Penetration Testing Report

Example

Prepared for:	Alice <alice@example.com>
Prepared by:	**Henrik Kramselund Jereminsen, Senior consultant hkj@zencurity.com**
Date:	February 8, 2024
Version:	1.0-draft

Penetration Testing ReportExample A/S

this is a sample report, may be copied and reused by anyone! See LICENSE file

Contents

1 Introduction 4

2 Target Overview 5

2.1 Goal and Strategy 5

2.2 Test actions performed 7

3 Executive Summary 8

4 Scanning 10

5 Overview of Open Ports 11

6 Host 10.0.60.74 12

7 Host 10.0.60.122 13

8 Host 10.0.60.123 15

A Whois 16

B DNS and Name Servers 17

C Test Servers 18

Revision History

Revision	Date	Author(s)	Description
1.0-draft	2024-01-01	HLK	Created

1 Introduction

This report is the result of a penetration test activity performed by Zencurity ApS (Zencurity) against the server IP-addresses provided by customer Template A/S. The activity was performed from February 9. until February 20. 20xx.

The primary goal for this test has been to uncover vulnerabilities in the environment which may allow attackers to gain unauthorised access to the network and servers. No denial-of-service (DoS) attacks has been performed. The report contains the digested summary of the vulnerabilities found in this environment. Further we have included some raw data from some of the tools used in this testing activity.

This is an example report created using the template
https://github.com/kramse/pentest-report

2 Target Overview

Security testing was performed against 6 IP-addresses in use by Template A/S. The targets has been the following IP-addresses::

IP address Host name Description 10.0.60.74 No name found Web server 10.0.60.122 No name found Web server 10.0.60.123 No name found VPN server / Netscaler gateway 10.0.60.140 No name found Web server 10.0.60.194 No name found Web server 10.0.60.195 No name found Web server

These addresses are routed by Global Connect and we have no further comments about routing.

Regarding whois information currently states that the subnet should be announced with origin - with the AS number AS25111 or AS2830 - which may have been correct previously.

The objects which are shown in appendix A should be removed is:

```
% Information related to '10.0.60.0/24AS2830'
route:          10.0.60.0/24
descr:          UUNET
origin:         AS1234
mnt-by:         AS4321-MNT
source:         RIPE # Filtered
```

Since this is marked with AS4321 - it probably requires contacting XXX Networks which are AS4321.

We also noticed that the main domain Template.dk and host name www.Template.dk are not the same IP. Template.dk has address xx.26.xx.130 Template.dk mail is handled by 10 Template-dk.mail.eo.outlook.com. www.Template.dk has address xxx.114.xxx.74

Also the IP xxx.26.xxx.130 redirects to www.Template.dk, so we recommend updating the IP to point directly at the real web site and server.

2.1 Goal and Strategy

The review performed is based on data from customer and active testing methods.

We have been given full insight into firewall configuration, Wi-Fi administration, VLAN information, IP address plan etc.

The review contains the following parts and items:

LAN Security Review:

- Software version of the devices
- Basic settings NTP, DNS, Syslog, SNMP
- Networks and VLAN isolation

Wi-Fi Security Review:

- Software version of the devices
- Networks and managed SSIDs
- LAN connection settings, VLAN isolation
- Unmanaged SSIDs
- Encryption settings
- Authentication settings

VPN Security Review:

- Software version of the devices
- Site-2-site VPN
- Client VPN
- Encryption settings
- Authentication settings

Firewall review:

- Software version of the devices
- Basic settings NTP, DNS, Syslog
- Management of system and users
- Management settings including encryption settings and users
- Firewall Zones
- Hosts and host groups
- Services and service groups
- Firewall Rules

2.2 Test actions performed

We have also carried out the following active sub-tasks in this test:

- Full TCP port scan of outside network - including ports 1-65535
- Sample TCP port scans of internal network
- Nmap service scanning - attempted service identification on open ports
- Sample UDP port scanning and service scan using Nmap UDP probes
- Metasploit Discovery and port scan tasks of outside network
- Metasploit Penetration task of outside network
- TLS scanning using multiple tools for identifying the supported server ciphers
- DNS lookups, traceroute, ICMP testing and other basic tasks
- Manual test cases against systems found

Port scan includes protocols TCP, UDP and IP scanning utilizing various scanning techniques. The service scan performs deeper identification by sending valid requests for the services, to try to identify the actual open service in more detail.

