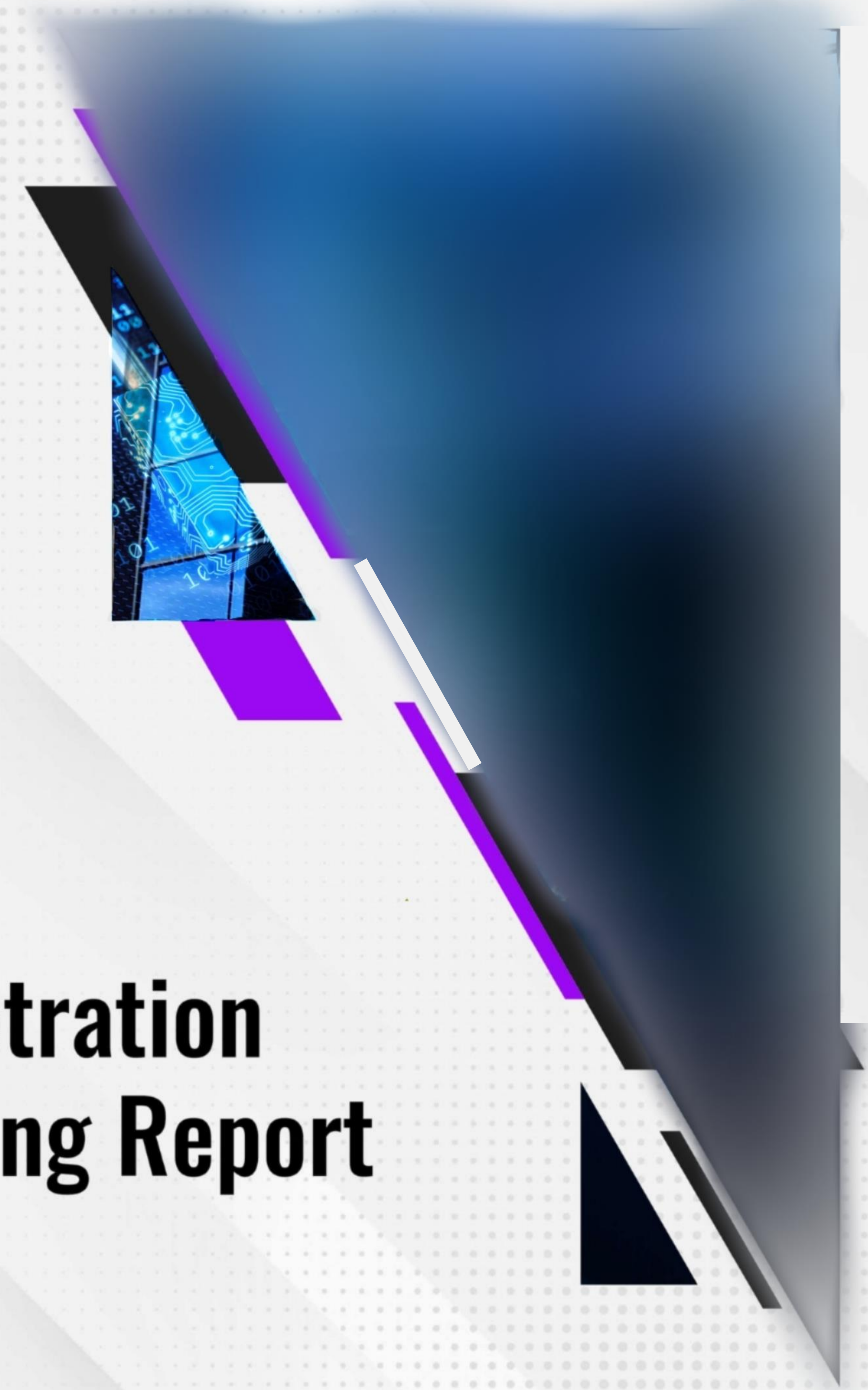


Penetration Testing Report

AMZ47

- **Certain information has been intentionally concealed due to security considerations.**
- **It might come to your attention that the Penetration Test focused on surface-level aspects, and that is related to the company's desire.**

TABLE OF CONTENTS:

• Introduction:

• Summary Of Findings:

• Vulnerabilities: (CVSS -Description - Risks - Solutions)

• Recommendation:

INTRODUCTION:

Cyber-Attacks are considered one of the biggest problems of the current era, because of the integration of the digital world in our lives, and businesses are most affected.

