



CYBERSECURITY

INTRODUCTION

Unauthorized server access can lead to:

- System exploration
- File manipulation
- Data theft
- Ransomware attacks
- Service disruption

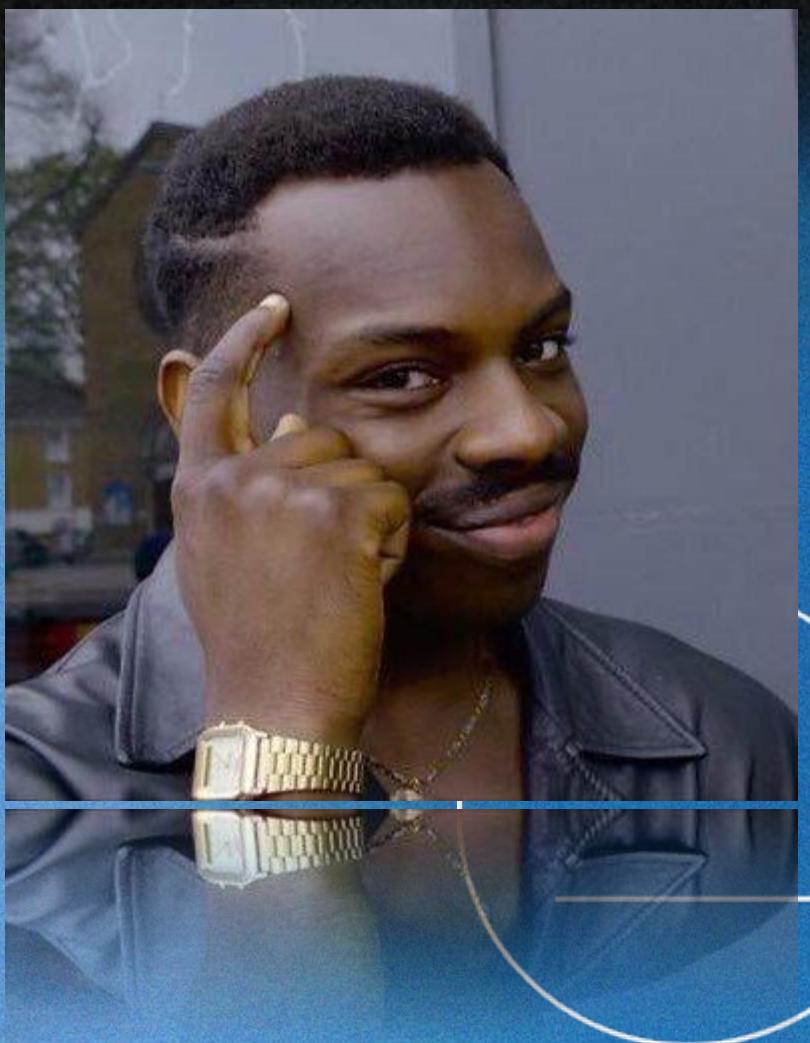
Consequences:

- Financial & reputational damage

Example:

- Marks & Spencer: £300M loss
- 7-week operational disruption





COMMON MINDSET

Common workplace mindset:

“It won’t happen to me — the world is too big.”



Reality:

Many still use weak passwords

People underestimate security risks

Belief leads to increased vulnerability

CYBER ATTACKERS



Cyber attackers are getting more sophisticated

We must adopt basic security practices (NIST & ISO 27001):

- Use strong, complex, unpredictable passwords
- Enable two-factor authentication (2FA)
- Keep systems & apps updated with latest patches

WHAT ACTUALLY HAPPENED?



Security assessment conducted on Debian WordPress server

Key finding:

