

RED TEAMS

Deel 2

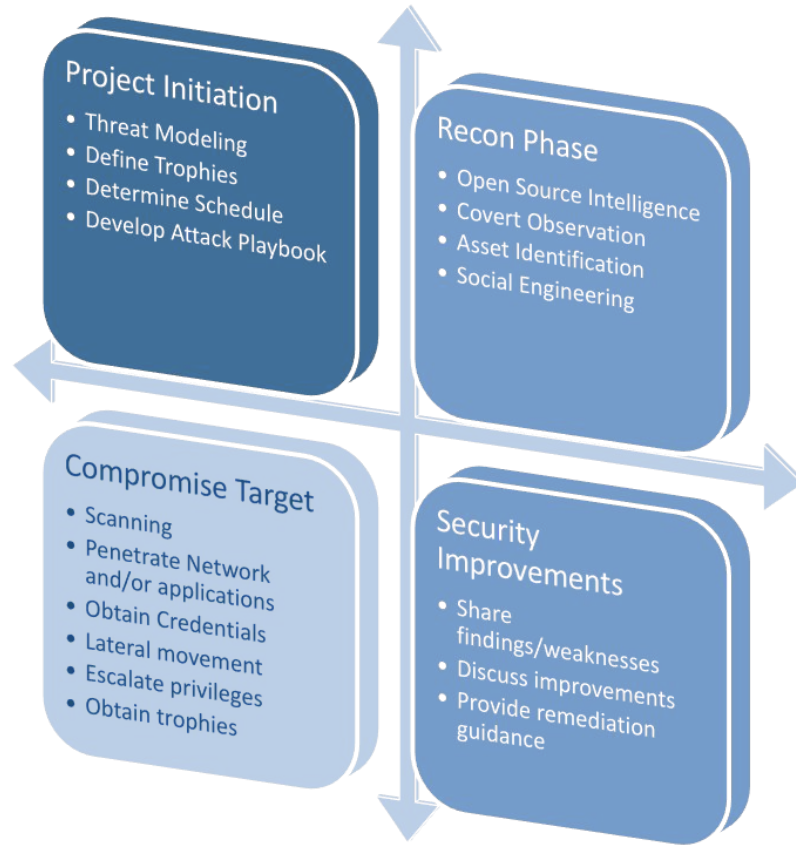






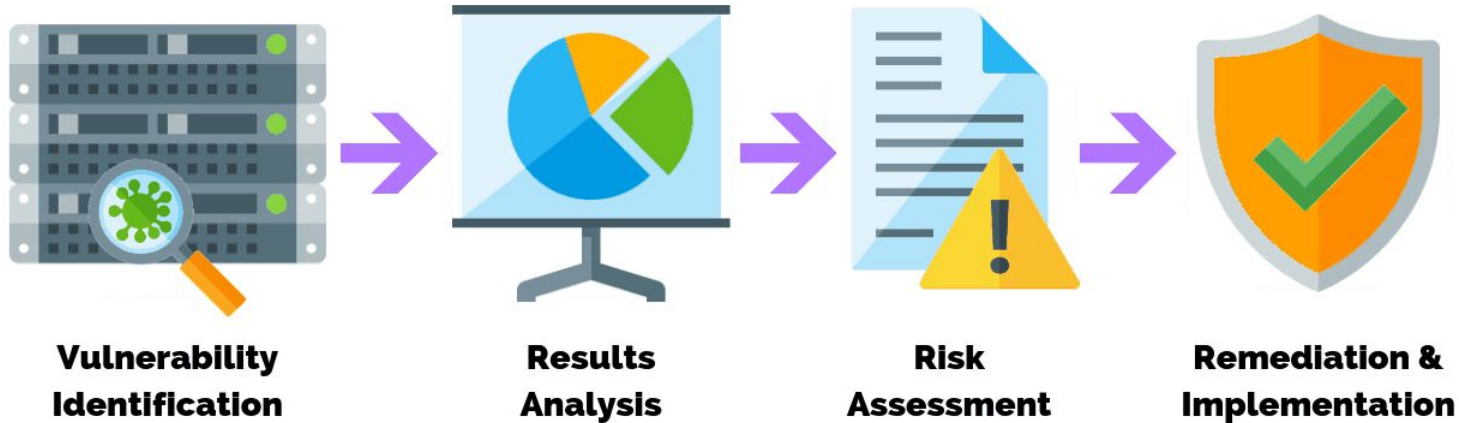
RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