Due to the nature of the UDP protocol it cannot be fully scanned, and results for UDP are more uncertain. Instead probes have been sent for the most popular protocols in use on top of UDP.

Exploitation has been attempted using exploits against open ports using exploits and specialized scanning for protocols identified.

3 Executive Summary

This report is the result of review activities performed by Zencurity ApS . The activities were performed in December 2023. Scope has been to perform a Network Review: Cloud Services security of the network at the main site.

The primary goal for this test has been to uncover weaknesses and vulnerabilities in the environment which may allow attackers to gain unauthorised access to the network and servers. We have discovered minor to high risk vulnerabilities in the tested systems.

examples only, hopefully no customer has all of these!

The main conclusions are:

- Port scan and visual inspection has revealed a number of older, insecure and outdated LAN network devices. Also single points of failure, single critical devices are found in the current network
  We recommend elmininating single point of failure for critical systems and services
- Port scan has identified a number of unmanaged devices or devices with default vendor credentials
- The network has a lot of management interfaces that can be attacked from the LAN
- Port scan has shown that traffic flows internally are almost unrestricted from LAN segments to other parts, and from on-site and into remote segments connected through VPN
  We recommend implementing basic filtering, to restrict data flows, and to ensure they are in place when needed in the future
- A malware incident and/or hacker activity in this network would have a high risk of infecting many parts of the infrastructure.
  We highly recommend creating new zones/VLANs for isolation and segregation
- Wireless networks managed by Example are encrypted using up-to-date protocols
- Wireless scan has identified a number of unmanaged wireless networks, or test networks with unknown security levels
- We have observed that Wi-Fi solutions are configured with multiple SSIDs sharing VLANs.
  We recommend reconfiguration of the VLAN settings
- Some wireless network use shared key systems WPA-Personal – with keys known by former employees that have left the organisation
  We recommend setting dates for removal of the wireless networks using WPA-Personal shared keys
- VPN solutions are configured with older and insecure encryption and integrity algorithms.
  We recommend reconfiguration of the VPN settings

- Firewall review has identified few problems with the firewall itself, as the firewall was reconfigured recently.
- Firewall review has shown the current firewall policies to be very open. Current policies allow devices in network segments used by employees, wired and wireless, to communicate freely – even across production, development and testing facilities. This is not according to best current practice and we recommend creating new zones/VLANs for isolation and segregation
- Firewall review show that networks are not separated and there is a high likelihood that problems in one area of the network will affect the whole network and all users
- ...

The overall conclusion is that the current network is not sufficiently protected from attacks due to almost no segregation of the zones used. This coupled with a user base that are allowed to connect and disconnect a number of devices, servers and systems create a high risk of security incidents involving large parts of the organisation.

We recommend the following initiatives regarding networks at Example are put into places with a priority to isolate and improve the networks and devices:

1. Unmanaged devices should be removed or controlled
2. Single point of failure should be eliminated to avoid disruptions to normal business
3. Best current security practices dictate the placement of the management ports on a dedicated management LAN or VLAN restricted to trusted Administrators.
4. VPN site-2-site settings should be updated, and requires few resources. This includes implementing basic filtering, that can be expanded in case of incidents
5. Client VPN solutions should have updated settings, and would benefit from a single solution. Client VPN should also have basic filtering implemented, that can be expanded in case of incidents
6. Traffic flows between segregated networks should be monitored closely
7. Port-security should be used for limiting the use of unmanaged devices, and limiting the effect of connecting other equipment that may affect the networks. Port-security can also be used for automatically joining a connecting user to the right network
8. ...