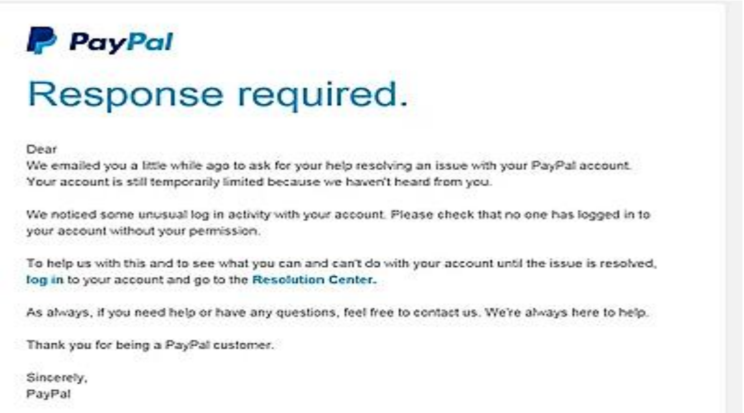
- where it is only in January 2019 alone More than 1.76 billion corporate records leaked.
- Ransomware attacks happen every 14 seconds in the world.
- 43% of cyber-attacks are targeted at small businesses and which was established recently.

And your company is not exempt from this matter, especially a it subsidiary of a large company such as [redacted] as it can be used as a means to penetrate the parent company. because They are not separate, the files are transferred between the two companies.

Yes, it is true that these cyber-attacks will not be able to reach production machines and cause work accidents, but they are still at the same level of danger, because they will target members of the administration (the company's money).

And the Cyber-Attacks have already happened, but **luckily** they weren't targeted but rather random, so they didn't cause a lot of damage.

There are a lot of **Phishing** attacks that have occurred and continue to occur, but the members of the administration were intelligent and did not fall into the trap.



PayPal

Response required.

Dear
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

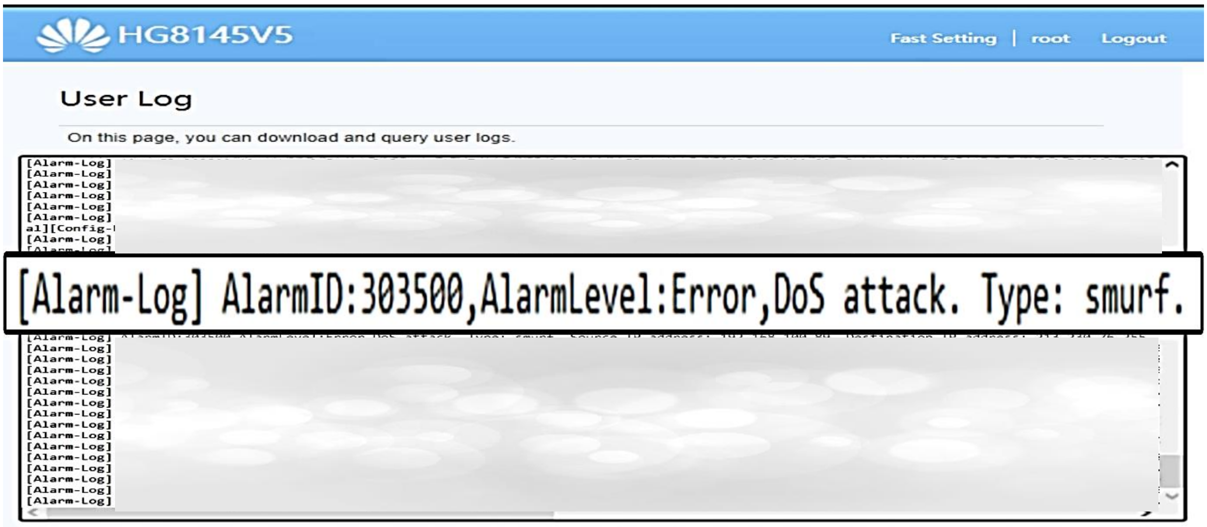
Sincerely,
PayPal

There are two company accounts whose password has been leaked. The password must be changed as soon as possible:

- [redacted]**@qq.com**
  (the Chinese e-commerce service **JD** suffered a data breach**)**
- [redacted]**@gmail.com**
  (China's largest online forum known as **Tianya** was hacked**)**

⚠ WARNING:

Also, I detect an attack by a virus (Trojan) where the company's devices are used as zombies in DDOS attacks (denial-of-service).

