NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 51: Metasploit Framework

CONCEPTS COVERED

- Metasploit Framework and Modules
- Metasploit Commands

Metasploit Framework

- Metasploit is a penetration testing platform/exploitation and vulnerability validation tool.
- It is one of the most useful security auditing tool since it contains information-gathering tools, web vulnerability plugins, modules, and an exploit development environment.
- It is available in Kali Linux and can be installed in Windows/Linux/MacOS.
- Two versions of Metasploit are available: *free* and *pro* version.

Metasploit Modules

- Metasploit contains a collection of various tools that are divided in terms of modules.
- The modules are:
  a) Exploits
  b) Payloads
  c) Auxiliary
  d) Encoder
  e) Nops
  f) Post

(a) Metasploit : Exploit Module

- **Exploit**: A piece of codes that is made to take advantage of System/Application bugs.
- It is the basic module in Metasploit which is used to take advantage of vulnerability available in a target system.
- Over 2000 exploits are available with this module that can be used to exploit Windows/Linux/Android/Mac operating systems.

(b) Metasploit : Payload Module

- Payload module consist over 500 payloads (malicious codes) that are used to establish communication channel between Metasploit framework and target system.
- The most common payloads are:
  - **Command shell**: helps to run collection of scripts or arbitrary commands against the host/target system.
  - **Meterpreter**: enables users to control the screen of a device using VNC and to browse, upload and download files.
  - **Dynamic payloads**: enable users to evade anti-virus defense by generating unique payloads.
  - **Static payloads**: enable static IP address/port forwarding to communicate between host and client systems.

(c) Metasploit : Auxiliary Module

- This is an additional module that can perform brute force attack, DoD attack, host and port scanning, vulnerability scanning, etc.
- It cannot give control to user system like exploits and payloads; however, it is very powerful for performing scanning and brute forcing.
- Over 1000 auxiliary codes are available with Metasploit auxiliary module.

(d) Metasploit : Encoder Module

- This module is used to bypass the anti-virus installed in target system.
- Anti-virus searches for bad hexadecimal codes to identify good and bad applications/program.
- Encoder module allow us to encode the payloads to avoid detection of bad codes.
- Over 45 encoding schemes are available with Metasploit encoder module.

(e) Metasploit : POST and NOPS Modules

- **NOPS**: This module helps to prevent the payload from crashing.
  - It provides additional support to payloads, e.g. if the payload is blocked by some applications then it generates a no-operation instructions for that payload.
- **POST**: This module is used to perform deeper penetration testing once the attacker is already accessing the target system.

Metasploit Modules

- Metasploit also consist of other modules such as *msfvenum* (environment to create new payloads), *msfconsol* (provide user interface for Metasploit), etc.
- It is written (everything including exploits and paylodes) in Ruby programming language.

Basic Steps Followed in Metasploit

- Scan the target system and find vulnerability (can be done using NMAP or using Metasploit auxiliaries).
- Pick which exploit to used based on the vulnerability found in target system.
- Configure exploit (i.e. set target IP, port number, etc.).
- Pick a payload to place in target system.
- Encode the payload.
- Execute the exploit.

Metasploit Commands

- All the commands can be found using *help* option. Some of the basic commands are listed here.
  - **Info**: Display information about modules/exploits/payloads (e.g. suitable OS, vulnerabilities, required configurations: i.e port number, host address etc).
  - **Use**: It selects a module/exploit/payload by name that we want to use.
  - **Show**: It lists all files inside a module in alphabetical order.
  - **Search**: Search exploits/payloads.

Metasploit Pros and Cons

- **Pros**
  - Open source
  - Frequent update
  - Huge community for help
- **Cons**
  - Too complex for beginners
  - Can crash systems if not used wisely (do not try in personal systems)
  - Requires deep knowledge

Demonstration: Metasploit Framework and its Modules

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 52: Miscellaneous Demonstrations

CONCEPTS COVERED

- Social Engineering using Metasploit
- Getting Windows Shell and Create Folder
- Password Dump from Target System

Demonstration: attacks using Metasploit framework

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 53: Webserver Vulnerability and Attacks

CONCEPTS COVERED

- Webserver Vulnerability Scanning
- SQL Injection Attacks

Webserver Vulnerability Scanning

- Web server is a program (both hardware and software) that hosts websites; attackers usually target software vulnerabilities and configuration errors to compromise web servers.
- Nowadays, network and OS level attacks can be well defended using proper network security measures such as firewalls, IDS, etc.
- However, web servers are accessible from anywhere on the Internet, which makes them less secured and more vulnerable to attacks.

Webserver Attacks

- Vulnerabilities in applications running on a webserver provide a broad attack path for webserver compromise.
- Following types of attacks can be done on webservers:
  - SQL Injection Attacks
  - Session Hijacking
  - Buffer Overflow Attacks
  - Cross-Site Scripting (XSS) Attacks
  - Denial-of-Service (DoS) Attacks
  - And many more.

Webserver Attacking Tools

- Many tools are available for vulnerability detection and assessment for webservers.
- Some of these tools are:
  - Metasploit
  - Hydra
  - dirb
  - SQLMAP
  - Acunetix
  - And many more

SQL Injection and SQL Injection Attack

- SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database.
  - It is a basic attack used to either gain unauthorized access to a database or to retrieve information directly from the database.
  - They do not exploit a specific software vulnerability, instead they target websites that do not follow secure coding practices for accessing and manipulating data stored in a relational database.