Finally, Zencurity recommends that Example A/S performs periodic security testing of its business to verify that mechanisms and processes implemented to protect critical company assets are working as expected. Especially the processes and mechanisms that will detect and respond to an attack.

OR

We have no further recommendations to the current environment, and can only recommend that the instructions from the vendors are following regarding the administration, software upgrading and control of this environment.

The following sections described in more detail the information uncovered during this testing.

4 Scanning

During this testing project we have uncovered open TCP ports and other services, as to be expected from such an environment. The open ports and services have been identified further and examined by tools known as service scanning. We have also concluded that a firewall/filtering device is in place, which can be seen in the responses received - and responses not received for port requests sent.

The open ports and services are shown below. The firewall in place is reported with the port status filtered, which is according to best current practice. Most ports are filtered which is good.

Due to the nature of the UDP protocol it cannot be fully scanned, and results for UDP are more uncertain. Instead probes have been sent for the most popular protocols in use on top of UDP. We have tried sending UDP probes for the 100 most popular UDP ports found on the internet. A full UDP port scan could not be completed as the firewall discards the probes without sending any indication if the UDP ports are open or not.

We have also performed invasive intrusion attempts at the services.

5 Overview of Open Ports

The found servers and open ports are shown below:

```
Hosts
=====

address       mac  name          os_name        os_flavor  os_sp  purpose  info  comments
-------       ---  ----          -------        ---------  -----  -------  ----  --------
10.0.60.74        10.0.60.74    Windows                          device
10.0.60.122       10.0.60.122   Windows 7                        client
10.0.60.123       10.0.60.123   embedded                         device
10.0.60.140       10.0.60.140   Windows Vista                    client
10.0.60.194       10.0.60.194   Windows 7                        client
10.0.60.195       10.0.60.195   Windows 2008                     server


Services
========

host          port  proto  name   state  info
----          ----  -----  ----   -----  ----
10.0.60.74    80    tcp    http   open   Microsoft-HTTPAPI/2.0

10.0.60.122   80    tcp    http   open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator
10.0.60.122   443   tcp    https  open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator

10.0.60.123   443   tcp    https  open    ( 302-/vpn/tmindex.html )

10.0.60.140   80    tcp    http   open    ( 302-https://10.0.60.140/ )
10.0.60.140   443   tcp    https  open    ( 403-Forbidden ( The page requires a client certificate as part of the au

10.0.60.194   80    tcp    http   open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator
10.0.60.194   443   tcp    https  open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator

10.0.60.195   80    tcp    http   open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator
10.0.60.195   443   tcp    https  open    ( 403-Forbidden ( The server denied the specified Uniform Resource Locator
```

6 Host 10.0.60.74

We have the following basic information about this host:

```
Nmap scan report for 10.0.60.74
Host is up (0.017s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft ISA httpd
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The ports and services found are expected with web servers

The ports identified are probably used for: port 80 HTTP Hypertext Transfer Protocol unencrypted

The protocols are expected in this environment.

Vulnerabilities
We have not uncovered vulnerabilities for this server and have no further recommendations.

7 Host 10.0.60.122

We have the following basic information about this host:

```
Nmap scan report for 10.0.60.122
Host is up (0.017s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Microsoft IIS
|_http-methods: No Allow or Public header in OPTIONS response (status code 403)
|_http-title: The page cannot be displayed
443/tcp open  ssl/http Microsoft IIS
|_http-methods: No Allow or Public header in OPTIONS response (status code 403)
|_http-title: The page cannot be displayed
| ssl-cert: Subject: commonName=*.Template.com/organizationName=Template A/S/stateOrProvinceNa
| Not valid before: 2010-12-14T11:50:26+00:00
|_Not valid after:  2015-12-14T11:50:24+00:00
|_ssl-date: 2015-02-20T07:49:51+00:00; 0s from local time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The ports and services found are expected with web servers

The ports identified are probably used for:

- port 80 HTTP Hypertext Transfer Protocol unencrypted
- port 443 HTTPS Hypertext Transfer Protocol Secure encrypted

The protocols are expected in this environment.

