https://hackcontrol.org/
Write to our email info@hackcontrol.org



# INTERNAL NETWORK PENETRATION TESTING

| | |
|---|---|
| **Report for:** | |
| **Date:** | |

# Table of Contents

# Executive Summary

Hack Control (Provider) was contracted by ____ (Client) to conduct the penetration testing of their internal network.

This report presents the findings of the security assessment of CLIENT`s network conducted between February 04th, 2018 – February 22nd, 2018.

The main subject of the security assessment is the CLIENT`s internal network.

Penetration test has the following objectives:

- identify technical and functional vulnerabilities;
- estimate their severity level (ease of use, impact on information systems, etc.)
- draw up a prioritized list of recommendations to address identified weaknesses.

According to our research after performing the penetration testing, security rating of CLIENT`s infrastructure was identified as **Medium**.

## Team

| Role | Name | EMAIL |
|---|---|---|
| Project Manager | John Johnson<br>(CEH, ISO27001 LA) | info@protectmaster.com |
| Penetration Testing Engineer | David Brown<br>(OSCP, eWPT, eCPPT) | engineer@protectmaster.org |

## Scope of Security Assessment

The testing area includes all client's systems located in the company's office.

Network segments, which are the entry point during testing, were agreed with the client. Based on existing documentation, the following network segments were selected: CLIENT11, CLIENT11, CLIENT11. During testing, an extension of the list of tested networks was agreed with the client and the following were added to it: CLIENT11, CLIENT11, CLIENT11. Wired and wireless Wi-Fi connection can be used to connect to the network (SSIDs correspond to the names of the segments).

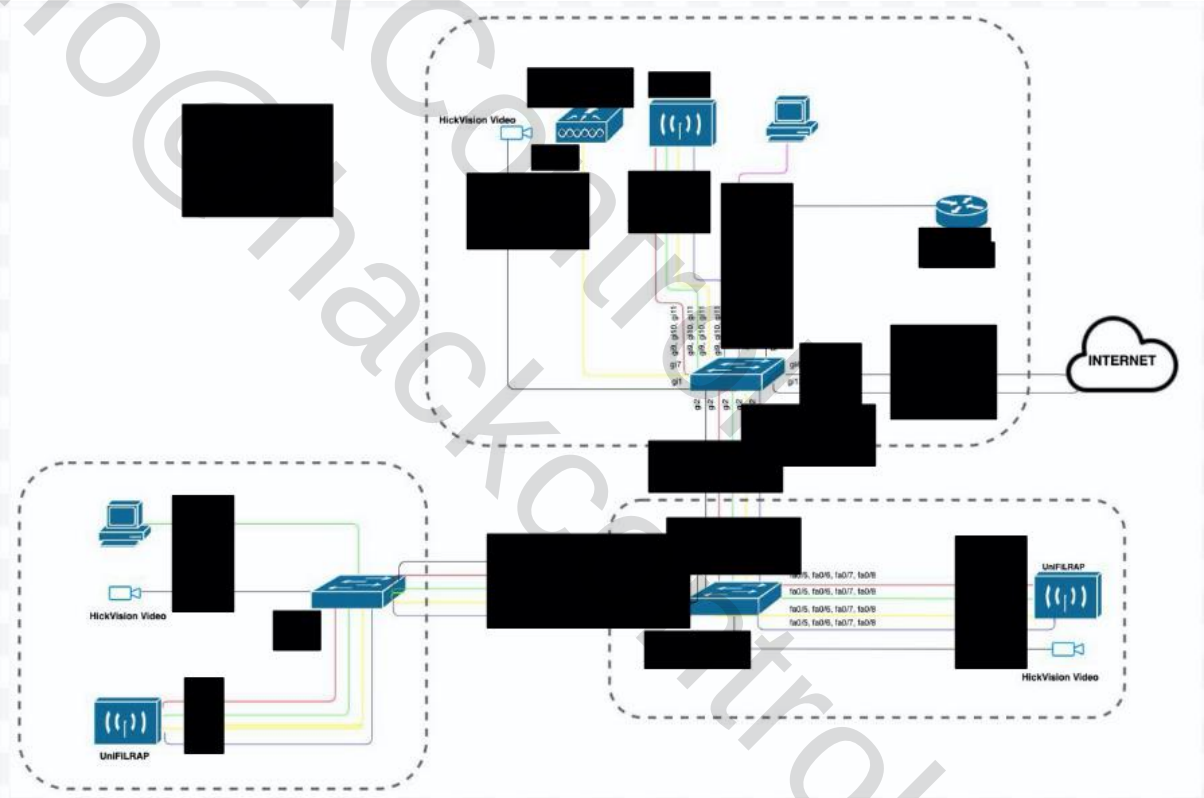



Figure 1 - Network diagram (provided by the client)

Table 1 - Subnet IP addresses (provided by the client)

| | |
|---|---|
| vlan000 | 192.168.0.0 |
| vlan000 | 192.168.0.0 |
| vlan000 | 10.8.0.0 |
| vlan000 | 192.168.0.0 |
| vlan000 | 10.254.0.0 |
| vlan000 | 192.168.0.0 |
| vlan000 | 10.6.0.0 |

The network diagram and IP address table may differ from the actual network.

## Methodology

The testing methodology is based on generally accepted industry-wide approaches to perform penetration testing for internal networks (NIST SP800-115, PTES, PCI Penetration Test Guidance).

Penetration tests include, at a minimum, checking for the following types of vulnerabilities:

- known vulnerabilities in operating systems and network components;
- using of insecure services;
- using of defaults credentials;
- vulnerable to MiTM components;
- testing to verify the effectiveness of segmentation tools;
- testing of Wi-Fi network vulnerabilities.

