Centro de
Investigación en
Computación

ISSAF

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Estándar
3. Reflexiones

Introducción

Definiciones

Introducción

Definiciones

ISSAF (*Information Systems Security Assessment Framework*)

- Fue creado por OISSG (*Open Information Systems Security Group*).
  - Draft v0.2.1, April 30, 2006.
  - El documento PDF tiene 845 páginas.
- Although it is no longer maintained and, therefore, a bit out of date, one of its strengths is that it links individual pentest steps with pentesting tools.
- It aims to provide a comprehensive guide in conducting a pentest and can be a good basis for developing your own custom methodology.

  - Las metodologías son genéricas así que al realizar un trabajo hay que explicar como la adecuamos a nuestro caso estudio.

Estándar

Descripción

Resumen

Estándar

Definiciones

ISSAF

- La metodología de Pentesting tiene 3 fases:

  Phase I. Planning and preparation

  Phase II. Assessment

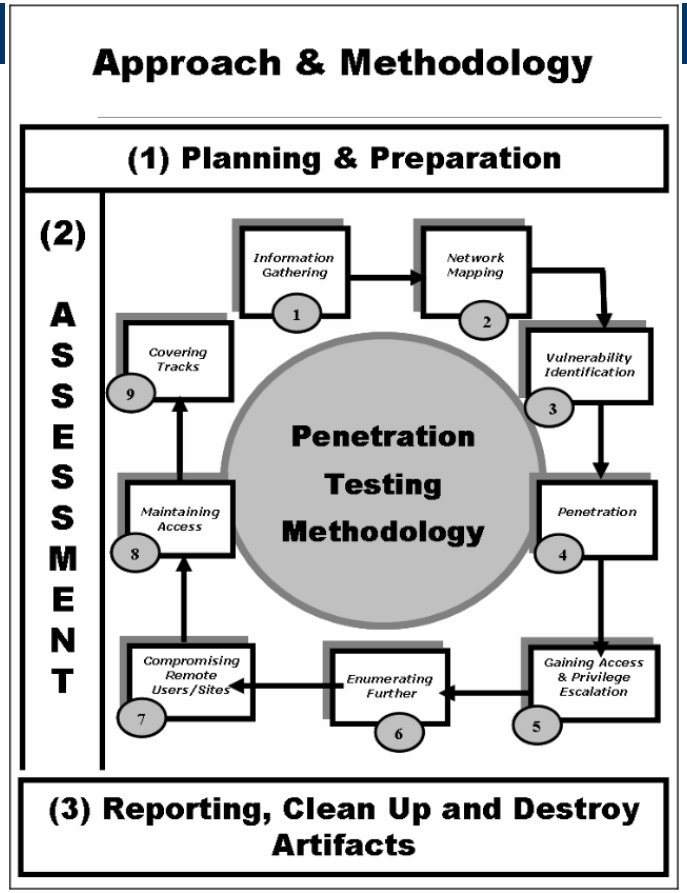
  Phase III. Reporting, clean-up and destroy artefacts

- Para la fase 3 hay 9 capas:
  1. Information Gathering
  2. Network Mapping
  3. Vulnerability Identification
  4. Penetration
  5. Gaining Access & Privilege Escalation
  6. Enumerating Further
  7. Compromise Remote Users/Sites
  8. Maintaining Access
  9. Covering Tracks.

Cada una de estas
Capas es ampliamente
Explicada en el documento

Estándar

Definiciones



Veamos ahora algunas de las capas

Estándar

Definiciones

1. Information Gathering

- Se divide en dos partes:
  1. Passive information gathering
  2. Active information gathering

Pasive 1.x

1. Locate the target Web presence
2. Examine the target using search engines
3. Search Web groups
4. Search employee personal Web sites
5. Search Security & Exchange Commission and finance sites
6. Search uptime statistics sites
7. Search system/network survey sites
8. Search on P2P networks
9. Search on Internet Relay Chat (IRC)
10. Search job databases
11. Search newsgroups (NNTP)
12. Gain information from domain registrar
    - Check for reverse DNS lookup presence
    - Check more DNS information
    - Check Spam database lookup
    - Check to change WHOIS information

1.1.1 Locate the Target Web Presence

Description

The first thing to do is to identify any online presence the target has using information from initial contacts, e.g. e-mails, business cards, brochures, leaflets, etc.