Vulnerabilities
This server supports SSL version 2 and SSL version 3 both which should be turned off.

```
Testing SSL server 10.0.60.122 on port 443
  Supported Server Cipher(s):
Accepted  SSLv2    128 bits  RC4-MD5
Accepted  SSLv2    112 bits  DES-CBC3-MD5
```

```
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    128 bits  RC4-MD5
Accepted  SSLv3    112 bits  DES-CBC3-SHA
```

We have not uncovered further vulnerabilities for this server and have no further recommendations.

8 Host 10.0.60.123

We have the following basic information about this host:

```
Nmap scan report for 10.0.60.123
Host is up (0.018s latency).
Not shown: 65534 filtered ports
PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https
|_http-methods: No Allow or Public header in OPTIONS response (status code 302)
| http-title: NetScaler Gateway
|_Requested resource was /vpn/tmindex.html
| ssl-cert: Subject: commonName=*.Template.com/organizationName=Template A/S/stateOrProvinceNa
| Not valid before: 2010-12-14T11:50:26+00:00
|_Not valid after:  2015-12-14T11:50:24+00:00
|_ssl-date: 2015-02-20T07:50:04+00:00; +13s from local time.
```

The ports and services found are expected with web servers

The ports identified are probably used for: port 80 HTTP Hypertext Transfer Protocol unencrypted port 443 HTTPS Hypertext Transfer Protocol Secure encrypted

The protocols are expected in this environment.

Vulnerabilities
This server supports SSL version 2 and SSL version 3 both which should be turned off.

```
Testing SSL server 10.0.60.123 on port 443
  Supported Server Cipher(s):
Accepted  SSLv3    256 bits  ECDHE-RSA-AES256-SHA
Accepted  SSLv3    256 bits  AES256-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-AES128-SHA
Accepted  SSLv3    128 bits  AES128-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-RC4-SHA
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    128 bits  RC4-MD5
Accepted  SSLv3    112 bits  ECDHE-RSA-DES-CBC3-SHA
Accepted  SSLv3    112 bits  DES-CBC3-SHA
```

We have not uncovered further vulnerabilities for this server and have no further recommendations.

Appendix A Whois

This section contains the whois information about the customer range. We always perform this lookup to ensure we are targetting the correct customer.

NOTE: in this test we observed that an extra route-object exist, which point to another origin AS number for this range. Customer should instruct network department to fix this to avoid future routing problems.

NOTE: we can see that ZENCURITY-MNT is allowed to make changes to these object, which is probably not relevant anymore and should be removed.

```
inetnum:        193.0.56.0 - 10.0.60.255
netname:        Template
descr:          Template A/S
country:        DK

% Information related to '10.0.56.0/22AS1234'

route:          10.0.56.0/22
descr:          Template Network
origin:         AS12345
mnt-by:         AS12345-MNT
source:         RIPE # Filtered
```

Appendix B DNS and Name Servers

We have performed lookups with regards to the main domain Template.dk Name servers for the domain (host -t ns Template.dk):

```
Template.dk name server ns1.ascio.net.
Template.dk name server ns2.ascio.net.
ns1.ascio.net has address 185.26.230.9
ns2.ascio.net has address 80.237.153.102
```

We have performed lookups with regards to the main domain Template.com Name servers for the domain (host -t ns Template.com):

```
Template.com name server ns2.ascio.net.
Template.com name server ns1.ascio.net.
Template.com name server ns4.ascio.net.
Template.com name server ns3.ascio.net.
ns1.ascio.net has address 185.26.230.9
ns2.ascio.net has address 80.237.153.102
ns3.ascio.net has address 54.183.16.145
ns4.ascio.net has address 72.32.149.232
```

This shows at least two name servers for domains, and these are placed in separate subnets. No further comments about domains.

Appendix C Test Servers

We have performed the testing from the IP addresses below:

- 91.xx.xx.0/28 main test range
- 185.xx.xx.0/24 main test range
- 10x.xx.xx.20 manual verification via VPN