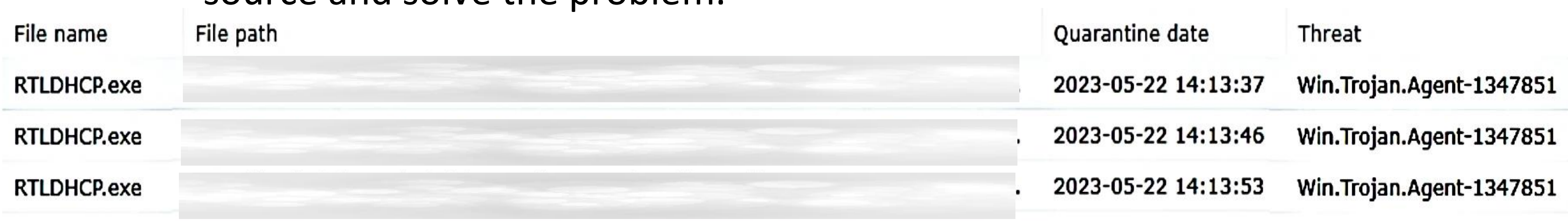


User Log

On this page, you can download and query user logs.

```
[Alarm-Log] [redacted]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
al][Config-I
[Alarm-Log]
[Alarm-Log] AlarmID:303500,AlarmLevel:Error,DoS attack. Type: smurf.
[Alarm-Log] [redacted]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
[Alarm-Log]
```

Because the matter urgent, I intervened, I scan **Synology** device, and I detect three Trojan files and deleted them, and install anti-virus in Device. but despite that, the attack is still continuing because the virus has spread in the network, and we need to scan all devices in the network to find the source and solve the problem.



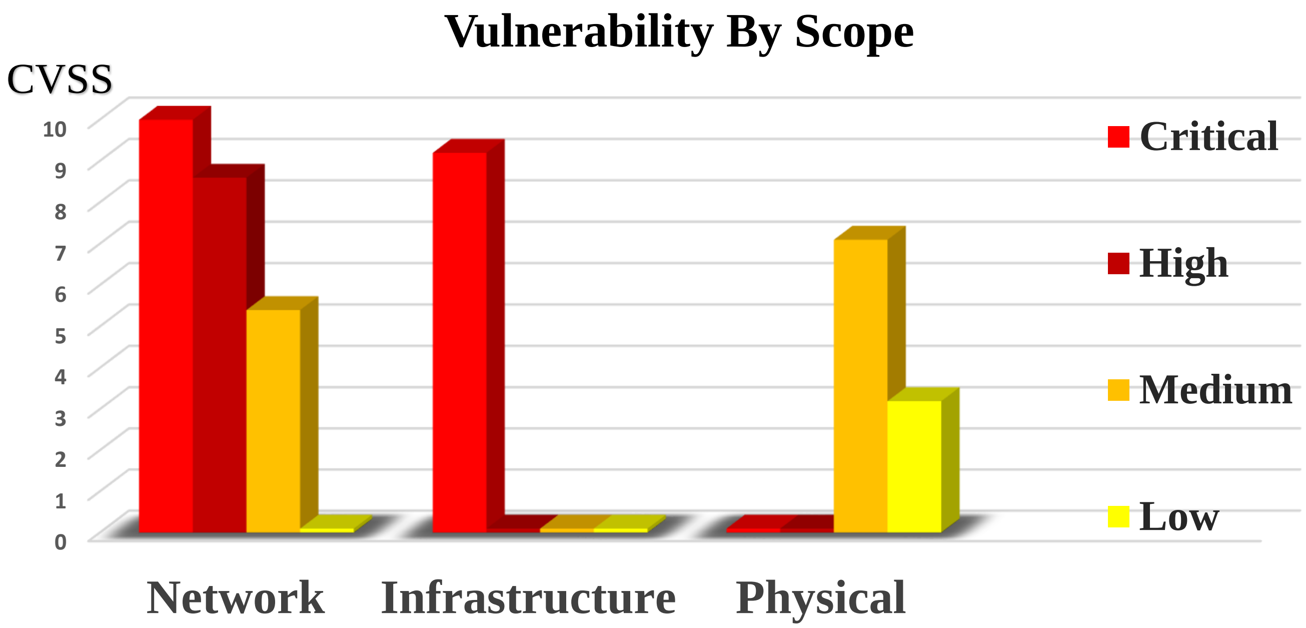
File name	File path	Quarantine date	Threat
RTLDHCP.exe	[redacted]	2023-05-22 14:13:37	Win.Trojan.Agent-1347851
RTLDHCP.exe	[redacted]	2023-05-22 14:13:46	Win.Trojan.Agent-1347851
RTLDHCP.exe	[redacted]	2023-05-22 14:13:53	Win.Trojan.Agent-1347851