Following this, you can take your contact's e-mail address or the website from the business card and/or brochure to gather more data.

Process

- Find target in all common search engines (using business name)
- Find Web presence (you may have this from the e-mail address already)
- B2B – Web points of presence for business-to-business transactions (e.g. A partner portal)
- B2E – Web points of presence for business-to-enterprise communication (e.g. Web-enabled intranet site)
- B2C – Web points of presence for business to customer transaction (e.g. an e-commerce website)

Tips

Generally one will get the best results using various keyword combinations such as:

- Target name
- Location
- Industry
- Product type
- Product lines/names
- Contact names

Countermeasures

Have a policy describing what information should or should not be published on the public website.

Links

Watching the Watchers II, by j0hnny:
http://johnny.ihackstuff.com/security/premium/04-01-2003-Watching_the_Watchers_II-2.ppt

Tools

The best choices in most situations are:

Estándar

Definiciones

1. Information Gathering

- Se divide en dos partes:
  1. Passive information gathering
  2. Active information gathering

Active 2.x

1. Email Systems – User Account Enumeration
2. SMTP Headers Analysis
…
9. Mirror Target Web Site
10. Global Countermeasures

1.1.26 Mirror Target Web Site
Description
It is wise to use offline browser such as HTTrack or preferably Wget to completely mirror all target websites (including any personal websites located).
Process
▪ Grab the target website offline ▪ Understand the Web implementation logic and chart out the logical Web-tree ▪ Note down the webserver(s) and server banners, and version information ▪ Search the local Web-tree for all e-mail addresses and other useful information, particularly the pages in the job posting sub-branch ▪ Check for repetitive words in the Web-tree; one can build a user/password list from this information ▪ Use tools which can build effective dictionaries from Web pages (words commonly used on the website are likely passwords in the organization)
Analysis/Conclusion/Observation
Both an attacker and an assessor will review the information gathered through this technique. Review the source code of all pages for the following (refer: web application section): • Comments (e.g. username and password) • Database connectivity • Meta tags • Confidential information • Hidden fields • Search for keywords (e.g. "pass", "password", "server", "database", "login") • Web programming patterns (i.e. errors and vulnerabilities could repeat in several pages)
Countermeasures
To avoid critical information leaks, organizations should ensure that: • Comments in production web pages and applications do not include sensitive information • Confidential information should be separated in different repositories from public information. Access to this information should be restricted and controlled (e.g. single access path with authentication controls in place)

Estándar

Definiciones

2. Network Mapping

- Scanning, OS Fingerprinting and Enumeration:
  1. Identify Live Hosts
  2. Determine running Services
  3. Find Open Ports
     i. TCP Port Scanning
     ii. UDP Port Scanning
     iii. Banner grabbing
  4. ARP Discovery
  5. Identify Perimeter Network (Router / Firewalls)
     i. Scan default firewall/Router ports
     ii. Perform FIN/ACK scan
     iii. MAP Router
  6. Etc.

Pag. 108 de las 845

1.1.34 Operating System Fingerprinting

B.2.1.8 PASSIVE OS GUESSING

Description

By sniffing and comparing the Time To Live and Window Sizes, one can identify the remote operating system in use.

This can be easily accomplished by using p0f or by putting a protocol analyzer to listen to traffic, and then doing manual analysis of the traffic that is captured.

Process

Setup a sniffer or a passive fingerprinting tool (e,g, p0f) into listening mode. You will be able to collect information on O.S. brands on the local network directly (unless you are in a switched environment).

Also, you will be able to collect information from all machines or servers establishing a connection to your equipment or with those machines that you try to connect to.

If doing manual fingerprint, you will have to analyze manually the network packets captured, in order to identify the system, using several techniques (e.g. initial ttl in header, window size in header, response to overlapped packets, etc.).

