CYBER VT2022

Case 3 Cyber Security Assessment #10

Jawdat Kour
Anas Kwefati
Hideo Tommaso Nishimura
Munish Sharma

Radio Sweden Pen testing phases

1- Planning:

During this phase the scope of the assessment needs to be determined. In addition, rules should be identified and goals set. Here, the foundations for the testing are laid, therefore no actual testing is carried out. The scope of the penetration testing is Radio Sweden AB's organization and IT systems. The penetration testers have the responsibility to report any incidents or changes to the systems as a result of the penetration testing to the incident management team.

Because penetration testing techniques may provoke loss of system availability, we aim to perform these tests in off-hours so as to reduce the effect on operations. However, in the event of operational impact, we advise Radio Sweden to establish an incident response plan during the security assessment. An additional consideration to be made is the exposure of confidential information or personally identifiable information (PII). Therefore, we advise the head of IT that, if possible, the penetration test is performed on systems storing only test data, rather than real PII.

2- Discovery:

There are two components to the discovery phase. The initial stage entails gathering data and scanning for potential access ways into systems and networks. The second stage involves analyzing various vulnerabilities using the testers' knowledge or public databases like the National Vulnerability Database (NVD). The following is a description of the discovery phase for the two penetration tests.

Part 1 - Intelligence gathering and scanning

In this part, we will do a port scanning in order to gather information regarding the network. We will be using tools such as nmap. We can also use social engineering, which will help to identify a possible target by searching LinkedIn or reading articles on the internet. And investigate the target's interests and vulnerabilities by looking through their social media channels and other websites.

Part 2 - Vulnerability Analysis

This phase of discovery involves gathering as much information about the target systems, networks, and their owners as possible without actually attempting to penetrate them. The analysis can be conducted by using:

- Vulnerability databases

- Vendor vulnerability announcements

- Asset management systems

- Threat intelligence (gathering data from open sources such as global threat databases) feeds

- Automated testing tools to identify vulnerabilities.

Automated scan is one technique that can be used to search for vulnerabilities of Radio Sweden, with the support of tools such as the software: Greenbone Security. However, vulnerability scanners only check for possible vulnerabilities, this phase exploits the vulnerabilities in order to confirm their existence.

3- Attack:

During the attack phase, the identified vulnerabilities are put to test. If a vulnerability is verified during the attack, security measures are developed to eliminate or at least mitigate the vulnerability. However, if the tester does not manage to penetrate, the vulnerability is not verified. Then it needs to be investigated whether the test failed due to lack of preparation during phase one and two, or if it is simply the case that the vulnerability is not a vulnerability. The attack phase for the two penetration tests is described below:

Social engineering

When the discovery phase is done the following step should be performed to gain access to the systems.

1. Write about a fake scoop in an email, sent from an anonymous email address (this creates a whiteblowing-feeling). This should be of interest of the selected target and contain attachments of malicious files.
If the tester has gained access to the system the tester should try to gain more privileges and explore the systems to gain access to additional systems.

Technical penetration

If a vulnerability in any ports or systems is found during the scanning process the following step should be performed.

1. Try to access important systems, machines or other networks. If password-protected, try standard passwords, character-related passwords and passwords from common password-databases. If the tester has gained access it can be examined if it’s possible to create any backdoors or if it's possible to execute a ransomware attack by gaining access to important files, databases etc and encrypting them.

The identified vulnerabilities are put to the test during the attack phase. If a vulnerability is discovered during the attack, security measures are created to minimize or at the very least mitigate the risk. If the tester is unable to infiltrate, however, the vulnerability is not

confirmed. Then it must be determined whether the test failed because of a lack of preparation during phases one and two, or if the vulnerability is simply not a vulnerability.

Vulnerabilities detected:

#	Description	Recommendation
1	Linux Kernel 4.14.x RedHat 'Mutagen Astronomy' Local Privilege Escalation	Apply security Hotflix RHSA-2018:2748 or increase system memory to 32GB or above
2	Windows Installer running in Windows 10 fails to properly sanitize input leading to an insecure library loading behavior.	Apply Windows 10 - 1909 security patches
3	Cisco Adaptive Security Appliances (ASA) 5500 firewall allows unauthorized remote attackers to cause a DoS	Apply access control list (ACL) and block the source IP address. Apply updates released by vendors
4	Catalyst 9800-40 Wireless Controller Firmware contains several security vulnerabilities	Update to latest IOS XE Software: Amsterdam-17.3.3 or later

4- Reporting:

The reporting phase is presented as the final phase, but it is important to note that reporting will be done throughout all the penetration testing phases. Initially, during the planning phase, an assessment plan should be developed, while reports should be written and presented to management and system administrators periodically during the discovery and attack phases. Keeping logs might also be appropriate during these phases. At the end of the testing a report will be compiled containing risk ratings, identified vulnerabilities, as well as proposed mitigations that could be taken to handle the identified vulnerabilities. The reporting documents will be made available to all relevant parties, for instance CEO, CIO, CISO etc. The reporting phase for the two penetration tests is described below:

Social engineering & Technical penetration

The responsible person for each penetration test compiles a final report together with the

team. The report should include all relevant details such as the involved parties, procedures/steps carried out, identified vulnerabilities/weaknesses and suggestions of possible mitigations of identified vulnerabilities/weaknesses. Eventual incidents and changes to the systems should also be stated in the report.

Security Controls and Metrics:

The goal of security metrics is to assess the effectiveness of the security controls we invest in.

Metric (Unit of measure)	**Purpose**	**Security controls**	**Motivation**
Spam detected/filtered	Indicator of email pollution	Email Security filter	Decrease the possibility of phishing attacks
Viruses and spyware detected in email message	Indicator of email spam	Email Security filter	Decrease the possibility of phishing attacks
Strict configuration of firewalls	Decrease the unauthorized access to users	Firewall management	Reduce access to the company's system
Security training for all employees	Decrease the weakness for social engineering attack	User vigilance	Create security awareness among employees
Detect unusual patterns	Discover behaviors that are unusual in case of an intrusions to the systems	IDS	Detect suspicious activities and flag them by alerting administrators