Impact of SQL Injection

- Information Disclosure
- Reputation Decline
- Compromised Data Integrity
- Compromised Availability of Data
- Denial of Service

Types of SQL Injection

- **Error Based SQL Injection:**
  - Attackers intentionally insert bad input into an application, causing it to throw database errors. The attacker then analyzes the database-level error messages that result in order to find an SQL injection vulnerability.
  - This exploitation may differ from one DBMS to the other.
- **Example**:
  - *error-based*: use errors to extract the data.
  - *UNION query-based*: combine a valid and invalid sql query
  - *stacked queries*: inject multiple sql queries in one go

Types of SQL Injection (contd.)

- **Blind SQL Injection:**
  - Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response.
  - This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
- **Example:**
  - *Boolean-based blind*: Analyze sql query output char by char (one by one).
  - *time-based blind*: The output of sql query is analyzed by time (how much time for one word password, how much time for two word etc.).

Demonstration: Web Application Vulnerability Scanning, Password Cracking

Demonstration: SQL Injection Attack

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 54: SQL MAP

CONCEPTS COVERED

- SQLMAP Tool and Commands

SQL MAP Tool

- SQLMAP is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
- SQLMAP supports almost all types of databases such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, IBM DB2, SQLite.
- Full support for all SQL injection techniques.
- It can extract information of database servers such as users, password hashes, privileges, roles, databases, tables and columns.

Feature of SQL MAP

- Can dump the entire database table.
- Connect database directly without passing any sql injection query (using IP address).
- Detect the flaw of database (any sql injection vulnerability).
- Allows search for specific database names, specific tables across all databases or specific columns across all database tables.
- Support for database process user privilege escalation via Metasploit's Meterpreter *getsystem* command.

SQL MAP Workflow

1. Find vulnerability
2. Identify possible injection points
3. Identify SQL injection vulnerabilities by using SQLMAP
4. Exploit SQL injection vulnerabilities

Some SQLMAP commands

- **--current-user**: recover session user
- **--current-db**: detect current database
- **--is-dba**: find if the current user is database administrator
- **--dbs**: list all database
- **--hostname**: get dbms server name
- **-f**: produces dbms version, OS information , architecture and patch level information

Some SQLMAP commands (contd.)

- **--user**: list all users of the database
- **--passwords**: list all users along with hashed password
- **--privileges**: list users with privilages
- **--sql-shell**: sql shell to execute your custom sql query
- **-D**: database name
- **-T**: table name
- **-C**: column name
- **--dump**: dump database table entries

Demonstration: SQLMAP Tool, exploiting SQL injection vulnerability using SQL MAP

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!

NPTEL ONLINE CERTIFICATION COURSES

Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering

Topic

Lecture 55: Cross Site Scripting

CONCEPTS COVERED

- Cross Site Scripting (XSS)
- Various types of XSS

Cross Site Scripting (XSS)

- Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into websites.
- XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.
- Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Cross Site Scripting (XSS)

- An attacker can use XSS to send a malicious script to an unsuspecting user.
- The end users browser has no way to know that the script should not be trusted, and will execute the script.
- Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.
- These scripts can even rewrite the content of the HTML page.
- XSS attacks can be categorized in three types: **stored**, **reflected** and **DOM based**.

(a) Stored XSS (Persistent or Type I)

- Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, etc.
- When victim tries to retrieve the stored data from the target server then it receives a malicious data, and the browser cloud also does not identify it as a malicious as it comes from a trusted source.
- **Example**: for any feedback form an attacker can submit an malicious code/payload and once the admin will open the feedback the payload will get executed.

(b) Reflected XSS or (Non-Persistent or Type II)

- Reflected XSS occurs when user input is immediately returned by a web application in an error message, search result, or any other response that includes some or all of the input provided by the user as part of the request.
- Reflected attacks are delivered via other approaches than user input such as email.
- When user clicks on the file then the payload is delivered to victim system.

(c) DOM Based (Type 0)

- In DOM Based XSS the entire tainted data flow from source to sink takes place in the browser.
  - The source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser.
- **Example**: the source (where malicious data is read) could be the URL of the page (e.g., *document.location.href*), or it could be an element of the HTML, and the sink is a sensitive method call that causes the execution of the malicious data (e.g., *document.write*).”

Types of XSS

- The three different types of XSS can overlap.
  - We can have both Stored and Reflected DOM Based XSS.
  - We can also have Stored and Reflected Non-DOM Based XSS too, but that's confusing.
- For this research community proposed and started using two new terms to help organize the types of XSS that can occur:
  - **Server XSS**
  - **Client XSS**

(a) Server XSS

- Server XSS occurs when untrusted user supplied data is included in an HTTP response generated by the server.
- The source of this data could be from the request, or from a stored location.
- As such, we can have both *Reflected Server XSS* and *Stored Server XSS*.
- In this case, the entire vulnerability is in server-side code, and the browser is simply rendering the response and executing any valid script embedded in it.

(b) Client XSS

- This occurs when untrusted user supplied data is used to update the DOM with an unsafe JavaScript call.
  - A JavaScript call is considered unsafe if it can be used to introduce valid JavaScript code into the DOM.
  - The source of this data could be from the DOM, or it could have been sent by the server (via an AJAX call, or a page load).
  - The ultimate source of the data could have been from a request, or from a stored location on the client or the server.
- As such, we can have both *Reflected Client XSS* and *Stored Client XSS*.

Demonstration: Cross Site Scripting

Demonstration: Attack using Malicious Files, Command Injection Attack

Counter Measures

- Keep webserver software patch updated.
- Block unsigned applets.
- Disable client-side scripting.
- Disable cookies.
- Use proxy servers for content filtering.
- Do not install scripting languages on web servers.
- Deny access from known malicious domains.
- Redirect malicious requests to pages with legal warnings.

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

Thank you!