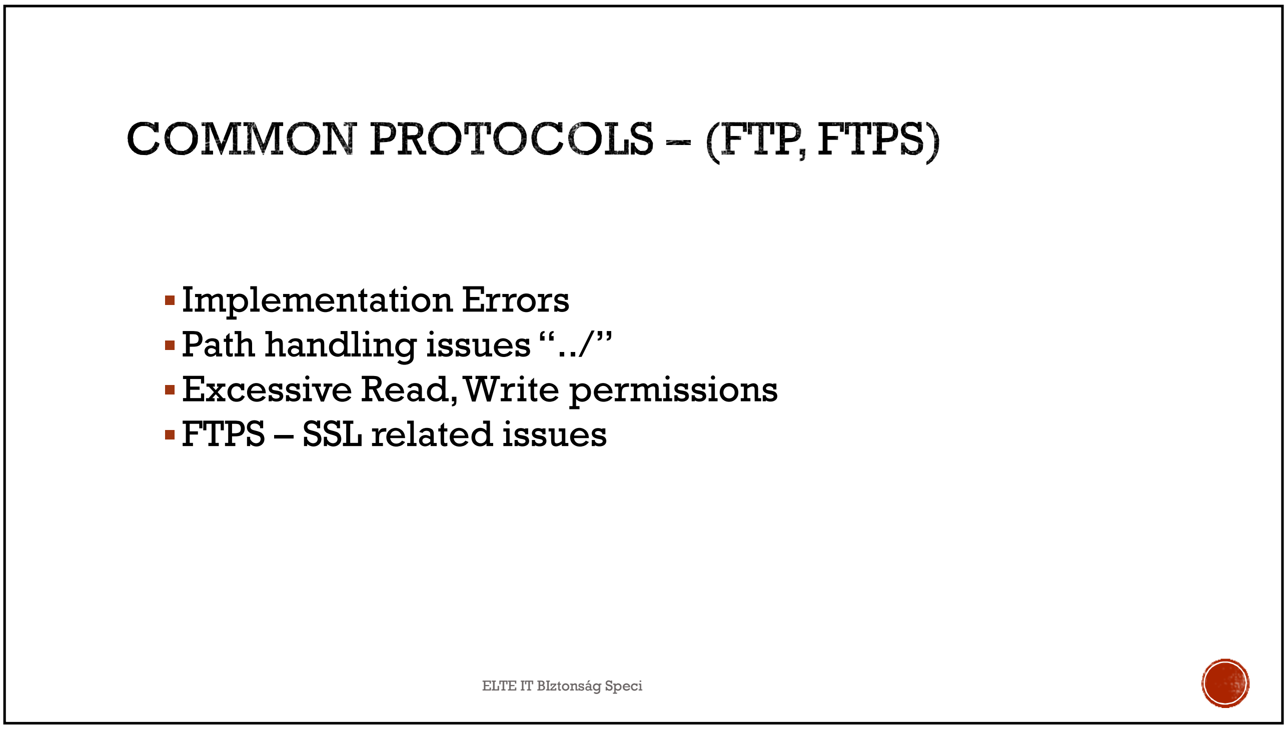


COMMON PROTOCOLS AND THEIR VULNERABILITIES



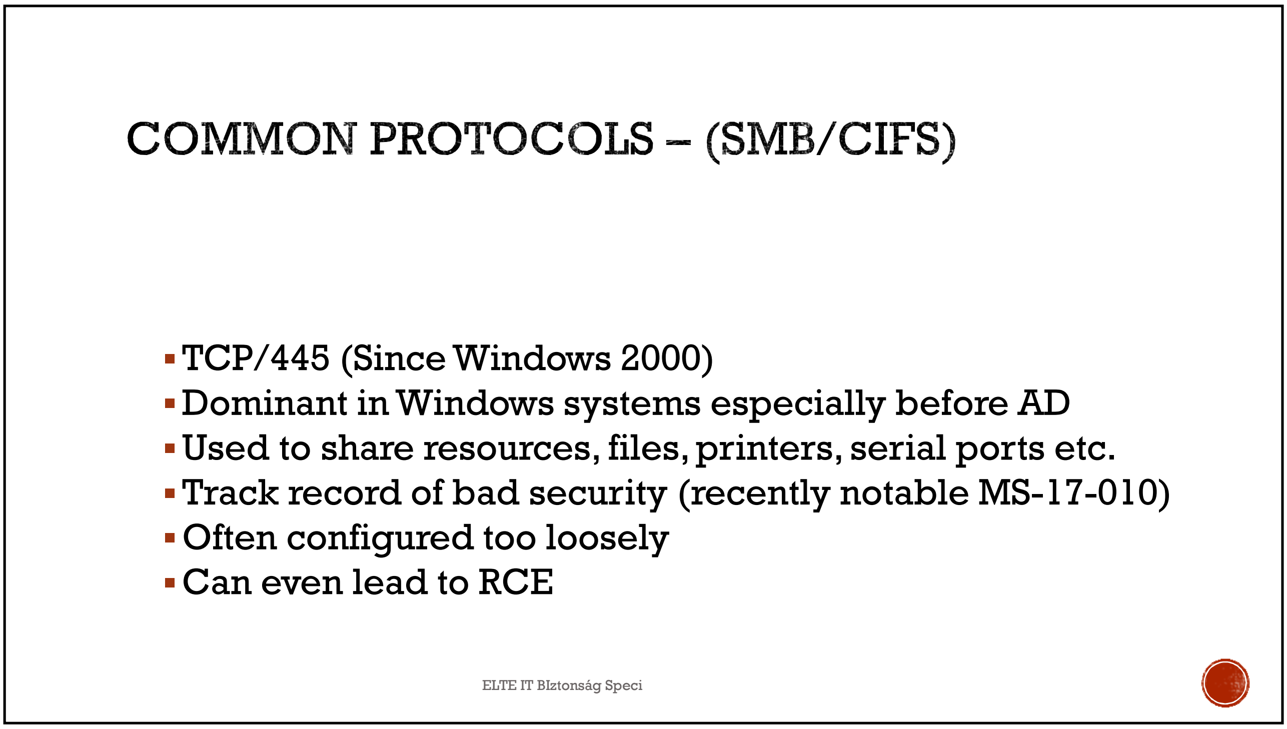
COMMON PROTOCOLS – (FTP, FTPS)

- Plaintext protocol (FTP) TCP/21
  - Used for file transfer (file transfer protocol)
- Complicated data flow
  - Control port, data port
  - Scanning the intranet!
- Default passwords
  - Including anonymous access
- No bruteforce protection
  - Credentials are sometimes tied into another system
    - Grants access to further resources!



COMMON PROTOCOLS – (FTP, FTPS)

- Implementation Errors
- Path handling issues "../"
- Excessive Read, Write permissions
- FTPS – SSL related issues

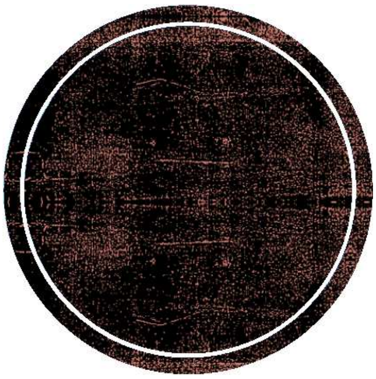


COMMON PROTOCOLS – (SMB/CIFS)

- TCP/445 (Since Windows 2000)
- Dominant in Windows systems especially before AD
- Used to share resources, files, printers, serial ports etc.
- Track record of bad security (recently notable MS-17-010)
- Often configured too loosely
- Can even lead to RCE