VULNERABILITY ANALYSIS

Vulnerability testing is the **process of discovering flaws in systems and applications** which can be leveraged by an attacker.



VULNERABILITY ANALYSIS

Once a vulnerability has been reported in a target system, it is necessary to determine the accuracy of the identification of the issue, and to research the potential exploitability of the vulnerability within the scope of the penetration test.

Types of vulnerability analysis

- Active, e.g.
 - automated application scans
 - banner grabbing
 - network scans
- Passive (metadata analysis and traffic monitoring)



VULNERABILITY ANALYSIS

- Sample output (Acunetix)

Scan Results	Status
Scan Thread 1 (http://testphp.vulnweb.com:80/)	Finished (213 alerts)
Web Alerts (213)	
Blind SQL Injection (34)	
CRLF injection/HTTP response splitting (verifi...	
Cross site scripting (2)	
Cross site scripting (verified) (34)	
Directory traversal (verified) (2)	
HTTP parameter pollution (2)	
Script source code disclosure (1)	
Server side request forgery (2)	
SQL injection (4)	
SQL injection (verified) (38)	
/AJAX/infoartist.php (1)	
/AJAX/infocateg.php (1)	
/AJAX/infotitle.php (1)	
/artists.php (2)	
/cart.php (5)	
addcart (3)	
variant 1	
variant 2	
variant 3	
del (1)	
login (1)	
/guestbook.php (1)	
/listproducts.php (4)	

acunetix

WEB APP

SQL injection (verified)

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the injection occurs when web applications accept user input that is directly placed into a SQL statement and does dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects **/cart.php**.

Discovered by: Scripting (Sql_Injection.script).

AcuSensor
Technology

Vulnerability details

Source file: **/hj/var/www/cart.php** line: **81**

Additional details:

SQL query: `SELECT * FROM carts WHERE cart_id='10ebceb64152145d987c385c96080bea' AND item=1ACUSTART''8JFMGACUEND`
"mysql_query" was called.

Attack details

URL encoded POST input **addcart** was set to **1ACUSTART''8JFMGACUEND**

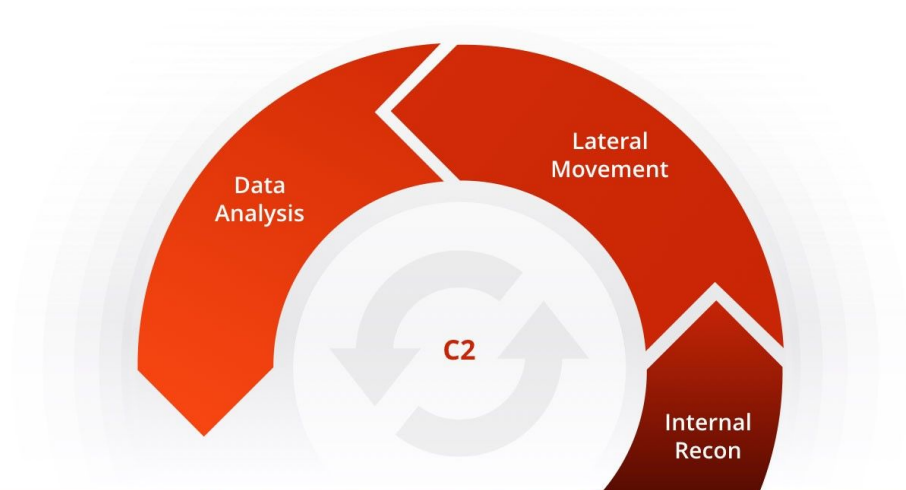
- View HTTP headers
- View HTML response
- Launch the attack with HTTP Editor
- Retest alert(s)
- Mark this alert as a false positive

The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system compromise. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, to execute additional queries. In some cases, it may be possible to read in or write out to files, or to execute commands on the underlying operating system.