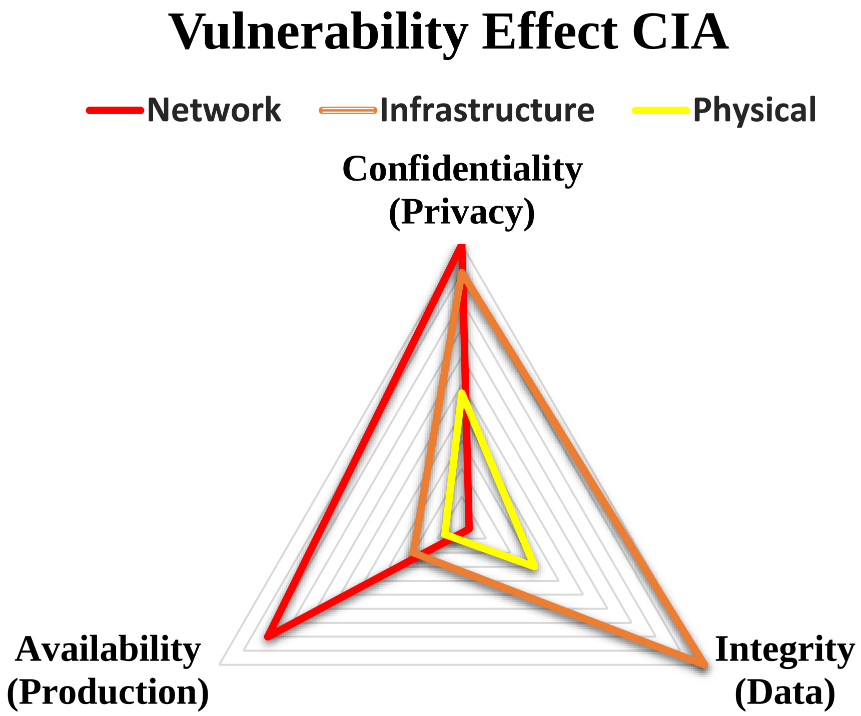
CVSS — Risk Classification

CVSS stands for **C**ommon **V**ulnerability **S**coring **S**ystem. It is a framework globally used to assess and quantify the severity of security vulnerabilities in computer systems and software.

Risk Level	Description
Critical **10 - 9.0**	the highest severity, representing vulnerabilities that pose a severe risk to system confidentiality, integrity, and availability. Exploiting be easy, without requiring user interactions. **You must prioritize promptly remedying.**
High **8.9 - 7.0**	have a high potential to cause harm and can have a severe impact on the confidentiality, integrity, or availability of the affected system. Exploiting relatively easy, and do not require complex conditions. **should be addressed.**
Medium **6.9 - 4.0**	have a moderate potential to cause harm and may have a significant impact on the confidentiality, integrity, or availability of the affected system. Exploiting require a certain level of skill or specific conditions.
Low **3.9 - 0.1**	have limited potential to cause harm and are often difficult to exploit. They may have minimal impact on the confidentiality, integrity, or availability of the affected system.

Summary Of Findings





Vulnerability :

- ⚠ The administrator password for the router is the default.
- ⚠ All users use the administrator account for normal daily use.
- ⚠ An Easy-to-Guess Password WIFI.
- ⚠ One password in several networks WIFI.
- ⚠ Not disable USB ports in public areas.
- ⚠ USB ports are not locked with a password.
- ⚠ All devices are connected in one VLAN.
- ⚠ BIOS settings are not password protected.

Risks :

- ⚠ Unauthorized Access to Sensitive Information, such as bank account passwords, email messages, and all other data.
- ⚠ Stop all digital or online works and activities.
- ⚠ Loss or Delete All Data.
- ⚠ Installation of Malicious Programs and Spread of Viruses and Malware.
- ⚠ Network Tampering, Disruption and System Manipulation.
- ⚠ Leaking sensitive information

