Case 3 Security Assessment Group 5

Fatima Bayloun
Sandra Börjesson
Muhammad Arsalan Khan Mughal
Nibha Priyadarshini

22nd April 2022

Executive Summary **3**

Definitions **3**

Penetration Testing **3**

- Planning 3
- Discovery 4
- Attack 5
- Reporting 6

Metrics **7**

Conclusion/Summary **8**

1. Executive Summary

The main objective of the penetration test on Radio Sweden is to assist the administrators and the ones responsible for the security of E-mails, Intrusion Detection Systems, and other components. The penetration testing is performed by using the ‘white hat’ penetration testers, where the main aim is to exploit the systems, networks, and applications inside the organization.

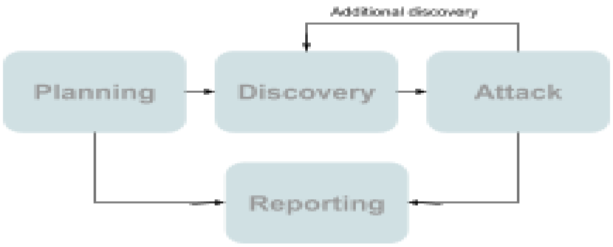
2. Definitions

White hat = Is a form of security testing, where the tester has internal/external knowledge about an organization and tests its functionality. The white hat testing indicates full access to the organization with the awareness of the organization (NIST SP 800-115).

Penetration testing = is known as an ethical attack where the pentester tries to attack the organization in order to find security flaws inside the organization (NIST SP 800-115)..

3. Penetration Testing

In the light of NIST SP 800-115, the penetration testing process is documented in this section following the *Four-Stage penetration Testing Methodology: Planning, Discovery, Attack, and Reporting.*



NIST SP 800-115 (5-2)

A. Planning

In this phase, it is important to state the perspective of the planned testing, which is set to be: an outsider’s attack (technical & non-technical). An example of a non-technical attack is the use of social engineering; which will be done by the tester/attacker pretending to be a help desk agent requesting a password from an employee.

In addition to the scope that is the assets covered by the penetration test; Based on the provided overall IT architecture, these assets are:

Computers (employees and journalists)	Network devices (Cisco Catalyst 9800 controller, Cisco 8808 routers, Cisco ASA 5500 firewalls, Aironet 3800 access points, HP Officeconnect 1850 Gigabit switches)
Servers (Windows 2016, Solaris 11.1, GNU/Linux)	Software and operating systems (?) (F-Secure Client Security anti-malware)

B. Discovery

In order to identify potential targets, information gathering techniques are to be conducted as the first part of this phase, and then the second part is a vulnerability analysis.

1. Intelligence gathering (passive and active methods)

Passive	Active
Collect unencrypted credentials or data (Network/packet Sniffing)	Social Engineering
Employee names and contact information (searching directory servers or web servers)	Vulnerability Scanning
Domains and additional IP address related info (address/location, timezone, etc..): WHOIS queries	Port scanning for “Network port and service identification” + identification of firewalls, IPS, IDS.
Hostnames and IP addresses (DNS interrogations)	Password attacks (brute-force or spraying)

2. Vulnerability analysis

This involves analyzing the collected data in part one and then comparing the identified services against vulnerability databases.

example:

- Cisco 8808 routers (CVE-code execution vulnerability) >> HIGH
- Cisco ASA 5500 firewalls (ASA- DoS Vulnerability) >> HIGH
- Windows server 2016 - (CVE elevation of privilege vulnerability) >> HIGH

C. Attack

1. Gaining access
2. Escalating privileges
3. System Browsing
4. Install additional tools

Below is an example of how an attack would be carried out based on one of the vulnerabilities analyzed above and following the 4 steps recommended in the NIST SP 800-115:

1. *Gaining access* = indicates that there is sufficient data being collected to gain access to the target.
2. *Escalating privileges* = The attacker will try to get more access to the system in order to get the full capacity.
3. *System Browsing* = Start to identify and access things in the system, as well tries to access additional components to the system.
4. *Install additional tools* = more tools are installed to get additional access to the system.