Root login via SSH using a password

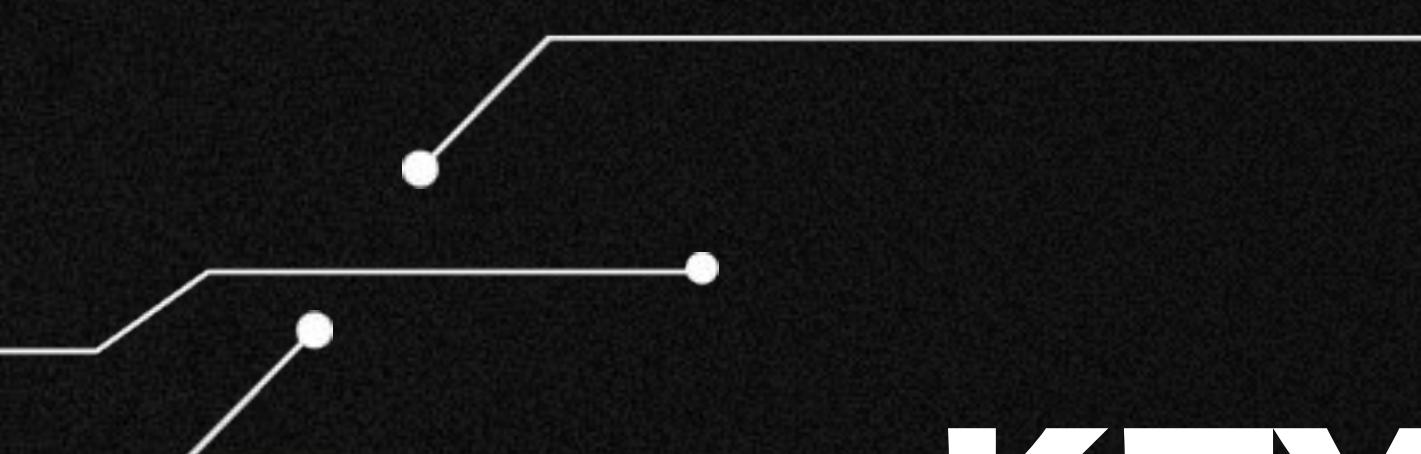
Source IP: 192.168.0.134

Conclusion:

Critical security gap

Required immediate action





KEY RESULTS



Security assessment results:

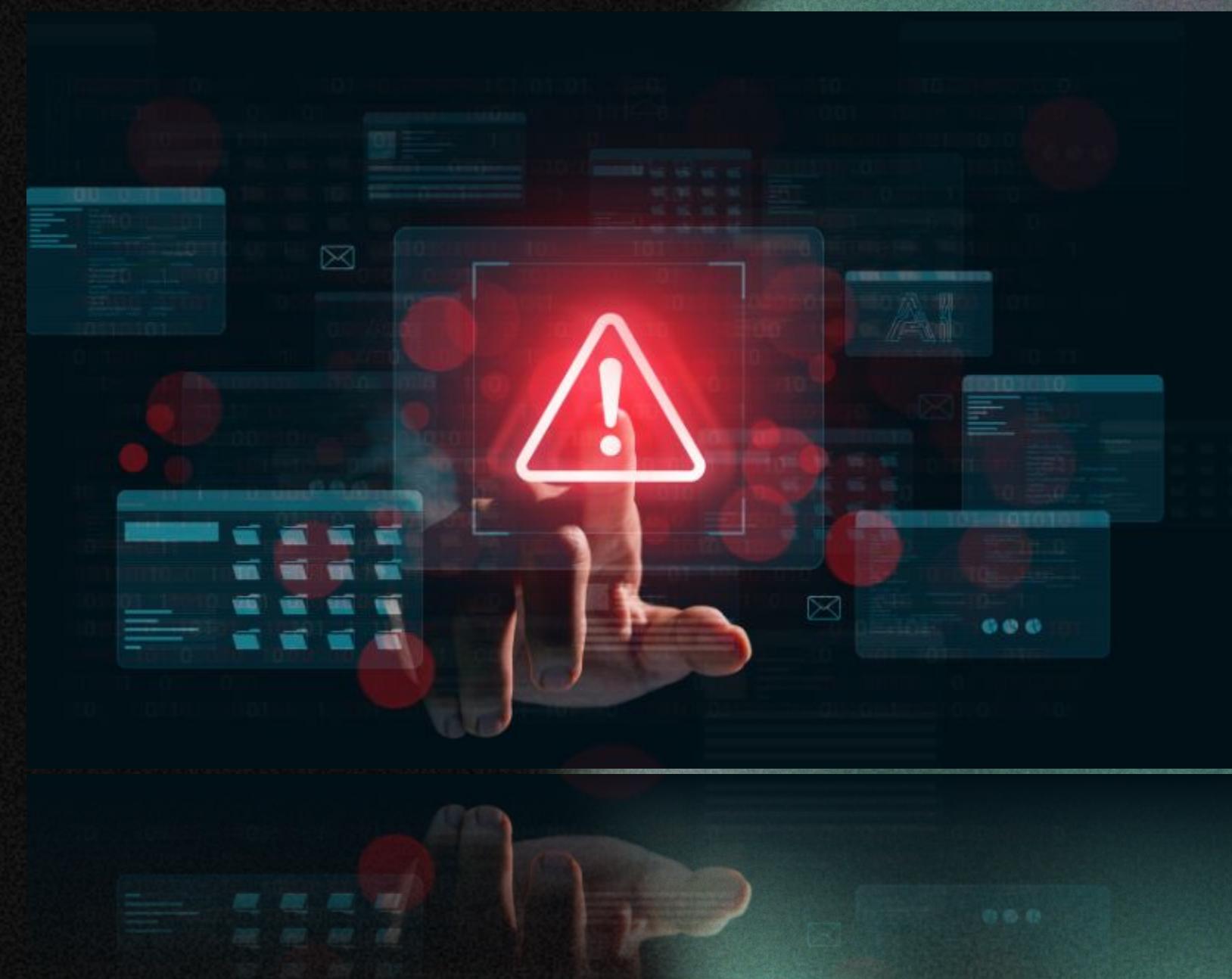
- 11 vulnerabilities found across critical systems
- 6 high-risk and 5 medium-risk issues
- All vulnerabilities successfully remediated