CRITICAL: DEFAULT PASSWORD

9.6 CVSS

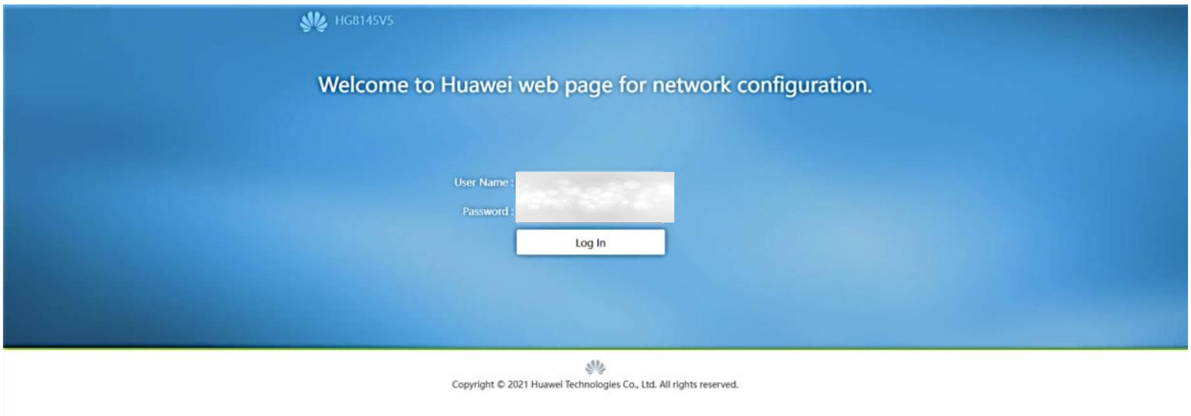
Network

⚠ **The administrator password for the router is the default.**

- **User Name:** [redacted]
- **Password:** [redacted]

Description:

The router's password is a default password provided by the factory, which is standardized across all routers and widely known. This poses a significant security risk as anyone connected to the network can potentially gain control over the entire network, as well as its devices and data.



HG8145V5

Welcome to Huawei web page for network configuration.

User Name : [redacted]

Password :

Log In

Copyright © 2021 Huawei Technologies Co., Ltd. All rights reserved.

Risks:

- ⚠ **By instructing the router to forward all data to hacker device, the hacker can gain access to all sensitive information transmitted over the network, such as bank account passwords, email messages, and all other data. (Just by knowing the router password)**
- ⚠ **Anyone can tamper the network settings, turn it off, or block the devices. (In the best case scenario, a full day's work will be wasted repairing the router.)**
- ⚠ **disable all network protection protocols, thus making all connected devices vulnerable to hacking easily…**

Solutions:

Change Password

Recommendations:

- ✓ **Do not use any default passwords.**
- ✓ **Use a complex password (P@ssW0rd-07).**
- ✓ **The password can only be known by the administrator IT.**

CRITICAL: Admin User

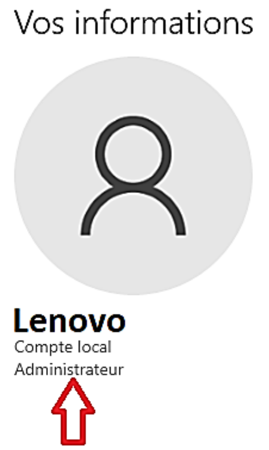
⚠ **All users use the administrator account for normal daily use.**

9.0
CVSS

Infrastructure

Description:

All people use Administrator account in their work and also in normal usage, that means they have all the permission to do anything. And they never need these permissions to do their job



Vos informations

Lenovo
Compte local
Administrateur

Risks:

- **Install viruses or malicious programs (deliberately or unintentionally) that spread to all the company's devices and pose a danger to them (such as ransomware).**
- **Execute malicious commands that pose a threat to the and data and the devices connected to the network.**
- **Delete all data.**
- **It can unintentionally cause the computer to crash.**

Solutions:

- **Use the normal user account.**
- **The right authorization for the right person for the right job at the right location.**
- **Close the administrator account with a password that only the administrator IT knows.**

Recommendations:

✓ **Using Windows Server to easily control all users access and give them the appropriate permissions (See Page 11).**

HIGH: Password Easy-to-guess

⚠ **An Easy-to-Guess Password WIFI.**

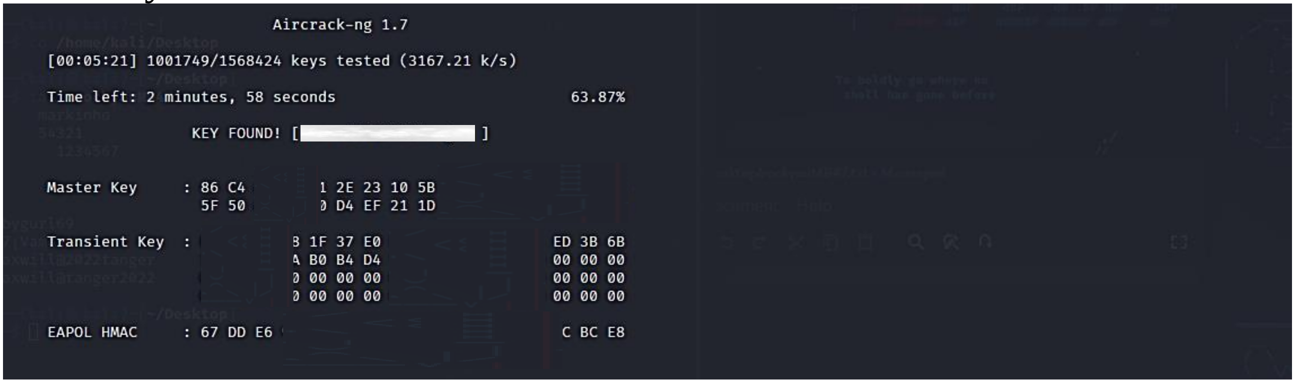
⚠ **One password in several networks WIFI.**