## Severity Definition

The level of criticality of each risk is determined based on the potential impact of loss from successful exploitation as well as ease of exploitation, existence of exploits in public access and other factors.

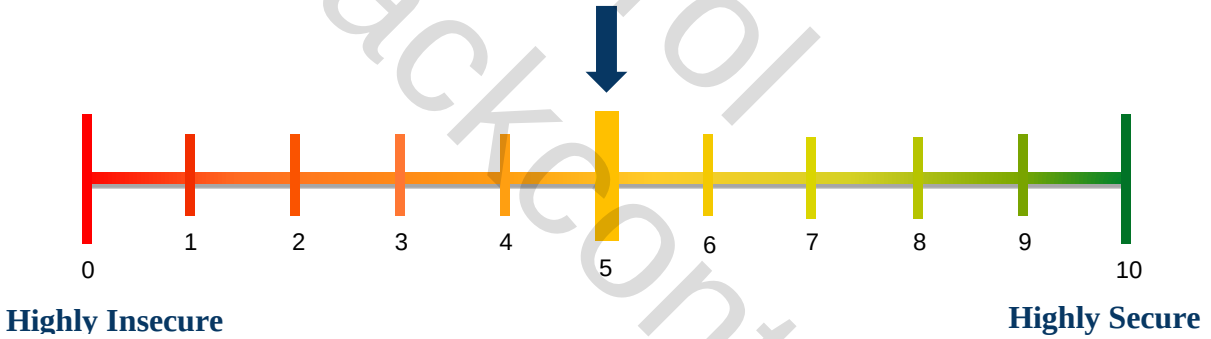
| Severity | Description |
|---|---|
| High | High-level vulnerabilities are easy in exploitation and may provide an attacker with full control of the affected systems, also may lead to significant data loss or downtime. There are exploits or PoC available in public access. |
| Medium | Medium-level vulnerabilities are much harder to exploit and may not provide the same access to affected systems. No exploits or PoCs available in public access. Exploitation provides only very limited access. |
| Low | Low-level vulnerabilities provide an attacker with information that may assist them in conducting subsequent attacks against target information systems or against other information systems, which belong to an organization. Exploitation is extremely difficult, or impact is minimal. |
| Info | These vulnerabilities are informational and can be ignored. |

## Summary of Findings

According to the following in-depth testing of the environment, the CLIENT's infrastructure requires some improvements.

| Value | Number of risks |
|---|---|
| High | 6 |
| Medium | 1 |
| Low | 5 |
| Info | 8 |

Based on our understanding of the IT Infrastructure, as well as the nature of the vulnerabilities discovered, their exploitability, and the potential impact we have assessed the level of risk for your organization to be Medium.



| Risk level | Vulnerabilities | Affected system | Recommendations |
|---|---|---|---|
| High | Possibility of MITM attack | All VLAN | Use VPN and AV with arp-spoofing protection functionality |
| High | Usage of Telnet Protocol | [redacted] | Replace Telnet with SSH |
| High | Standard password for network equipment | [redacted] | Change username and password |
| High | Vulnerable to Eternal Blue attack | [redacted] | Install security updates |
| High | SNMP Agent uses standard network names | [redacted] | Change the default network name and enable request filtering |
| High | Unencrypted transmission of information over HTTP | [redacted] | Use HTTPS or SSH |
| Medium | Usage of weak login credentials to access the database | [redacted] | Change username and password. Enable Firewall for Developers' PCs |
| Low | Use of vulnerable versions of Oracle MySQL | [redacted] | Upgrade all versions to Oracle MySQL 5.7.29 or later. Enable Firewall for developers' PCs. |
| Low | No valid certificate | [redacted] | Install a valid certificate |
| **Risk level** | **Vulnerabilities** | **Affected system** | **Recommendations** |

| | | | |
|---|---|---|---|
| Low | SSL / TLS service uses Diffie-Hellman groups with insufficient key length | [redacted] | Use a key length of 2048 bits or use ECDHE |
| Low | SSH Server is configured to use weak encryption algorithms | [redacted] | Use strong encryption algorithms |
| Low | No brute force protection on SSH | [redacted] | Set brute force password protection |
| Info | Possibility of data exchange between clients of the guest network | [redacted] | Disable the Client To Client Forwarding parameter in vlan23 |
| Info | User password calculation vulnerability | [redacted] | Make sure that the latest software version is used |
| Info | Remote code execution vulnerability | [redacted] | Make sure that the latest software version is used |
| Info | Timestamps enabled in TCP packets | [redacted] | Disable TCP timestamps |
| Info | Weak MAC algorithms are used | [redacted] | Disable weak MAC algorithms |
| Info | Same passwords for Office (network10) and Management (network12) | [redacted] | Change password for the network Management (network12) |
| **Risk level** | **Vulnerabilities** | **Affected system** | **Recommendations** |
| Info | Successful interception of handshake from networks: “network101”, “network10” | [redacted] | Use WPA2 Enterprise |
| Info | Fake access point creation | | Integrate WIPS |

# Key Findings

## Possibility of MITM attack (Man in the middle)

| #1 | Description |
|---|---|

MITM (man in the middle) - is a method of compromising a communication channel in which an attacker, having connected to the channel between contractors, interferes in the transmission protocol, deleting or distorting information.