EXAMPLE 1 – ETERNAL BLUE

- Microsoft's implementation of SMB contained a crucial flaw → vulnerability
- The NSA weaponized the vulnerability instead of disclosing it
- The exploit got leaked
- Chaos ensued → Widespread exploitation, ransomware, WannaCry, NotPetya



COMMON PROTOCOLS – (NFS)

- TCP/2049
- Used for file sharing (Network File System)
- "no_root_squash" option is set for exports
- The "privileged ports" option is not set (not really relevant anymore)
- Client machines mount shares without "nosuid"

COMMON PROTOCOLS – (DNS)

- UDP/53, TCP/53
- Recursive protocol for resolving domain names
- Open Recursive DNS Servers Denial-of-Service (DoS)
  - Requesting queries with source IP spoofing
  - Large response leads to amplification
- Cache poisoning attack
  - Additional information section is cached by DNS server
    - Redirecting the name server
    - Redirecting the NS record

EXAMPLE 2 – BANRISUL BANK

- Brazilian bank had its entire DNS architecture compromised
- The attackers built an entire fake bank
- For multiple hours, all traffic was redirected to the fake bank
- Damage was immense

COMMON PROTOCOLS – (SNMP)

- TCP/161, UDP/161
- Default credentials, community string
  - Modification of system parameters
- Vendor specific MIBs
  - Even code execution may be possible

COMMON PROTOCOLS – (SSL)

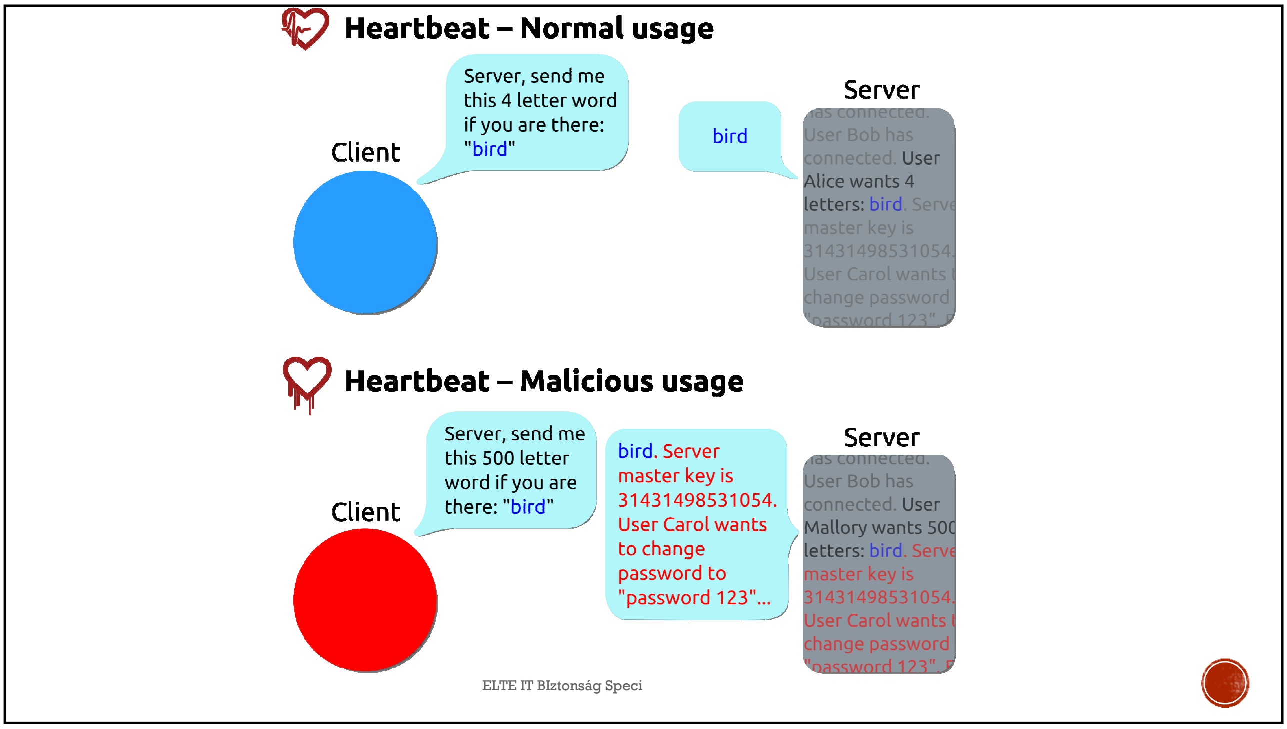
- Weak Encryption Issues
  - Weak Ciphers are used by the server
    - No Cipher order is forced by the server
  - Weak protocol versions are allowed (SSLv1, SSLv2, SSLv3, TLS/1.0)
- Weak, bad certificate issues
  - Incomplete Chain of Trust
  - Weak hashing algorithm
- Weak parameters
  - Small encryption keys
  - Small DH parameters