Red Team Operations Attack Lifecycle



EXPLOITATION

Initial Compromise:
Abuse weaknesses found



EXPLOITATION

Initial Compromise:

Abuse weaknesses found, in the software (configuration)

Initial foothold

Once RCE,RFI or other compromise is found, try and get shell access through code:

Good cheatsheet: <http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

EXPLOITATION: ESTABLISH PERSISTENCE

persistence

/pə'sist(ə)ns/ 

noun

the fact of continuing in an opinion or course of action in spite of difficulty or opposition.

"Cardiff's persistence was rewarded with a try"

synonyms: **perseverance**, **tenacity**, **determination**, **resolve**, **resolution**, **resoluteness**, **staying power**, **purposefulness**, **firmness of purpose**, **patience**, **endurance**, **application**, **diligence**, **sedulousness**, **dedication**, **commitment**, **doggedness**, **persistence**, **pertinacity**, **assiduity**, **assiduousness**, **steadfastness**, **tirelessness**, **indefatigability**, **stamina**; **More**

- the continued or prolonged existence of something.
"the persistence of huge environmental problems"



Find a safe hiding spot

EXPLOITATION: ESTABLISH PERSISTENCE

Example for a php web application:

WSO PHP Shell - hide it in an accessible web directory

The screenshot displays the WSO PHP Shell interface. At the top, system information is shown: Username: Linux lamp 4.15.0-47-generic #50-Ubuntu SMP Wed Mar 13 10:44:52 UTC 2019 x86_64 [Google] [Exploit-DB]; User: 33 (www-data); Group: 33 (www-data); Php: 7.2.15-0ubuntu0.18.04.2 Safe mode: OFF [phpinfo]; Datetime: 2019-04-14 22:02:49; Hdd: 15.68 GB Free: 9.27 GB (59.09%); Cwd: /var/www/html/ drwxr-xr-x | home |. On the right, network information is displayed: Server IP: 10.0.2.15, Client IP: 192.168.56.1, and a UTF-8 encoding indicator.

Below the system info is a navigation bar with tabs: [Back] [Home] [Upload] [Download] [Files] [Info] [Php] [Safe mode] [Setting tools] [Shell data] [Network] [Logout] [Add remove].

The main section is titled "File manager" and contains a table with columns: Name, Size, Modify, Owner/Group, Permissions, and Actions. The table lists various files and directories, including core, drupal-8.5.0, modules, new_folder, profiles, sites, themes, vendor, composer.json, composer.lock, diy.php, hello.sh, index.php, LICENSE.txt, README.txt, robots.txt, simple1.php, simple2.php, simple3.php, web.config, weeveily.php, and wso.php.

At the bottom, there are four sections for file operations: "Copy" with a submit button, "Change dir:" with a text input field containing /var/www/html/ and a submit button, "Read file:" with a submit button, and "Make dir: [Writeable]" with a submit button. There are also buttons for "Make file: [Writeable]", "Execute:", "Upload file: [Writeable]", and a "Browse..." button.

EXPLOITATION: ESTABLISH PERSISTENCE

EXAMPLE FOR WINDOWS WORKSTATION

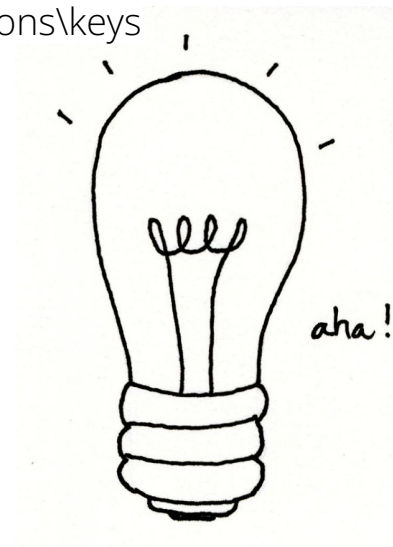
Meet Office Trusted locations!

HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\Trusted Locations\keys

Did you know?

When placed in a trusted location, Office Templates will automatically execute...




And template directories are a Trusted location by default












EXPLOITATION: ESTABLISH PERSISTENCE

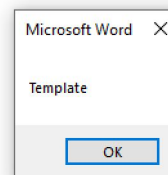
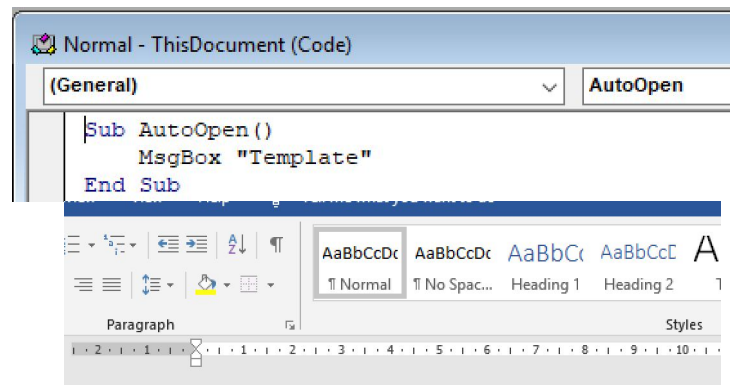
EXAMPLE FOR WINDOWS WORKSTATION

crosoft\Office\16.0\Word\Security\Trusted Locations\Location0

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 Description	REG_SZ	0
 Path	REG_EXPAND_SZ	%APPDATA%\Microsoft\Templates

AppData > Roaming > Microsoft > Templates >

Name	Date modified	Type	Size
 Document Themes	04/04/2019 20:41	File folder	
 LiveContent	17/11/2018 17:02	File folder	
 SmartArt Graphics	19/11/2018 10:39	File folder	
 ~\$Normal.dotm	03/12/2018 21:20	Microsoft Word M...	1 KB
 Bring your presentations to life with 3...	09/01/2019 21:44	Microsoft PowerP...	4,041 KB
 Formula tutorial(2).xlsx	14/02/2019 20:45	Microsoft Excel Te...	487 KB
 Formula tutorial.xlsx	21/09/2018 00:11	Microsoft Excel Te...	488 KB
 Get more out of PivotTables.xlsx	21/09/2018 00:12	Microsoft Excel Te...	430 KB
 Normal.dotm	04/04/2019 22:35	Microsoft Word M...	16 KB



EXPLOITATION: PRIVILEGE ESCALATION

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

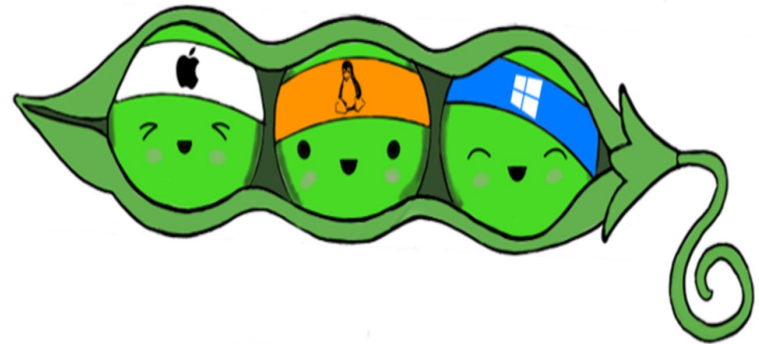
Windows Local privilege escalation explained in 10mins: <https://www.youtube.be/DllyKgfkOQ>