Attack type	gaining access	escalating privileges	system browsing	install additional tools
Phishing email	Sending a trojan attached in an email message to an employee	after clicking on the attachment the attacker will gain access to the user's computer and try to get admin rights	the attacker will browse the system(s) looking for sensitive data/documents/credentials and additional entry points	a backdoor can be installed (rootkit, keylogger, ransomware, worm, etc..) to gain more control and access more sensitive data
Misconfigurations in firewall	Attacker from the outside world gets access to firewalls	Attacker analyses the firewall system, tries to get more access to the existing network set up and tries to make changes	Attacker will look for systems with sensitive data, sensitive processes and tries to get access to them	Tries to install tools like rootkit, keylogger, ransomware to get more control. An attacker can stop the processing of existing systems

D. Reporting

Vulnerability	Security Control	Metrics		
		concern	Data source	Metric
Code execution vulnerability	firmware updates	Routers/network	Firewall logs/ event management system	#bad authenticated logins #Frequency of code execution in unplanned times #Number of errors identified during code execution
Elevation of Privilege vulnerability	update Windows server 2016	Data & Users' credentials	logs	#Number of new users gained more privilege
DoS		Hosts/systems/servers/ Availability	Manual tracking + host monitoring system	host uptime(%, hours),
Employees security awareness	Educate & train users	Data/documents/credentials -prevent Phishing attacks-	Internal systems (e.g. HR)	#training hours/ %new/existing employees completing security training

*More about the metrics can be seen in the next section, section 4.

- Clean up
  After finishing the test, the team has to inform the targets at Radio Sweden about any changes made as part of the test and about the cleaning up process carried on at the end. This process includes removing any created users, restoring system configurations, and cleaning any mess caused by the penetration testing team.

4. Metrics

The primary goal of using metrics is to quantify data and understand security risks. The diagnostic metrics chosen for Radio Sweden were the perimeter defenses, where the main focus was on the E-mail and the intrusion detection system.

5.1 Control Metrics

Perimeter defense metrics			
E-mail			
	Purpose	**Sources**	**Unit of Measure**
“How many e-mails are being sent per day”	To find out the speed of the e-mail traffic, and to get an overall view of the traffic.	E-mail system	**Number**
“Detected spam/filtered e-mails”	To see the efficiency of the spam filtering software.	Filtrering software for E-mails.	**%**
“Not detected spam/filtered e-mails”	To see the overall view of detected and undetected spam e-mails and filter the e-mails more efficiently.	Filtrering software for E-mails.	**%**
“Viruses and other malicious code being detected in e-mail messages”	As the previous one, to detect and filter out e-mails that show any indication of spam or malicious code.	Filtrering software for E-mails.	**%**

Perimeter defense metrics			
Event log/ IDS/			
Intrusion Detection Systems	**Purpose**	**Sources**	**Unit of Measure**
“False positives recorded in the IDS”	To get an overview of the activities being caught by IDS, in order to improve its functionality.	Security information and event management system.	**%**
“False negatives being recorded in the IDS”	To get an overview of the activities being caught by IDS, in order to improve its functionality.	Security information and event management system.	**%**
“Changes of rules or updates /monitoring being done in the IDS”	To see how often is being handled, to ensure that it records new threats.	Security information and event management system.	**%**

Conclusion/Summary

There are limitations to this penetration testing. One is that the testing could impact the network and systems inside the target environment. As well, this report will not be providing a complete picture of security for Radio Sweden, however, it will give a detailed document regarding the most severe attack on the organization. This report has been discussing the threats to the E-mails, routers, and firewalls. It has as well mentioned the current Intrusion Detection System in Radio Sweden. The identified stakeholders such as administrators of Radio Sweden should be reading and discussing the results of the penetration testing. The results should also provide the organization with information on how they could mitigate these threats, how to decrease the impact of the vulnerabilities and how they could improve their security inside of Radio Sweden.