Your LOGO

REPORT PENETRATION TESTING

Client: JOAS ANTONIO

Author	
Date	
Version	

Contents

List of Figures

LOGO

List of Tables

Endereço:
Telefone:

1 Document Control

1.1 Document Issuer

Address	
Telephone	
Email	
Author	

1.2 Document History

Date Issued	Version	Comment	Author

Table 1: Report Publication History

1.3 Non Disclosure Statement

This document contains intellectual property rights and copyright, which are proprietary to the Cyber Security UP. The work and the information it contains are submitted for the purpose of making a proposal, fulfilling a contract or as marketing collateral. It is to be treated as confidential and shall not be used for any other purpose. It shall not be copied or disclosed to third parties in whole or in part without the prior written consent of the Cyber Security UP.

1.4 Comments on Report

The Cyber Security UP welcomes comments and feedback on our reports. Any comments on this report should be passed to the Cyber Security UP within 10 working days of the report being issued to the client. If no comments are provided within this timeframe the client will be deemed to have accepted the report and its findings in full.

1.5 Statement of Limitation

This work was performed under the standard the Cyber Security UP terms and Conditions of Sale. The Cyber Security UP tested the systems at the requested time and is unable to comment on the security or vulnerabilities that existed prior to or after the testing was performed. All testing is time limited and it might not be possible to fully investigate every issue or find all possible security issues. The Cyber Security UP cannot comment on systems that were outside of the scope of this report, were unavailable at the time of testing or where the required access was not provided. This report should not be considered to be a list of all vulnerabilities or issues that exist on the system or environment. The Cyber Security UP cannot comment on the fixes applied to systems after this test without technically assessing them.

2 Technical Summary

The following document summarises the results of the penetration test undertaken by the Cyber Security UP on behalf of Client.

2.1 Scope of Testing

2.1.1 Assessment

I conducted a Penetration Test of the mobile phone organisation foophones. This included the following testing ele-ments:

Also from a OWASP Web Application Perspective

Internal aspects for the organisation were also tested once a machine was compromised as well as the ability to escalate privileges on compromised machines. Finally how easy it is for an attacker to pivot onto other internal networks with the final aim being to exploit the DMZ server which was accomplished.

2.1.2 Targets

2.1.3 Testing Dates

This assessment was conducted between DATE.

2.2 Assessment Team

This assessment was performed by the following consultants:

2.3 Source IPs

All external testing took place from the dedicated exam environment, the source address I was given is listed below.

2.4 Critical Recommendations

Multiple Critical Vulnerabilities were discovered during the engagement which led to the full compromise of the web server machine on the initial network, it was then possible to pivot to the corporate network to continue exploitation of other Windows machines through psexec and a buffer overflow exploit and then finally to pivot to the final DMZ network. Where the compromise of previous machines on proceeding subnets allowed for the disclosure of credentials to access the DMZ server via SSH.

2.5 General Recommendations

Multiple unsupported operating systems were discovered to be running on all hosts throughout the network infrastruc-ture as well as unpatched software which should be remedied immediately doing so would help to mitigate many of the more critical vulnerabilities discovered on these hosts.

As previously mentioned in the report multiple Type Vulnerabilitys are present on the initial web application. Sanitizing all user input as well as deploying a WAF would help to mitigate many of these found issues. Anti-virus must be deployed on all machines in the organisation in order to stop the running of malicious executables such as Mimikatz for example which can be used on a compromised Windows host to pull credentials from memory.

Within the Windows environments the psexec modules should be disabled in order to stop users remotely authenticating

with other Windows file share devices via just a username and hash of the password. SMB signing should also be enabled on all Windows hosts. All hosts should be checked for easy privilege escalation points such as SUID binaries and whether sudo privileges have been at all misconfigured. Kernel versions on all hosts must be checked for available privilege escalation exploits.

The Customer Management Portal application running on one of the hosts was discovered to be vulnerable to a buffer overflow exploit and should be immediately disabled and its application source code completely rewritten as at present it is possible to leverage this buffer overflow to gain remote code execution and ultimately spawn a shell which is what I managed to do during the engagement.

All software and applications running on hosts in the network should be at the latest version and also fully patched. I make particular reference to a running instance of WINSCP which allowed me to run a post exploitation module against it within Metasploit to gain working credentials for the final server in the DMZ network.

2.6 Statistics

2.6.1 Issue Severity vs. Likelihood Map

The following table displays the number of issues according to both severity and likelihood.

Likelihood \ Severity	Critical	High	Medium	Low
High	0	0	0	0
Medium	0	0	0	0
Low	0	0	0	0

2.6.2 Issue Severity Averages

No. Hosts Tested	5
Average No. Issues Per Host	3.60
Average No. Critical Issues Per Host	1.40
Average No. High Issues Per Host	1.60
Average No. Medium Issues Per Host	0.40
Average No. Low Issues Per Host	0.20

2.7 Overall Conclusion

In comparison to similarly scoped engagements from a black box perspective the foophones external internal and ap-plication level of security was found to be incredibly poor. Gaining a foothold onto the network through the initial web application is a trivial task for any potential threat actor. With the application being vulnerable to multiple critical Type Vulnerabilitys leading to complete takeover.

Once a device was compromised privilege escalation as well as pivoting to reach other parts of the internal infrastructure was also possible as mentioned in the report no anti virus solution appeared present on any of these devices allowing for the unrestricted upload, download and execution of malicious payloads. Outdated Operating Systems and unpatched software appeared to make up the majority of the environment that was encountered during the engagement.