### Evidence

| Client | Server | Protocol | Username | Password | Valid login | Login timestamp |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | HTTP | [redacted] | N/A | Unknown | 2020-01-31 23:42:45 UTC |
| | | SNMPv1 | | public | Unknown | 2020-01-31 23:59:54 UTC |

```
0 hosts [redacted]
DHCP:

ARP poisoning victims:

GROUP 1 : ANY (all the hosts in the list)

GROUP 2 : ANY (all the hosts in the list)
HTTP : 10.8.15.200:80 -> USER: [redacted]
HTTP : 10.8.15.200:80 -> USER:
HTTP : 10.8.15.200:80 -> USER:
```

### Recommendations

- Use VPN and AV with arp-spoofing protection functionality

## Usage of the vulnerable Telnet Protocol

| #2 | Description |
|---|---|

The Telnet service is launched on the remote host, which transmits the username and password in unencrypted form. An attacker could reveal login names and passwords by listening to traffic in the Telnet service.

### Evidence

Location:
vlan128 -> ipv4:10.6.15.1, ma[redacted] (Cisco Systems)
vlan23 -> ipv4:10.8.15.1, mac[redacted] (Cisco Systems)

**Result: Telnet Unencrypted Cleartext Login**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| Telnet Unencrypted Cleartext Login | 4.8 (Medium) | 70% | [redacted] | 23/tcp (IANA: telnet) | |

**Summary**
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

**Solution**
**Solution type:** Mitigation

Replace Telnet with a protocol like SSH which supports encrypted connections.

**Vulnerability Detection Method**
Details: Telnet Unencrypted Cleartext Login [redacted]

Version used: 2019-06-06T07:39:31+0000

### Recommendations

- Replace Telnet with SSH, which supports encrypted connections.

## Standard password for network equipment

| #3 | Description |
|---|---|

Standard username/password combination for users

### Evidence

Location: vlan23 -> ipv4: [redacted], mac: [redacted] (Cisco Systems)

**Result: HTTP Brute Force Logins With Default Credentials Reporting**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| HTTP Brute Force Logins With Default Credentials Reporting | 9.0 (High) | 95% | [redacted] | 80/tcp | |

**Summary**
It was possible to login into the remote Web Application using default credentials.

As the NVT 'HTTP Brute Force Logins with default Credentials' (OID: [redacted]1) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

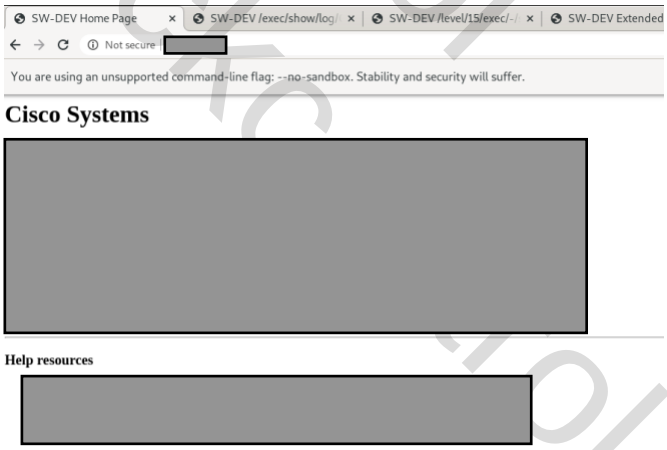
**Vulnerability Detection Result**

```
It was possible to login with the following credentials <Url>:<User>:<Password>:<HTTP status code>

http://[redacted] 200 OK
http://[redacted] 200 OK
```

**Solution**
**Solution type:** Mitigation

Change the password as soon as possible.




### Recommendations

- Change username and password to non-standard, according to a high level of security

## Vulnerable to RCE Attack, MS17-010

| #4 | Description |
|---|---|

Remote Code Execution Vulnerabilities exist in the Microsoft Server 1.0 Message Block (SMBv1) due to improper processing of certain requests. An unauthenticated remote attacker could exploit these vulnerabilities using a specially created package to execute arbitrary code and subsequently disclose confidential information. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

### Evidence

Location: vlan21 -> ipv4: [redacted], mac: [redacted] (Chicony Electronics)

```
       =[ metasploit v5.0.70-dev                          ]
+ -- --=[ 1960 exploits - 1094 auxiliary - 336 post        ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops             ]
+ -- --=[ 7 evasion                                        ]

msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts [redacted]
rhosts => [redacted]
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] [redacted]  - Host is likely VULNERABLE to MS17-010! - Windows 7 U
ltimate 7601 Service Pack 1 x64 (64-bit)
[*] [redacted]  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

Links:
https://technet.microsoft.com/en-us/library/security/MS17-010
https://github.com/worawit/MS17-010

### Recommendations

- Install security updates

## SNMP Agent uses standard network names

| #5 | Description |
|---|---|

Possibility to get the default network name for the remote SNMP server. An attacker can use this information to gain more knowledge about the remote host or to reconfigure the remote system.

### Evidence

Location: vlan23 -> ipv[redacted], mac:[redacted] (D-Link International)

```
era@kali:~$ sudo snmpwalk -v 2c -c private [redacted]
iso.3.6.1.2.1.1.1.0 = STRING: "D-Link DES-3028 Fast Ethernet Switch"
iso.3.6.1.2.1.1.2.0 = OID: [redacted]
iso.3.6.1.2.1.1.3.0 = Timeticks: (178473982) 20 days, 15:45:39.82
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 3
iso.3.6.1.2.1.1.8.0 = Timeticks: (178473986) 20 days, 15:45:39.86
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.0
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.0
```

