CH1

What is footprinting and which goals does it achieve. Describe the basic steps that should be performed for a through footprinting analysis.

CH2

Describe at least one technique to determine which services are running or listening on a remote host. Discuss pro and cons, and which tools you may use in practice.

What are ping sweeps? Describe at least two host discovery techniques, and at least one tool used to perform host discovery.

Stack fingerprint - operating system detection

CH3

Discuss the differences between scanning and enumeration. Describe at least one enumeration technique.

Discuss the differences between scanning and enumeration. Describe at least three enumeration techniques, and discuss the countermeasures for each of these techniques.

SNMP enumeration, which account you need, countermeasure.

Describe the technique to enumerate the Microsoft’s Server Message Block (SMB) service. What information can be enumerated from the SMB service? Under what assumptions is each of such enumeration possible? Discuss the tools, explain how each of them works, and also the countermeasures for this enumeration attack. Is Microsoft providing a facility to prevent SMB enumeration?

enumerazione dell' Active directory in Windows con tool

enumerazione dell' Active directory in Windows con tool

SNMP

CH4

What are the three main network password exchange protocols used in Windows systems? Describe the pass-the-hash and pass-the-ticket attacks and countermeasures.

Explain what steps attacker should take to cover his tracks after successfully gaining administrator privileges on Windows system in order to avoid detection. Attackers can hide their files in the system?

extracting password windows ok

Describe at least three Windows security features available with Windows 200 and above. Are there published attacks that bypass these three security features? P.s. the presentation of Windows Firewall and Automated Updates will not be evaluated. ok

The Administrator account of a Windows server has been compromised. Host software cannot be re-installed for business reasons. With these assumptions, how do you plan and implement post-exploit activities for the host recovery. In particular, list the areas of the system on which to intervene, to restore the host’s security. Discuss in detail at least one of these areas of intervention, listing the activities to be carried out, the tools, the line commands to be used, etc. ok

Explain what steps an attacker should take to cover his tracks after successfully gaining administrator privileges on Windows system in order to avoid detection. How attackers can hide their files in the system?

extracting password windows

CH5

Describe at least one attack method to gain remote access on a UNIX system. Describe at least one attack method to gain root access. Discuss pro and cons.

Describe UNIX permission system and the main attack vectors related to permission system.

Explain briefly what a buffer overflow attack is. Describe at least one buffer overflow technique that allows hackers gain remote access to a Unix system even when data execution prevention is enabled. Describe at least two countermeasures against standard overflow attack in Unix system.

How attackers use back channel to gain remote access to a Unix system? Describe an attack scenario and explain the possible commands that attackers use to create a back channel. Discuss the possible countermeasures.

What are symlinks and how do they work? How can an attacker exploit symlinks (provide an example)? Provide at least one countermeasure.

Briefly describe at least two main services in Unix system that are often remotely attacked. For each of this services, explain how the remote attack occurs and discuss the possible countermeasure.

What are shared libraries in Unix? Describe the general advantages of shared libraries, and the possible Cybersecurity issues that they introduce. Assume that a root program called `program1`, which uses a shared library `libshared.so`, is executed every time at system startup. If libshared.so is not present in the system, under which conditions can you exploit this to run arbitrary code with root privileges? How would you do it?

Describe in detail the Unix permissions system. Explain at least one of the three special modes. What are the security implications of SUID? (clone)

Describe APT in the context of Unix systems. In particular, describe Trojan, sniffers, log cleaning and kernel rootkits, and briefly discuss some countermeasures for each of these points.

Describe in detail the UNIX permission system. Explain at least one of the three special modes. What are the security implications of SUID?

Symlink. What are symlinks and how do they work? How can an attacker exploit symlinks (provide an example)? Provide at least one countermeasure.

Briefly describe at least two main services in Unix Systems that are often remotely attacked. For each of these services explain how the remote attack occurs and discuss the possible countermeasures.