8.3 CVSS

Network

Description:

The password used can easily be guessed. Because it consists of general information about the company ([redacted]). The hacker does not guess and experiment manually, but rather uses programs that give it only possible words, and it does everything, as it can try more than 2000 passwords per second, and this means that it will inevitably find the password. Which is what I tried as the program took only 2 minutes and 58 seconds to find it:



```
                               Aircrack-ng 1.7

      [00:05:21] 1001749/1568424 keys tested (3167.21 k/s)

      Time left: 2 minutes, 58 seconds                          63.87%

                          KEY FOUND! [ [redacted] ]


      Master Key     : 86 C4 [redacted] 1 2E 23 10 5B
                       5F 50 [redacted] 0 D4 EF 21 1D

      Transient Key  : [redacted] 3 1F 37 E0 [redacted] ED 3B 6B
                                  A B0 B4 D4             00 00 00
                                  0 00 00 00             00 00 00
                                  0 00 00 00             00 00 00

      EAPOL HMAC     : 67 DD E6 [redacted]                C BC E8
```

Risks:

- **Of course, an easy-to-guess password is easy to hack, and this puts all data and devices connected to the network at risk.**
- **Using one password in several WIFI networks makes it easier for a hacker to penetrate all networks because he can target the weakest or closest network that can be accessed from outside the company and extract the password.**
- **The mobile devices of the members of the administration can be easily targeted as they automatically connect to the nearest network.**

Solutions:

- **Using complex passwords that do not contain any public information related to the company.**
- **Use a different password for each WIFI network.**

Recommendations:

✓ **Giving each category of company members a private Wi-Fi network that only they connect to.**

MEDIUM: Ports USB

⚠ **Not disable USB ports in public areas.**
⚠ **USB ports are not locked with a password.**

6.9 CVSS

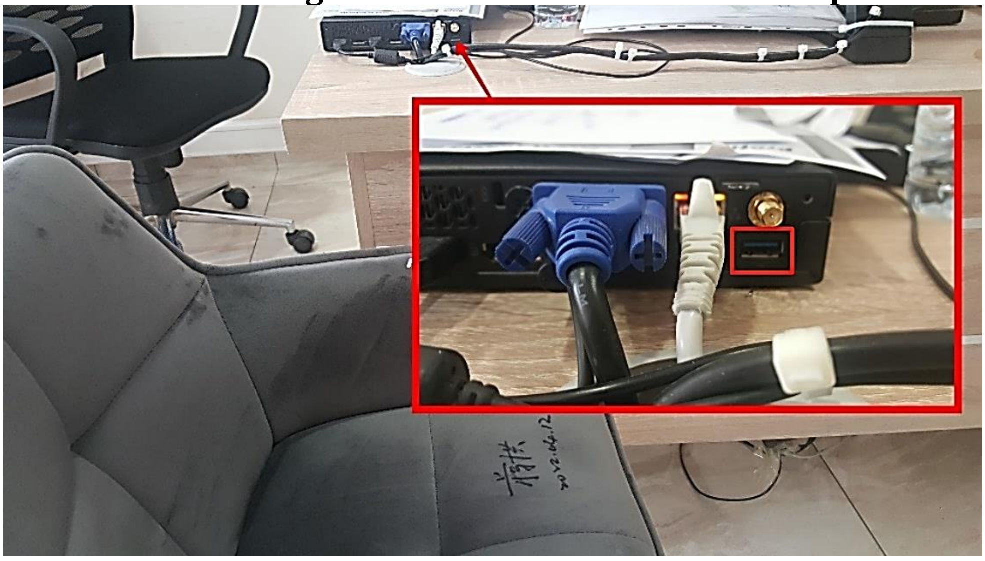
Physical

Description:

There is no protection for the USB ports, anyone can connect any device into the computer without requiring any authorization, even in devices located in dangerous public areas, thereby gaining access to the infrastructure.