Linux Local privilege escalation explained in 20mins: <https://youtu.be/oYHAI0cgur4>

Tools:

<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite>

<https://github.com.cnpmjs.org/DominicBreuker/pspy>



EXPLOITATION: TOOLS



The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

POST-EXPLOITATION

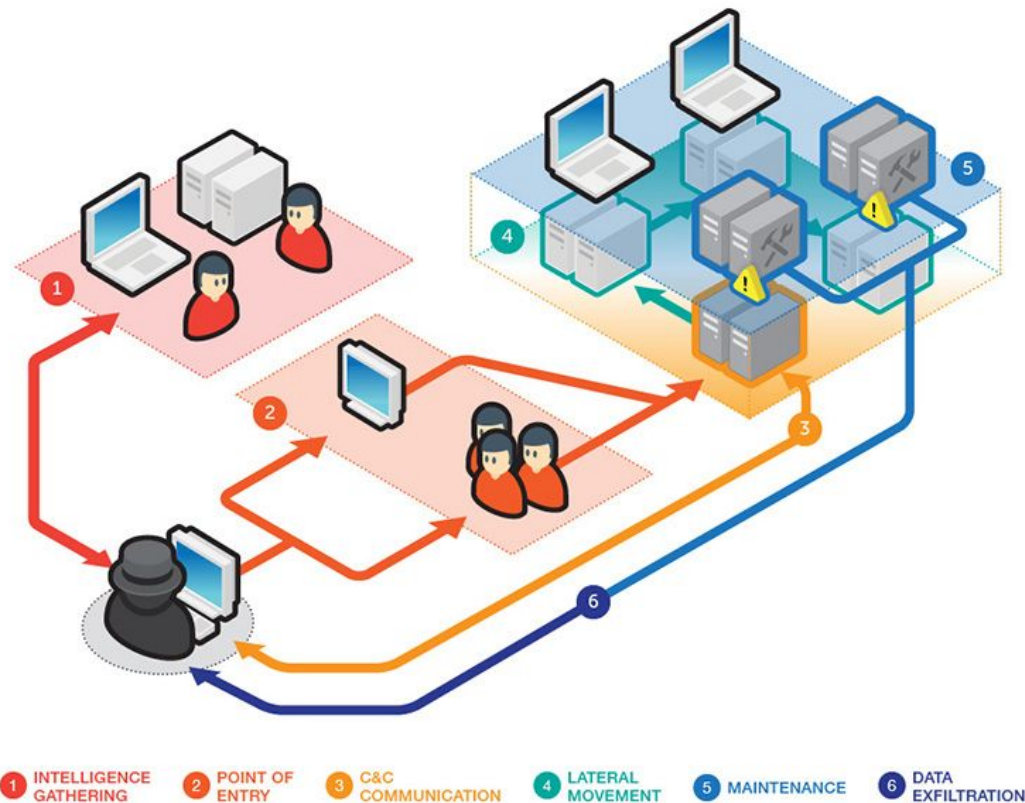
The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network.

- Infrastructure Analysis (for potential targets deeper in the network)
- Pillaging (e.g. personal information, credit card information, passwords, etc.)
- Data Exfiltration
- Persistence (e.g. installation of backdoor or creating an alternate user account)
- Cleanup (after the penetration test has been completed)

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

POST-EXPLOITATION: DO IT AGAIN!

Lateral movement within the network is needed most of the time, reiterate the previous steps by doing internal recon, vulnerability analysis and exploitation/ post-exploitation until you've reached your goal.



REPORTING

Reporting is done in most all cases either to external clients or internal bosses/teams. The report is broken down into two (2) major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.

1. Executive Summary: Specific goals of the Penetration Test and the high level findings of the testing exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization which may be impacted by the identified/confirmed threats.