```
era@kali:~$ sudo snmpwalk -v 2c -c public [redacted]
iso.3.6.1.2.1.1.1.0 = STRING: "D-Link DES-3028 Fast Ethernet Switch"
iso.3.6.1.2.1.1.2.0 = OID: [redacted]
iso.3.6.1.2.1.1.3.0 = Timeticks: (178480133) 20 days, 15:46:41.33
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = ""
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 3
iso.3.6.1.2.1.1.8.0 = Timeticks: (178480137) 20 days, 15:46:41.37
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.0
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.0
```

CVE: CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-1999-0792, CVE-2000-0147, CVE-2001-0380, CVE-2001-0514, CVE-2001-1210, CVE-2002-0109, CVE-2002-0478, CVE-2002-1229, CVE-2004-1474, CVE-2004-1775, CVE-2004-1776, CVE-2011-0890, CVE-2012-4964, CVE-2014-4862, CVE-2014-4863, CVE-2016-1452, CVE-2016-5645, CVE-2017-7922.

### Recommendations

- Change the default network names and filter incoming UDP packets going to this port

## Unencrypted transmission over HTTP

| #6 | Description |
|---|---|

An attacker could use this situation to compromise or eavesdrop on an HTTP connection between a client and server using the man in the middle attack to gain access to sensitive data, such as usernames or passwords

### Evidence

Location:
vlan23 -> ipv4: [redacted] mac: [redacted] 1 (Cisco Systems)
vlan23 -> ipv4: [redacted] mac: [redacted] (Cisco Systems)
vlan23 -> ipv4: [redacted] 0, mac: [redacted] (D-Link)
vlan23 -> ipv4: [redacted] 1, mac: [redacted] (DrayTek)

**Result: Cleartext Transmission of Sensitive Information via HTTP**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| Cleartext Transmission of Sensitive Information via HTTP | 4.8 (Medium) | 80% | [redacted] | 80/tcp | |

**Summary**
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

**Vulnerability Detection Result**

```
The following URLs requires Basic Authentication (URL:realm name):

http://10.8.15.4/:"level 15 access"
```

**Links:**
https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

### Recommendations

- Use encrypted HTTPS traffic or use SSH

## Usage of weak login credentials to access the DB

| #7 | Description |
|---|---|

We managed to login as root with the password "123456".

### Evidence

Location: vlan21 -> ipv4: [redacted], mac: [redacted] (Apple)

```
root@kali:~# mysql -h [redacted] -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1867
Server version: 5.7.28 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> exit
Bye
root@kali:~#
```

### Recommendations

- Set a non-standard username and change password to a more strong one
- Enable Firewall for Developers' PCs

## Using vulnerable versions of Oracle MySQL

| #8 | Description |
|---|---|

Links:
https://www.oracle.com/security-alerts/cpuapr2019.html#AppendixMSQL
https://www.oracle.com/security-alerts/cpujul2019.html#AppendixMSQL
https://www.oracle.com/security-alerts/cpuoct2019.html#AppendixMSQL
https://www.oracle.com/security-alerts/cpujan2020.html#AppendixMSQL

### Evidence

Location:
vlan21->ipv4: [redacted] mac: [redacted] (MySQL 5.7.26)
vlan21->ipv4: [redacted] mac:3[redacted] (MySQL 5.7.25)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.25)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.27)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.26)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.28)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.28)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.24)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.26)
vlan21->ipv4: [redacted], mac: [redacted] (MySQL 5.7.28)

**Result: Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.16 Security Update (2019-5072835) - Windows**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| Oracle MySQL 5.7.x < 5.7.27, 8.0.x < 8.0.16 Security Update (2019-5072835) - Windows | 7.5 (High) | 80% | [redacted] | 3306/tcp | |

**Summary**
Oracle MySQL is prone to multiple vulnerabilities in libcurl.

**Vulnerability Detection Result**

Installed version: [redacted]
Fixed version:
Installation path / port:

**Result: Oracle MySQL 5.7.x < 5.7.29 Security Update (cpujan2020) - Windows**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| Oracle MySQL 5.7.x < 5.7.29 Security Update (cpujan2020) - Windows | 4.0 (Medium) | 80% | [redacted] | 3306/tcp | |

**Summary**
Oracle MySQL is prone to multiple vulnerabilities.

**Vulnerability Detection Result**

Installed version: [redacted]
Fixed version:
Installation path / port:

For MySQL 5.7.0 - 5.7.25: CVE-2019-2581, CVE-2019-2628, CVE-2019-2566, CVE-2019-2592, CVE-2019-2632, CVE-2019-1559, CVE-2019-2683, CVE-2019-2627, CVE-2019-2614.
For MySQL 5.7.0 - 5.7.26: CVE-2019-2758, CVE-2019-2778, CVE-2019-2741, CVE-2019-2757, CVE-2019-2774, CVE-2019-2797, CVE-2019-2791, CVE-2019-3822, CVE-2018-16890, CVE-2019-3823, CVE-2019-2805, CVE-2019-2740, CVE-2019-2819, CVE-2019-2739, CVE-2019-2737, CVE-2019-2738, CVE-2019-2758, CVE-2019-2778, CVE-2019-2741, CVE-2019-2757, CVE-2019-2774, CVE-2019-2797, CVE-2019-2791, CVE-2019-2946, CVE-2019-2914, CVE-2019-2993, CVE-2019-2960, CVE-2019-2938, CVE-2019-5443, CVE-2019-5435, CVE-2019-5436.
For MySQL 5.7.0 - 5.7.27: CVE-2019-2922, CVE-2019-2923, CVE-2019-2924, CVE-2019-2910, CVE-2019-2946, CVE-2019-2914, CVE-2019-2993, CVE-2019-2960, CVE-2019-2938, CVE-2019-5443, CVE-2019-5435, CVE-2019-5436.
For MySQL 5.7.0 - 5.7.28: CVE-2020-2579, CVE-2020-2577, CVE-2020-2589, CVE-2020-2660, CVE-2020-2584, CVE-2020-2572.

**Recommendations**

- Upgrade all versions to Oracle MySQL 5.7.29 or later.
- Enable Firewall for developers' PCs

## No valid certificate

| #9 | Description |
|---|---|

The certificate has expired.

### Evidence

Location: vlan23 -> ipv4:[redacted], mac:[redacted] (Ubiquiti Networks)
vlan21 -> ipv4:[redacted], mac:[redacted](Apple)

**Result: SSL/TLS: Certificate Expired**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| SSL/TLS: Certificate Expired | 5.0 (Medium) | 99% | [redacted] | 443/tcp | |

**Summary**
The remote server's SSL/TLS certificate has already expired.

**Vulnerability Detection Result**