COMMON PROTOCOLS – (SSL)

- Protocol Issues
  - Freak (Factoring RSA Export Keys)
  - Logjam (Export DH parameters)
  - BREACH, CRIME (Compression related issues)
  - POODLE (Padding Oracle attack)
  - Heartbleed (Memory leak)

EXAMPLE 3 – HEARTBLEED

- Buffer overread vulnerability in OpenSSL
- Exploits the heartbeat keepalive functionality
- Lets attackers read chunks of server memory
- Difficult to control but can leak anything: passwords, secret keys etc.

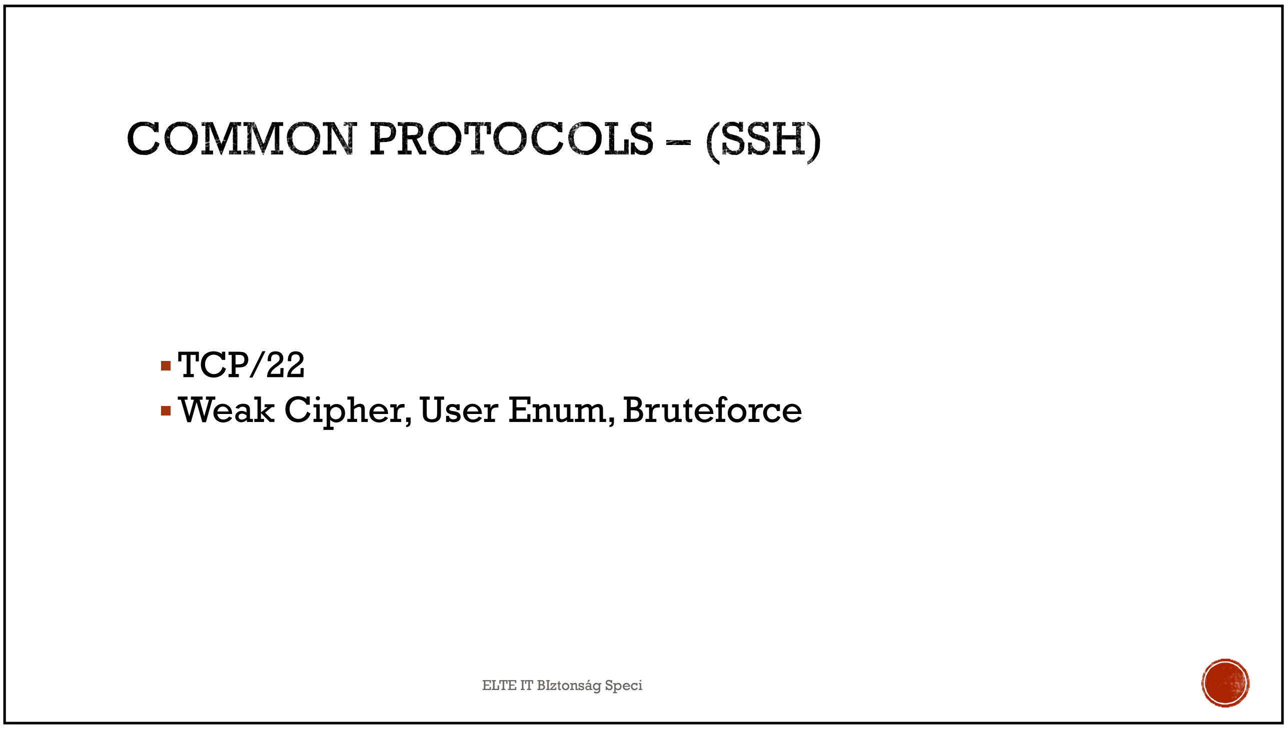


Heartbeat – Normal usage

Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". F

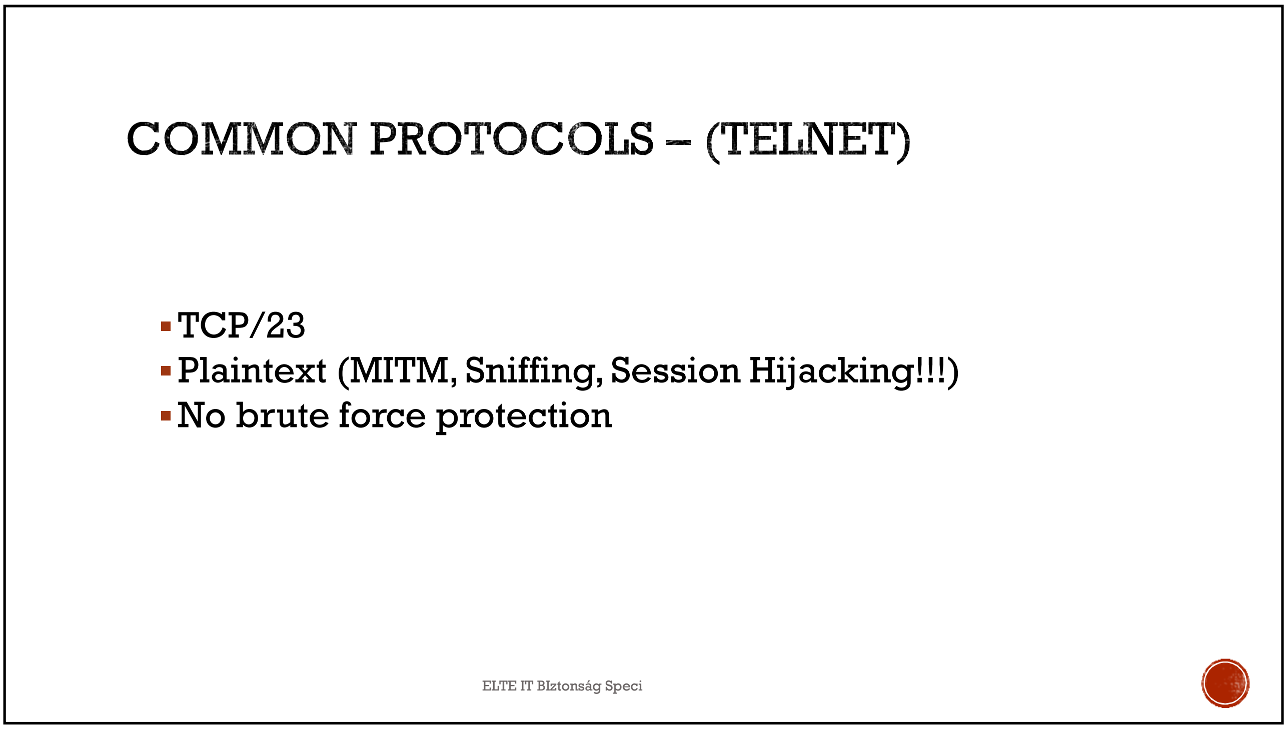
Heartbeat – Malicious usage

Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". F



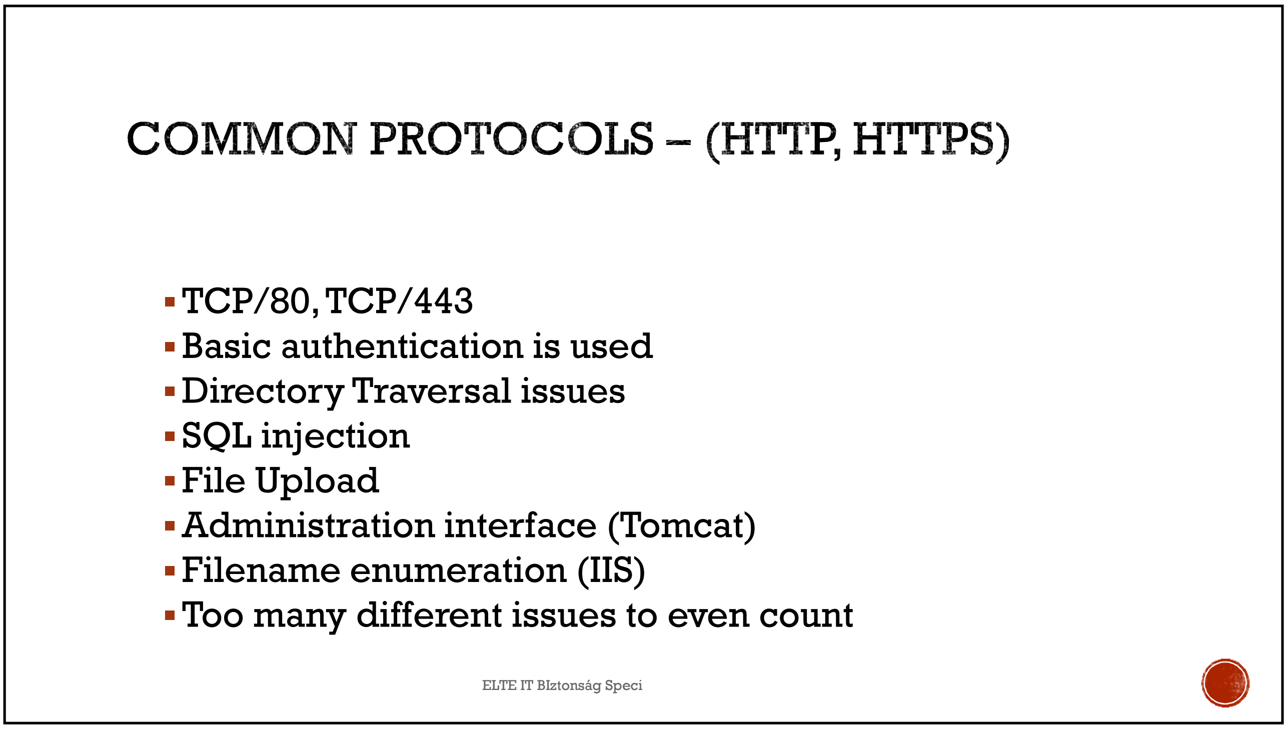
COMMON PROTOCOLS – (SSH)

- TCP/22
- Weak Cipher, User Enum, Bruteforce



COMMON PROTOCOLS – (TELNET)

- TCP/23
- Plaintext (MITM, Sniffing, Session Hijacking!!!)
- No brute force protection



COMMON PROTOCOLS – (HTTP, HTTPS)

- TCP/80, TCP/443
- Basic authentication is used
- Directory Traversal issues
- SQL injection
- File Upload
- Administration interface (Tomcat)
- Filename enumeration (IIS)
- Too many different issues to even count