The Penetration Testing Execution Standard, used under GNU Free Documentation License 1.2

REPORTING

2. Technical Report

Help your team getting better, guide others through findings and help make improvements (in case of friendlies)

Learn to make good reports!

Make sure everyone understands what/how it works!

Title

- Vulnerability type
- Domain
- How
- “Reflected XSS in example.com/profiles via name parameter”

Description

- General information of the vulnerable endpoint or component.
- Vulnerability type found
- The causes of vulnerability

Reproduction

- 1.
- 2.
- 3.
- ...

Attack Vector/Payload (Usually included in Reproduction)

- Tools and commands used to perform the attack

Exploitability

- Attack cases and conditions

Impact

- What attacker can do as a result of the vulnerability

Recommendation (Optional)

- How to fix the vulnerability

Reference (Optional)

- External sites related to the vulnerability

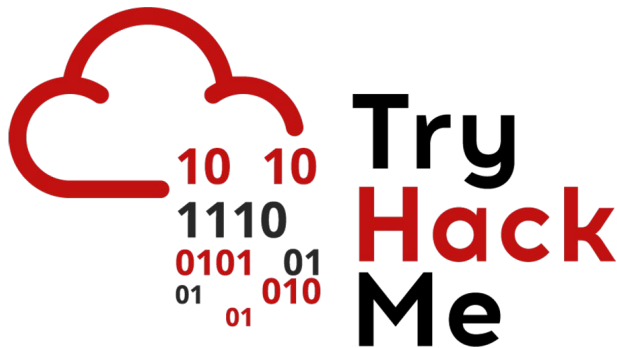
Now you try!

<https://tryhackme.com/room/vulniversity>

Guided from Boot to Root!

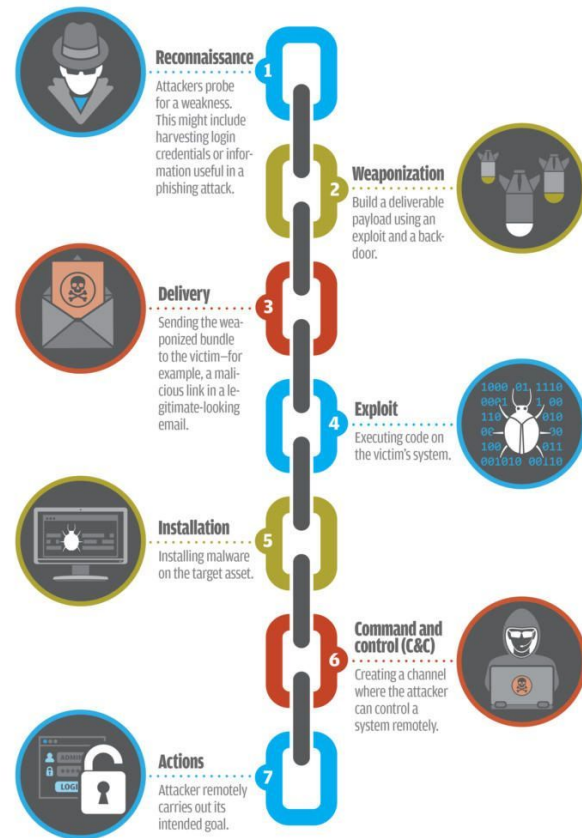
Vergelijkbaar met HackTheBox, maar met iets meer educatieve, guided, content. Ook iets meer boxen om specifieke dingen uit te leggen, in deze bvb: nmap, Burpsuite, Priv Esc dmv SUID.

(Met extra walkthroughs, dus geen ENKELE reden om het niet te proberen!)



What is the **CYBER KILL CHAIN**?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.



PLURALSIGHT VIDEOS



PLURALSIGHT

Pluralsight video: [link](#)

Relevant : Introduction to Pen Testing using Metasploit

Pluralsight video: [link](#)

Relevant : Exploiting & Post-Exploiting with Metasploit

Pluralsight video: [link](#)

Relevant : Web Application Penetration Testing Fundamentals