```
The certificate of the remote service expired on 2020-01-02 00:03:10.

Certificate details:
subject ...: L=San Jose,ST=CA,C=US
subject alternative names (SAN):
None
issued by .: L=San Jose,ST=CA,C=US
serial ....: [redacted]
valid from : 2010-01-01 00:03:10 UTC
valid until: 2020-01-02 00:03:10 UTC
fingerprint (SHA-1): 8[redacted]
fingerprint (SHA-256):[redacted]
```

### Recommendations

- Install a valid certificate

## SSL/TLS service uses with insufficient key lengths

| #10 | Description |
|---|---|

SSL/TLS service uses Diffie-Hellman groups with insufficient key lengths <2048.
The Diffie-Hellman (DH) Group is several large numbers that are used as the basis for DH calculations. The security of the final secret depends on the size of these parameters. It turned out that 512 and 768 bits are weak, and 1024 bits are strong enough from ordinary hackers, but vulnerable to attackers with very powerful equipment.

### Evidence

Location:
vlan23 -> ipv4: [redacted] mac: [redacted] (Ubiquiti Networks)
vlan21 -> ipv4: [redacted]8, mac: [redacted] (Apple)

**Result: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability**

| Vulnerability | | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|---|
| SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability | | 4.0 (Medium) | 80% | [redacted] | 443/tcp | |

**Summary**
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

**Vulnerability Detection Result**

```
Server Temporary Key Size: 1024 bits
```

Links:
https://weakdh.org/
https://weakdh.org/sysadmin.html

### Recommendations

- Use a key with a length of 2048 bits or more, or use Diffie-Hellman on elliptic curves (ECDHE)

## SSH Server use weak encryption algorithms

| #11 | Description |
|---|---|

SSH Server is configured to use weak encryption algorithms.
The following weak encryption algorithms are supported by the remote service: 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, arcfour, blowfish-cbc, cast128-cbc, twofish-cbc, twofish128-cbc, twofish192-cbc, twofish256-cbc.

### Evidence

Location: vlan23 -> ipv4:[redacted], mac:[redacted] (D-Link International)
Arcfour (and RC4) has problems with weak key and should no longer be used.

**Result: SSH Weak Encryption Algorithms Supported**

| Vulnerability | | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|---|
| SSH Weak Encryption Algorithms Supported | | 4.3 (Medium) | 95% | [redacted] | 22/tcp | |

**Summary**
The remote SSH server is configured to allow weak encryption algorithms.

**Vulnerability Detection Result**

```
The following weak client-to-server encryption algorithms are supported by the remote
service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
blowfish-cbc
cast128-cbc
twofish-cbc
twofish128-cbc
twofish192-cbc
twofish256-cbc
```

Links:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

### Recommendations

- Use strong encryption algorithms

## No brute force protection on SSH

| #12 | Description |
|---|---|

No brute force protection on SSH

### Evidence

Location: 000.000.000.000, 1[redacted]

```
root@kali: ~
root@kali:~# medusa -h [redacted] -u test -P /root/Desktop/8-mo
re-passwords.txt -M ssh -f -v 6
Medusa v2.2 [http://[redacted] (C) JoMo-Kun / Foofus Networks <j
mk@foofus.net>

GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 1
GENERAL: Total Passwords: 61682
ACCOUNT CHECK: [ssh] Host: [redacted] (1 of 1, 0 complete) User:
 test (1 of 1, 0 complete) Password: [redacted] (1 of 61682 complete)
ACCOUNT CHECK: [ssh] Host: [redacted] (1 of 1, 0 complete) User:
```

```
root@kali: ~
 test (1 of 1, 0 complete) Password: [redacted] (112 of 61682 complete)
ACCOUNT CHECK: [ssh] Host: [redacted] (1 of 1, 0 complete) User:
 test (1 of 1, 0 complete) Password: [redacted] (113 of 61682 complete)
ACCOUNT CHECK: [ssh] Host: [redacted] (1 of 1, 0 complete) User:
 test (1 of 1, 0 complete) Password: [redacted] (114 of 61682 complete)
```

### Recommendations

- Set brute force password protection

## Data exchange between clients of the guest network

| #13 | Description |
|---|---|

Possibility of data exchange between clients of the guest network

### Evidence

Location: vlan23 -> ipv4:[redacted], SSID: network101

```
root@kali:~# ping [redacted]
PING [redacted] 56(84) bytes of data.
64 bytes from [redacted]: icmp_seq=1 ttl=255 time=188 ms
64 bytes from [redacted]: icmp_seq=2 ttl=255 time=160 ms
^C
--- [redacted] ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 160.071/174.265/188.460/14.194 ms
root@kali:~# ping [redacted]
PING [redacted] 56(84) bytes of data.
64 bytes from [redacted]: icmp_seq=1 ttl=128 time=44.6 ms
64 bytes from [redacted]: icmp_seq=2 ttl=128 time=66.9 ms
^C
--- [redacted] ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 44.588/55.741/66.894/11.153 ms
```

### Recommendations

- Disable the Client To Client Forwarding parameter in vlan23

## User password extracting vulnerability

| #14 | Description |
|---|---|

A potential vulnerability allows extracting the cookie value and use it to extract the password from the router.

### Evidence

Location: vlan23 -> ipv4:[redacted], mac:[redacted](D-Link International)