The web application must be completely overhauled to begin with as this is currently the potential threat actors publicly available initial entry point to the internal network. User input must be sanitized as previously mentioned by the server with tags and malicious characters being stripped. Encoding must also be added when user input is processed by the server and a Web Application Firewall must be deployed and fine tuned to catch malicious payloads this will help to mitigate the multiple Type Vulnerabilitys I found on the application. An anti-virus solution should also be deployed on the discovered devices.

3 Issue Summary

The table in this section offers a technical summary of the vulnerabilities that were discovered during the test.

3.1 Table Of Vulnerabilities Discovered

Issue Title	Severity	Likelihood	Type Vulnerability	Hosts
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	Critical	High		
Vulnerability (1 Host Affected)	High	High		
Vulnerability (1 Host Affected)	High	High		
Vulnerability	High	High		

Issue Title	Severity	Likelihood	Type	Hosts
(1 Host Affected)				
Vulnerability (1 Host Affected)	High	High		10.185.11.127
Vulnerability (1 Host Affected)	Medium	High		10.185.10.34
Vulnerability (1 Host Affected)	Medium	High		foophonesels
Vulnerability (1 Host Affected)	Medium	High		foophonesels
Vulnerability (1 Host Affected)	Medium	High		10.185.10.34
Vulnerability (1 Host Affected)	Medium	High		10.185.10.34
Vulnerability (1 Host Affected)	Medium	High		foophonesels
Vulnerability (1 Host Affected)	Low	Low		10.185.10.27

Table : Issue Summary Table

4 Security Issues Identified

4.1 Vulnerability

No. Hosts Affected:	0	Severity:	Critical	Likelihood:	High	Type:	Type Vulnerability

Explanation of Issue

Figure 1:

List of Hosts Identified

Recommendation

.

Endereço:
Telefone:

Common Vulnerability Scoring System (CVSS)

Base Score:	7.1	Base Vector:	AV:L/AC:L/Au:N/C:C/I:C/A:C
Overall Score:	7.1		

.

A Definitions

A.1 Vulnerability Severity

Vulnerabilities are provided with a severity scale that has been individually determined by the CNS Tester taking into consideration the results of the test performed within the customer's unique environment.

No automated tools are used to determine this severity scale.

Severity	Description
Critical	A critical vulnerability is one that has been performed by CNS and has led to the target being compromised by the vulnerability.
High	A high vulnerability is one that is confirmed as a positive vulnerability and can lead to a network or host breach and may lead to the target being compromised.
Medium	A medium vulnerability is one that may disclose further information that may lead to an attack or where unnecessary details were found that may decrease the security of the target e.g. unnecessary open ports.
Low	A low vulnerability regards information found during the test that may not be an immediate threat to the company. However the company should review the information and determine the correct course of action.

Table : Definition of Severities

A.2 Likelihood of Vulnerability

It can also be useful to determine the risk on the likelihood of a specific vulnerability occurring on the target host. There-fore the vulnerability is assessed individually to determine this risk.

NOTE: The table below should only be used as an indication of the likelihood of the threat.

Likelihood	Description
High	A vulnerability that has a high likelihood is either publicly available and is very common, or is a relatively easy exploit to run. Either case should be reviewed as soon as possible. Viruses, worms, Trojans, default settings etc. are all examples of high likelihoods.
Medium	A vulnerability that has a medium likelihood is one which requires a certain amount of skill to run or one that is difficult to find unless the target host was specifically targeted. To actually perform the exploit may require various steps or knowledge of the application or service to be successful. Specific application vulnerabilities such as SQL injection, XSS attacks are examples of medium likelihoods.
Low	A vulnerability that has a low likelihood is one which is either extremely difficult to run or is not publicly known or available. If a vulnerability has a low likelihood, it does not necessarily mean that it will have a low severity.

Table : Definition of Likelihoods

A.3 Vulnerability Types

Vulnerabilities are categorised into specific types to help the customer assess the threat. The following table details the vulnerability types further:

Type	Description

Continued on next page...

Type	Description

Table : Definition of Vulnerability Types

B Host Enumeration

Following the network discovery phase, each host was examined in turn for signs of any vulnerabilities or mis-configurations that might give an attacker a route into the network. Each host was enumerated to see which ports were open to the outside world. Each of these ports were then examined further to determine the applications running on the ports and the ways in which these applications might be subverted.

B.1 Operating System Detection

This test attempts to gain the fingerprint of the operating systems for each host. Knowing the operating system is a distinct advantage to finding vulnerabilities. The scan generally gives a percentage on how successfully it guesses the OS.

Host	OS Detected

Table : OS Detection Table

B.2 Port Enumeration

TCP/IP Ports can be in one of 3 states:-

- Open = Target host will accept connections to that port
- Filtered = A firewall or filter is in place stopping the port scan
- Unfiltered or Closed = No firewall or filter has interfered with the scan, which has determined that the port is closed to connections.

Open ports are generally the target ports to exploit. However for a dedicated hacker, filtered ports could also potentially be a target. This test will investigate what state the ports are in for each host.

Host	Port	Protocol	Description	Status

Continued on next page...

Host	Port	Protocol	Description	Status

Table : Port Scan Summary Table

C Graph Pack

C.1 Number of Vulnerabilities by Type

Figure : Number of Vulnerabilities by Type

C.2 Number of Vulnerabilities by Severity

Figure : Number of Vulnerabilities by Severity

.