SECURITY ISSUES IDENTIFIED

6 High-Risk Vulnerabilities Identified:

-  Weak system passwords
-  WordPress admin weak credentials
-  Database weak passwords
-  SSH root access enabled
-  Insecure FTP service
-  Mail server weak password



SECURITY ISSUES IDENTIFIED

5 Medium-Risk Vulnerabilities Identified:

-  Untrusted SSL certificate
-  Outdated Intel Media SDK
-  WordPress security issues
-  Apache misconfigurations
-  Multiple vulnerabilities on port 80



IMPACT OF THE VULNERABILITIES FOUND



These weaknesses could have allowed attackers to take control of systems, steal sensitive data, or interrupt business activities.



Authentication & Access Control Improvements

- Replaced weak passwords
- Disabled SSH root login
- Created secure WordPress admin account
- Updated database passwords



```
debian@debian:~  
File Edit View Search Terminal Help  
debian@debian:~$ mysql -u root -p  
Enter password:  
Welcome to the MariaDB monitor. Commands end with ; or \g.  
Your MariaDB connection id is 5  
Server version: 10.11.11-MariaDB-0+deb12u1 Debian 12  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]> SELECT user, host, authentication_string FROM mysql.user;  
+-----+-----+-----+  
| User      | Host     | authentication_string |  
+-----+-----+-----+  
| mariadb.sys | localhost | *9169F93E9A567E622D2ED0A92E66E1386CC6CEE9 |  
| root       | localhost | *9BC1027E82A43E17500D9DEEB3583757DF489EAD |  
| mysql      | localhost | *5DF285B9FB938FDE524299514192AA3273C6E994 |  
| wordpressuser | localhost | *B0819EFB427A10FD0463B0961096B138B3539B73 |  
| user       | localhost | *A48EBA4E53215A0E640F90BB90C70DA9484E222F |  
+-----+-----+-----+  
5 rows in set (0.048 sec)  
  
MariaDB [(none)]>  
  
MariaDB [(none)]>  
2 rows in set (0.048 sec)  
+-----+-----+  
| user      | localhost | *55554846A01C006B80670430A51234A8E84A* |  
| wordpressuser | localhost | *3618B4361A75A0138B323B13 |  
+-----+-----+
```

Service Security Enhancements

-  Replaced insecure FTP
 -  Configured Apache security headers
 -  Updated WordPress core, plugins, and themes
 -  Removed unused Intel Media SDK



System Hardening Measures

-  Changed SSH port
-  Set connection limits & timeouts
-  Secured file permissions
-  Blocked access to sensitive config files



```
debian@debian:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         -----      ---
80/tcp                      ALLOW IN   Anywhere
443/tcp                     ALLOW IN   Anywhere
Anywhere                   DENY IN    192.168.0.134      # Blocked root
SSH login
80/tcp (v6)                 ALLOW IN   Anywhere (v6)
443/tcp (v6)                ALLOW IN   Anywhere (v6)

debian@debian:~$
```



BUSINESS IMPACT

- Strengthened database security
- Hardened WordPress
- Blocked unauthorized access
- Secured communications



-  Security level improved
-  100% remediation
-  Proactive measures





TOOLS AND TECHNOLOGIES USED IN THE ANALYSIS



Exterro FTK Imager	[1] For creating forensic disk images.
Autopsy	[2] For digital forensic investigation and analysis.
Kali Linux	[3] Is a security testing platform.
Nmap	[4] For network discovery and vulnerability scanning.
Rootkit Hunter	[5] To detect rootkits, backdoors, and local exploits.
Hashcat	[6] For password recovery and strength testing.
Nessus Essentials	[7] For identifying and assessing system vulnerabilities.

CHALLENGES

- 🔥 Project was challenging at first
- 🤔 Initial thought: “I can't do it.”
- 📚 Daily research and persistence led to success
- ✓ Eventually found the solution





WHY CHOOSE A CAREER IN CYBER SECURITY ?

- 📈 3.5 million cybersecurity jobs unfilled worldwide (2023)
- 🚀 Work with cutting-edge technologies
- 🛡️ Protect organizations from cyber threats
- 🎯 Offers diverse career paths, strong job security & growth





THANK YOU!