```
root@kali: ~
root@kali: ~    root@kali: ~

 - 10.8.15.200:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
 - 10.8.15.200:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
 - 10.8.15.200:80 http exploits/routers/cisco/secure_acs_bypass

[+] 10.8.15.200 Device is vulnerable:

   Target        Port     Service     Exploit

   ------        ----     -------     -------

   [redacted]    80       http        exploits/routers/dlink/dwl_3200ap_password_disclosure


[-] 10.8.15.200 Could not find default credentials
rsf (AutoPwn) > use exploits/routers/dlink/dwl_3200ap_password_disclosure
rsf (D-Link DWL-3200AP Password Disclosure) > set target [redacted]
[+] target => [redacted]
rsf (D-Link DWL-3200AP Password Disclosure) > run
[*] Running module exploits/routers/dlink/dwl_3200ap_password_disclosure...
[*] Attempting to get cookie...
[+] Cookie retrieved: 00137ed4
[*] Starting bruteforcing cookie value...
```

Links:
https://www.exploit-db.com/exploits/34206

### Recommendations

- Make sure that the latest software version is used

## Remote code execution vulnerability

| #15 | Description |
|---|---|

The ubiquitin controller is potentially vulnerable to an injection of an OS command without authorization.

### Evidence

Location: vlan23 -> ipv4:[redacted], mac:[redacted] (Ubiquiti Networks)

```
root@kali: ~
root@kali: ~

[*] 10.8.15.10 Could not verify exploitability:
 - 10.8.15.10:80 http exploits/routers/shuttle/915wm_dns_change
 - 10.8.15.10:80 http exploits/routers/3com/officeconnect_rce
 - 10.8.15.10:80 http exploits/routers/dlink/dsl_2730b_2780b_526b_dns_change
 - 10.8.15.10:80 http exploits/routers/dlink/dsl_2640b_dns_change
 - 10.8.15.10:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce
 - 10.8.15.10:80 http exploits/routers/dlink/dsl_2740r_dns_change
 - 10.8.15.10:80 http exploits/routers/billion/billion_5200w_rce
 - 10.8.15.10:80 http exploits/routers/asus/asuswrt_lan_rce
 - 10.8.15.10:80 http exploits/routers/netgear/dgn2200_dnslookup_cgi_rce
 - 10.8.15.10:23 custom/tcp exploits/routers/cisco/catalyst_2960_rocem
 - 10.8.15.10:80 http exploits/routers/cisco/secure_acs_bypass

[+] 10.8.15.10 Device is vulnerable:

   Target         Port     Service     Exploit
   ------         ----     -------     -------
   10.8.15.10     80       http        exploits/routers/linksys/eseries_themoon_rce


[-] 10.8.15.10 Could not find default credentials
rsf (AutoPwn) > back
rsf > use exploits/routers/linksys/eseries_themoon_rce
```

Links:
https://www.rapid7.com/db/modules/exploit/linux/http/linksys_themoon_exec

### Recommendations

- Make sure that the latest software version is used

## Timestamps enabled in TCP packets

| #16 | Description |
|---|---|

The remote host uses TCP timestamps and, therefore, makes it possible to calculate the uptime of the device.

### Evidence

Location:
vlan23->ipv4: [redacted] mac: [redacted] (Cisco Systems)
vlan23->ipv4: [redacted], mac: [redacted] (Ubiquiti)
vlan23->ipv4: [redacted]-21, *.108 (Ubiquiti APs)
vlan23->ipv4: [redacted]0, mac: [redacted] (D-Link)
vlan23->ipv4: [redacted]1, mac: [redacted] (DrayTek)

**Result: TCP timestamps**

ID: [redacted]
Created: Wed Jan 29 01:06:50 2020
Modified: Wed Jan 29 01:06:50 2020
Owner: admin

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| TCP timestamps | 2.6 (Low) | 80% | [redacted] | general/tcp | |

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Vulnerability Detection Result**

```
It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 302510879
Packet 2: 302510990
```

### Recommendations

- Disable TCP timestamps

## Weak MAC algorithms are used

| #17 | Description |
|---|---|

The following weak client-server MAC algorithms are supported by the remote service: HMAC-md5, HMAC-MD5-96, HMAC-SHA1-96.

### Evidence

Location:
vlan23 -> ipv4: [redacted], mac: [redacted] (D-Link International)

**Result: SSH Weak MAC Algorithms Supported**

| Vulnerability | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|
| SSH Weak MAC Algorithms Supported | 2.6 (Low) | 95% | [redacted] | 22/tcp | |

**Summary**
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

**Vulnerability Detection Result**