Risks:

- ⚠ **The company can be hacked during a job interview where the hacker can connect a device such as USB RUBBER DUCKY or BASH BUNNY and it will take 7 seconds for the device to do the thing it was programmed on, either it will automatically copy all the data or it will spread a virus or it will give the hacker access to the computer remote.**



- ⚠ **The risk can be internal, where an employee without authorized access copies confidential data and leaks it either as an act of retaliation against another employee or the company itself.**

Solutions:

- **Lock USB ports with a password.**
- **Use USB Defender.**
- **Disable USB ports in public areas.**

Recommendations:

- ✓ **Use a different password on each computer.**
- ✓ **Only the owner of the computer knows the password.**

MEDIUM: All in One Vlan

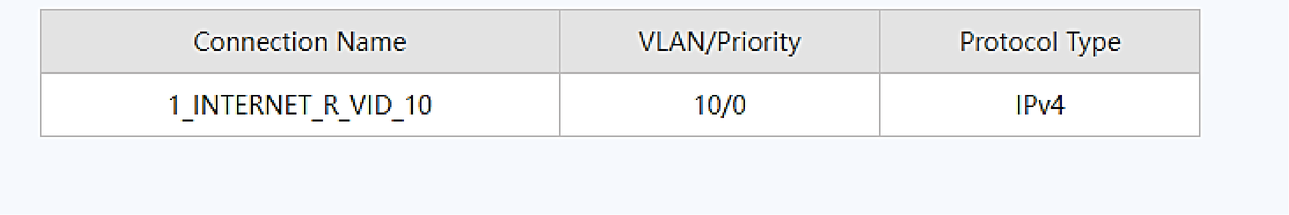
⚠ **All devices are connected in one Vlan.**

5.1 CVSS

Network

Description:

All wired and wireless connected devices, company computers, phones and personal devices are connected in one vlan:



Connection Name	VLAN/Priority	Protocol Type
1_INTERNET_R_VID_10	10/0	IPv4

Risks:

- ⚠ **If a single device becomes infected with a virus, it can potentially spread to all other devices connected to the network.**
- ⚠ **The network's vulnerability to hacking increases due to the presence of personal devices connected that do not adhere to security standards.**
- ⚠ **Ordinary users have the capability to spy on administrative devices.**

Solutions:

- **Create a vlan for each category of company members.**

Recommendations:

- ✓ **Permanently separate work devices from personal devices.**

LOW: BIOS settings

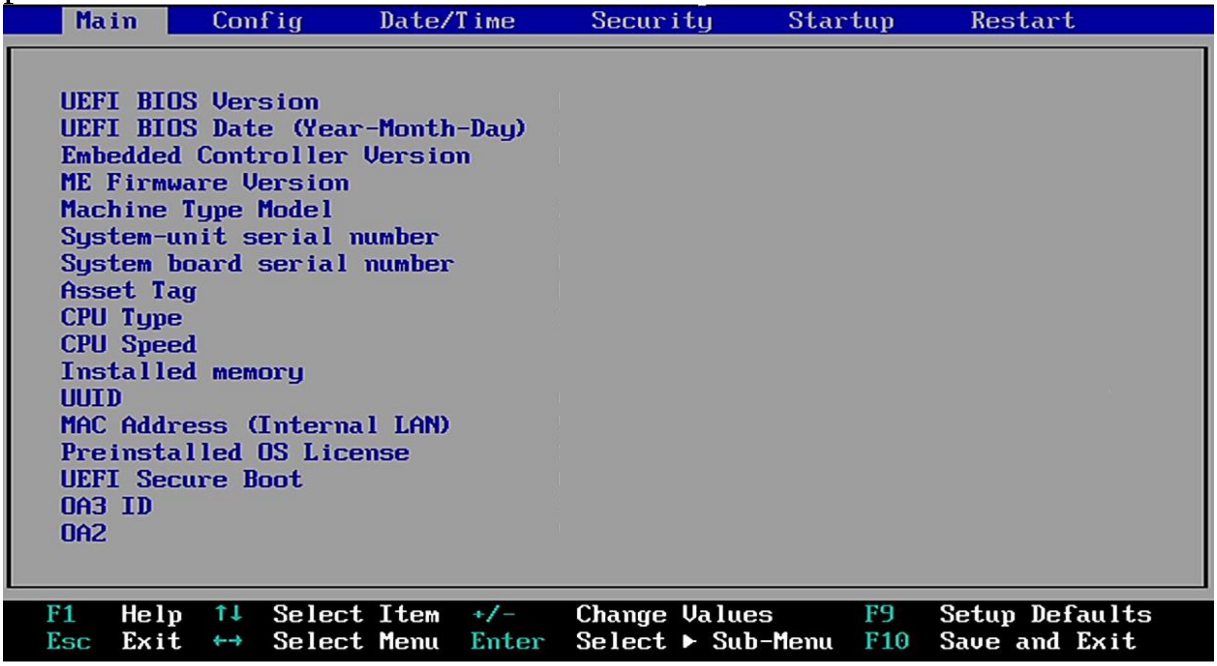
⚠ **BIOS settings are not password protected.**