CH6

An ongoing APT attack has compromise one of the Windows server. With this assumption, how do you plan and implement the forensics activities for the analysis of this host? In particular describe the order in which the evidence should be collected and the forensics methodology, the tools, the command lines etc. to be used to analyze suspicious host.

Describe the six main steps that constitute an APT attack and indicate for each one the artifacts/traces that are usually left into the victim system. When detecting an APT attack, the tools used by the administrators may be compromised so as the return false information. Describe at least 8 of the 22 recommended checks.

Following a successful APT attack, in the phase of the forensic analysis which focuses on the filesystem of a Windows System, which interesting files should be collected to analyze the attacker activities? List at least three files. Registry keys and page/swap/hibernations files will not be considered valid answers. For each of the files you listed, describe its default location, the information it contains and which tools should be used for its analysis.

“Collecting Interesting Files” è il capitolo per rispondere a questa domanda

An ongoing Advanced persistent threat (APT) attack has compromised one of the Windows servers. With this assumption how do you plan and implement the forensics methodology, the tools, the command lines, etc. to be used, to analyze the “suspicious’ host.

CH7

VoIP Attacks. Describe VOIP Enumeration, Denial of Service and other attacks against VoIP. Which tools are used? Write console commands. Which countermeasures?

Describe at least three attacks to a VoIP network. Include in your description at least the activities to be carried out, the tools, and the command lines to be used. What are the possible countermeasures for each of these attacks? For example, one of the possible VoIP attacks is the enumeration of VoIP users (this attack will not be considered if you discuss it in your answer).

Attacchi VoIP. Mi sembra User enumeration.

Citrix vulnerabilities

VoIP attacks (no enum)

CH8

Deauthentication attacks.

Describe at least one method for attacking WPA. Which countermeasures can be used?

Describe at least one method to attack WPA Enterprise. What are the possible countermeasures?

Wireless interface sniffing

CH9

Explain what is Advanced Technology Attachment security mechanism. Describe the step of the attack which is able to bypass ATA security. How to defend against such a bypass?

Firmware reversing e wireless interface sniffing

Describe at least two techniques for hacking devices (hardware). In particular, describe the attacks against hardware devices that store sensitive informations.

CH10

Explain differences between Cross-Site scripting and Cross Site Request Forgery. Which countermeasures can be used?

Describe the SQL injection technique in web applications. Discuss the possible countermeasures. Describe at least one automated SQL injection tool.

What does it mean that the HTTP protocol is stateless? What limitations come from this fact? What are HTTP sessions and what are the major techniques to implement sessions? Describe in detail the functioning of at least one of these techniques.

What is a Blind SQLi? Make a concrete example.

CSRF, token e XSS (why anti-CSRF tokens don’t work as countermeasure if there is a XSS vulnerability).

What is a Cross Site Scripting (XSS) and what are its goals and causes? What types of XSS exist? Describe at least two types of XSS in detail.

Describe in detail Cross Site Request Forgery (CSRF). Provide one concrete attack example. What are CSRF tokens? How do they work?

Explain why blind SQLi is sometimes needed to exploit a SLQ injection vulnerability. How do you manually perform a blind SQLi? Describe a vulnerable scenario and provide a concrete example.

What is XSS and what are its goals and causes? What types of XSS exist? Describe at least two types of XXS in detail.

Describe in detail CSRF. Provide one concrete attack example. What are CSRF tokens? How do they work?

CSRF

CH11

Hacking Other Androids: Describe at least three methods to attack others Android devices. What are the possible countermeasures?

Can Linux security tools be ported to Android? Which tools? Write console commands.

Data Stealing, Capability leaks, URL Malware.

Four Android (>=3.0) security measures and if there are known exploits.

Describe the following attacks to Android devices: Capability Leaks, Carrier IQ, Cracking Google Wallet. What are the possible countermeasures?

Hacking Other Androids: Describe at least three methods to attack other Android devices. What are the possible countermeasures for these three attacks?

Hacking Other Androids: Describe at least two methods to attack others Android devices. What are the possible countermeasures?

Android 3.0 and later security features

Esercizi Pratici CH5 + CH10