```
The following weak client-to-server MAC algorithms are supported by the remote service:

hmac-md5
hmac-md5-96
hmac-sha1-96
```

Links:
https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

### Recommendations

- Disable weak MAC algorithms

## Same passwords for Office and Management networks

| #18 | Description |
|---|---|

Same passwords for Office and Management networks

### Evidence

Office and Management passwords

### Recommendations

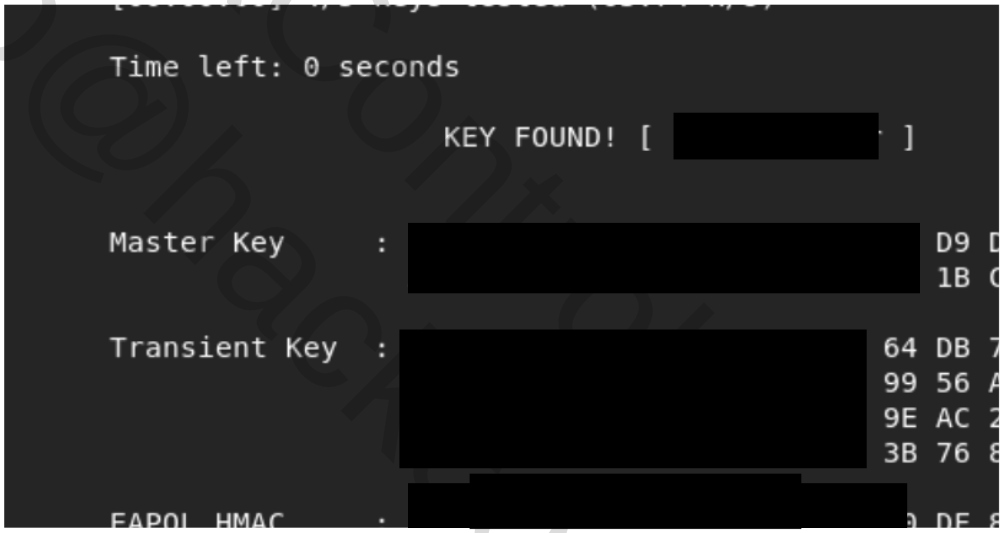
- Change password for the network Management (network12)

## Successful interception of handshake from networks

| #19 | Description |
|---|---|

Successful interception of handshake from networks: “network101”, “network10”

**Evidence**





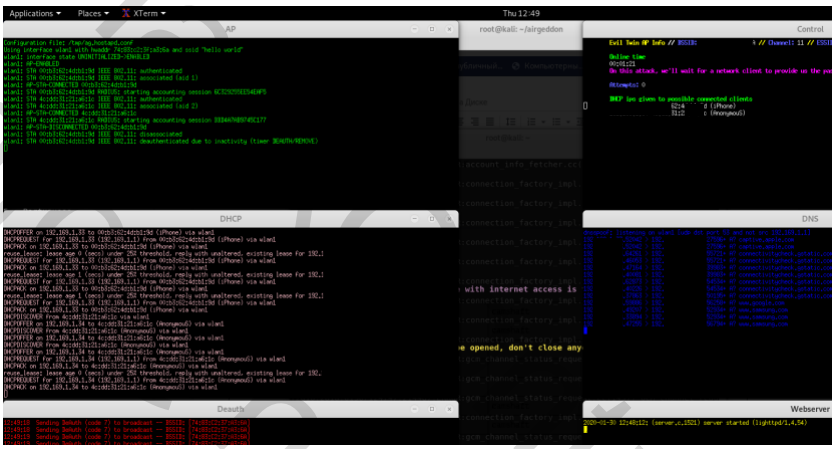
**Recommendations**

- Use WPA2 Enterprise

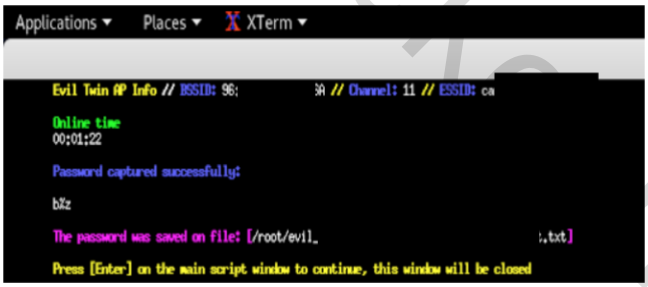
## Fake access point creation

| #20 | Description |
|---|---|
| A fake access point has been created, the process of intercepting clients to obtain a password from wifi network. | |

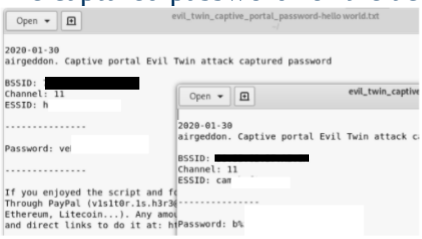
### Evidence



Fake access point creation.
A fake access point has been created, the process of intercepting clients to obtain a password from wifi network.




The captured password for the access point using the user interception method.




Finally intercepted passwords.

| Recommendations | Integrate: |
|---|---|

| | |
|---|---|
| | https://www.watchguard.com/wgrd-products/access-points/wips |

## Appendix A. Services and Open Network Ports

At the time of testing, the following services were available in the WAN:

| IP Address | Description | Open Ports | Status | Services | Version |
|---|---|---|---|---|---|
| 000.000.000.000 | WAN-port Cisco | 22/tcp | open | ssh | Cisco SSH 1.25 |
| | | 23/tcp | open | telnet | Cisco IOS telnet |
| | | 2001/tcp | open | telnet | Cisco router telnetd |
| | | 4001/tcp | open | tcpwrapped | |

Identified services and open network ports in landscape orientation here.

## Appendix B. WiFi Testing

| SSID | MAC Address | WPA/WPA2 | WPS | Vendor |
|---|---|---|---|---|
| network101 | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | Netcore Technology Inc. |
| network | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| network | :00:00:00 | PSK-(TKIP\|CCMP) | 1.0 | ALFA. INC. |
| network | :00:00:00 | PSK-CCMP<br>PSK-CCMP | | MERCURY COMMUNICATION TECHNOLOGIES CO.LTD. |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | |
| [Hidden] | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| Vending | :00:00:00 | PSK-CCMP<br>PSK-CCMP | | |
| network | :00:00:00 | PSK-CCMP | 1.0 | Routerboard.com |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | |
| network | :00:00:00 | PSK-CCMP | 1.0 | TP-LINK TECHNOLOGIES CO.LTD. |
| network | :00:00:00 | MGT-(TKIP\|CCMP)<br>MGT-(TKIP\|CCMP) | | TP-LINK TECHNOLOGIES CO.LTD. |
| network | :00:00:00 | PSK-CCMP | | ASUSTek COMPUTER INC. |
| network | 00:00:00 | PSK-CCMP | 1.0 | ASUSTek COMPUTER INC. |
| network | | PSK-CCMP<br>PSK-CCMP | | |

| | | | | |
|---|---|---|---|---|
| network101 | FE:EC:DA:00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| **SSID** | **MAC Address** | **WPA/WPA2** | **WPS** | **Vendor** |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | |
| [Hidden] | 00:00:00 | PSK-CCMP | | |
| network | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| network101 | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | |
| network101 | :00:00:00 | PSK-CCMP | | Ubiquiti Networks Inc. |
| network10 | 00:00:00 | PSK-CCMP | | |
| network10 | :00:00:00 | PSK-CCMP | | |
| network | :00:00:00 | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | Ubiquiti Networks Inc. |
| [Hidden] | :00:00:00 | MGT-CCMP | | |
| [Hidden] | :XX:XX:X<br>X | PSK-CCMP | | |
| network | :XX:XX:X<br>X | PSK-(TKIP\|CCMP)<br>PSK-(TKIP\|CCMP) | | Netcore Technology Inc. |
| network12 | :XX:XX:X<br>X | PSK-CCMP | | Ubiquiti Networks Inc. |

| | | | | |
|---|---|---|---|---|
| network | 64:EE:B7:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Netcore Technology Inc |
| [Hidden] | 7A:8A:20:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| network | B4:FB:E4:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| **SSID** | **MAC Address** | **WPA/WPA2** | **WPS** | **Vendor** |
| [Hidden] | A6:83:C2:XX:XX:XX | PSK-CCMP | | |
| [Hidden] | 0E:EC:DA:XX:XX:XX | PSK-CCMP | | |
| network | B4:FB:E4:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| [Hidden] | 0E:EC:DA:XX:XX:XX | PSK-CCMP | | |
| [Hidden] | B6:FB:E4:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| [Hidden] | 0E:EC:DA:XX:XX:XX | MGT-CCMP | | |
| network101 | 78:8A:20:XX:XX:XX | MGT-CCMP | | Ubiquiti Networks Inc. |
| network | FC:EC:DA:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Ubiquiti Networks Inc. |
| [Hidden] | 2E:EC:DA:XX:XX:XX | PSK-CCMP | | |
| network101 | 74:83:C2:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| [Hidden] | FC:EC:DA:XX:XX:XX | PSK-CCMP | | |
| [Hidden] | 76:83:C2:XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |

| | | | | |
|---|---|---|---|---|
| [Hidden] | B6:FB:E4::XX:XX:XX | PSK-CCMP | | Ubiquiti Networks Inc. |
| network | FE:EC:DA:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Ubiquiti Networks Inc. |
| network | FE:EC:DA:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Ubiquiti Networks Inc. |
| [Hidden] | 86:83:C2:XX:XX:XX | MGT-CCMP | | |
| **SSID** | **MAC Address** | **WPA/WPA2** | **WPS** | **Vendor** |
| eney | 70:8B:CD:XX:XX:XX | PSK-CCMP | 1.0 | ASUSTek COMPUTER INC. |
| network | CE:2D:E0:XX:XX:XX | PSK-CCMP PSK-CCMP | 1.0 | Routerboard.com |
| [Hidden] | 1E:EC:DA:XX:XX:XX | MGT-CCMP | | |
| network | E4:BE:ED:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Netcore Technology Inc. |
| network | 00:72:63:XX:XX:XX | PSK-(TKIP\|CCMP) PSK-(TKIP\|CCMP) | | Netcore Technology Inc. |
| [Hidden] | 30:85:A9:XX:XX:XX | PSK-CCMP | | ASUSTek COMPUTER INC. |
| network | CC:2D:E0:XX:XX:XX | PSK-CCMP PSK-CCMP | 1.0 | Router+A1 |

## Networks for which handshake was intercepted

| MAC Address | SSID | Пароль |
|---|---|---|
| 1E:EC:DA:XX:XX:XX | network10 | ***** |

| | | |
|---|---|---|
| 9A:8A:20:XX:XX:XX | network10 | ***** |
| 78:8A:20:XX:XX:XX | network101 | ***** |
| 74:83:C2:XX:XX:XX | network101 | ***** |
| 78:8A:20:XX:XX:XX | network101 | ***** |
| FC:EC:DA:XX:XX:XX | network101 | ***** |
| 7A:8A:20:XX:XX:XX | network12 | ***** |



## Appendix C. Testing Segmentation Tools

The penetration testing verifies that segmentation controls/methods are operational and effective according to existing network diagram.

| ---> | vlan20 | vlan21 | vlan22 | vlan23 | vlan24 | vlan25 |
|---|---|---|---|---|---|---|
| vlan20 | + | - | - | + | - | - |
| vlan21 | - | + | - | - | - | - |
| vlan22 | + | + | + | + | + | + |
| vlan23 | - | - | - | + | - | - |
| vlan24 | - | - | - | - | + | - |
| vlan25 | - | + | + | + | - | - |