3.0 CVSS

Physical

Description:

The basic system (BIOS) settings of the computer are not password protected.



```
   Main      Config        Date/Time      Security      Startup      Restart

  UEFI BIOS Version
  UEFI BIOS Date (Year-Month-Day)
  Embedded Controller Version
  ME Firmware Version
  Machine Type Model
  System-unit serial number
  System board serial number
  Asset Tag
  CPU Type
  CPU Speed
  Installed memory
  UUID
  MAC Address (Internal LAN)
  Preinstalled OS License
  UEFI Secure Boot
  OA3 ID
  OA2

 F1    Help   ↑↓  Select Item  +/-    Change Values       F9    Setup Defaults
 Esc   Exit   ↔   Select Menu  Enter  Select ► Sub-Menu   F10   Save and Exit
```

Risks:

- ⚠ **Disable security protocols.**
- ⚠ **Computer stability (system cooling and performance) can be tampered with, damaging the computer.**
- ⚠ **Tampering with computer settings and making it not work**

Solutions:

- **Lock BIOS with a Password**

Recommendations:

- ✓ **The password can only be known by the administrator IT.**

RECOMMENDATION : Necessary

Active Directory:

Description:

Active Directory is a directory service developed by Microsoft that functions as a centralized database to manage and organize network resources within a Windows domain environment. It provides a hierarchical structure for storing and managing information about network objects, such as user accounts, computers, groups, printers, and other network resources.

Advantages:

- Centralized Management of all devices in one operating system.
- Centralization of all data.
- Manage User authentication, permissions and group policy.
- Scalability.

Tasks:

I. Planning & Design Topology of Infrastructure.
II. Infrastructure Preparation.
III. Domain Controller Deployment.
IV. User and Group Migration.
V. Resource Integration.
VI. Testing, Validation and Documentation.

RECOMMENDATION : Necessary

Password:

Description:

Most of the weaknesses in the company are related to passwords, so the best solution is to follow the recommendations to create strong passwords:

Recommendation:

- Avoid Personal or Public Information About Company.
- Do not use any default or common password.
- Use a unique password for each of your accounts.
- using a passphrase instead of a single word.
- Avoid using simple patterns or sequences ("12345678" or "qwerty").
- Regularly Update Passwords for critical accounts.
- The password is known by the owner only, to avoid any attempt to evade responsibility in the event of an accident.
- Complexity:
  - Randomly mixing uppercase and lowercase letters, numbers, and special characters.
  - Incorporate substitutions and variations in your passwords:
    (a > @ … E > 3 … O > 0 … I > 1 … S > $)

RECOMMENDATION : Important

End Point Security:

Traditional antivirus software does not offer adequate protection against complex attacks.
Endpoint security providing comprehensive protection of all devices such as desktops, laptops, and mobile devices from internal/external sophisticated malware and evolving zero-day threats.

Backup Storage:

Backup storage serves as the ultimate solution when encountering any data-related issues. It is crucial to ensure that the stored data is well protected and kept separate from the Internet and the company's network. This is because many data-targeting attacks, such as ransomware, have the potential to spread rapidly throughout the entire network.

RECOMMENDATION : Good Addition

VLAN (Virtual Local Area Network) By logically segmenting a physical network into multiple virtual networks, VLANs provide flexibility, scalability and security as they isolate traffic and restrict access between different VLANs. also enable more efficient network management by allowing network administrators to control and prioritize traffic based on VLAN membership.

Identifying the problem is 50% of the solution,
and the other 50% is implementing the solution.

I have knowledge of both aspects.

Allow me to introduce an exclusive cybersecurity service aimed at Hardening your company's systems against potential cyber threats. Our comprehensive approach includes penetration testing to meticulously uncover and address vulnerabilities within your organization. Additionally, we offer the expertise of a dedicated Security Operations Center (SOC) Analyst to promptly respond to and mitigate any security incidents that may arise. Our commitment extends to a wide array of cybersecurity services beyond these, tailored to meet your specific needs and challenges.

I'm ready, just waiting for your call