Examples/Results

Using p0f for scanning incoming connections:

```
# p0f
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 231 sigs (13 generic), rule: 'all'.
192.168.1.101:1298 - Windows XP SP1, 2000 SP3 (2)
  -> 192.168.1.102:22 (distance 0, link: ethernet/modem)
192.168.1.102:2298 - Linux 2.5 (sometimes 2.4) (4) (up: 2 hrs)
  -> 10.1.1.1:80 (distance 0, link: ethernet/modem)
```

Using p0f for scanning responses to outgoing connections:

```
# p0f -A
p0f - passive os fingerprinting utility, version 2.0.5
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN+ACK) on 'eth0', 57 sigs (1 generic), rule: 'all'.
xxx.xxx.xxx.xxx:80 - FreeBSD 5.0 [high throughput] (up: 1411 hrs)
  -> 192.168.1.102:2945 (distance 12, link: sometimes DSL (3))
```

Analysis/Conclusion/Observation

Passive OS guessing will provide information on the O.S. brand and version. This information will be useful to tune active tests (e.g. vulnerability scanning).

Estándar

Definiciones

3. Vulnerability Assesment (Identification)

- Al igual que otras secciones tiene:
  1. Description
  2. Aim / Objetive
  3. Process
- 6 Steps:
  1. Identifying vulnerable services for known vulnerabilities
     Using service banners , O.S./service fingerprints, open ports and all relevant information from previous stages.
  2. Perform vulnerability scan by automated scanners for known vulnerabilities
  3. Identify un-disclosed vulnerabilities [Optional]
  4. Make a list of all vulnerabilities found
  5. Perform false positive and false negative verification
  6. Make a final list of vulnerabilities and recommend immediate measures

Estándar

Definiciones

9. Covering the tracks

- Actividades
  1. Hide files
     i. Hide Files (UNIX)
     ii. Hiding the files using rootkits.
     iii. Putting files into un-accessible directories
     iv. Hide Files (Windows)
  2. Clear logs
     i. Check history
     ii. Edit log files

Estándar

Definiciones

Problemas

1. Complejo para principiantes
2. Incompleto
3. Trae información de:
   - Herramientas que ya no existen.
   - Puertos usados por productos (podrian cambiar).

A pesar de lo anterior es bastante citado.

Recomendación

Usarlo como complemento con otros estándares.

E SWITCH SECURITY ASSESSMENT

E.1 DESCRIPTION

Switch and Layer 2 security is hardly considered in their implementation. In order to perform comprehensive security test, it is important to take the concept of security to the last step and ensure complete testing of switches and layer 2 in network. One hole is sufficient to expose corporate LAN security. An attacker doesn't need to attack higher layer if bottom layer can give access to him.

E.2 PURPOSE

[Text]

Write purpose of this document not purpose of device (e.g. Router, Firewall, IDS)

E.3 REQUIREMENT

[Text]

E.3.1 Understand Organization's environment

[Text]

E.3.2 Technical Requirements

[Text]

E.4 EXPECTED RESULT

[Text]

E.5 METHODOLOGY / PROCESS

[Text]

Brief Intro and Table of Contents

E.5.1 Assess General Switch Security

- Identify Switch's management interface IP
  - Using Discovery Protocol (CDP in case of Cisco)

Reflexiones

Trabajo a futuro

Lluvia de ideas

Reflexiones

Ideas

Si uno usa la terminología BPM se tiene:

Procesos
Subprocesos
Procedimientos

Y además hay diferentes tipos de procesos.

Si uno analiza este framework observaría:

1. Hay muchas macro actividades
2. Hay muchas sub-actividades
3. Para cada actividad hay que ejecutar varias herramientas (comandos). De hecho hay que instalar y configurar algunas.
4. Para cada actividad hay que capturar evidencias y generar reportes.
5. Para cada actividad hay que asignar roles: el que la realiza, el que revisa/ valida los resultados.
6. Hay varias personas que hacer la Administración de todo

Lo mismo pasa si uno reflexiona lo que pasa con los otros frameworks, estándars, etc.

Reflexiones

Ideas

¿Como facilitamos todo el trabajo?
¿Como automatizamos tareas?
¿Como hacemos cálculos al inicio para planear y para dar seguimiento?

1. Con archivos de office: Excel, plantillas.
2. Con aplicaciones: nativas o web.

¿Existe o creamos una ad-hoc?

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652