JANUARY, 2024

METASPLOIT ESSENTIALS

EVERYTHING THAT YOU NEED

VIEH GROUP

AKASH BASFOR

Exploitation:

Command: `use exploit/[exploit_name]`
Description: Selects an exploit module for a specific vulnerability.
Tactic: Identify target vulnerabilities and choose appropriate exploits.

Payload Generation:

Command: `generate -t [payload_type]`
Description: Generates a payload for various platforms.
Tactic: Create custom payloads for specific evasion and targeting.

Post-Exploitation:

Command: `post/multi/manage/shell_to_meterpreter`
Description: Transforms a shell session into a more powerful Meterpreter session.
Tactic: Upgrade to Meterpreter for advanced post-exploitation capabilities.

Lateral Movement:

Command: `use post/windows/manage/psexec`
Description: Executes commands on remote Windows systems using PsExec.
Tactic: Move laterally within a network by leveraging existing credentials.

Exploit Database Integration:

Command: `db_import [path_to_nmap_results]`
Description: Imports Nmap scan results into the Metasploit database.
Tactic: Leverage the database for targeted and efficient exploitation.

Resource Scripting:

Command: `resource [script_path]`
Description: Executes a series of Metasploit commands from a script.
Tactic: Automate repetitive tasks and complex attack scenarios.

AV Evasion:

Command: `generate -t [payload_type] -e [encoder]`
Description: Encodes payloads to evade antivirus detection.
Tactic: Bypass security measures by obfuscating payloads.

Brute Forcing:

Command: `use auxiliary/scanner/ssh/ssh_login`
Description: Brute force SSH credentials using a specified wordlist.
Tactic: Gain unauthorized access through credential guessing.

Client-Side Exploitation:

Command: `use exploit/windows/browser/[exploit_name]`
Description: Targets client-side vulnerabilities in web browsers.
Tactic: Exploit user interactions to gain access.

Pivoting:

Command: `set route [subnet] [session_id]`
Description: Enables routing through a compromised host to reach other subnets.
Tactic: Maintain access and move laterally across segmented networks.

Evidence Collection:

Command: `post/multi/gather/arp_scanner`
Description: Collects ARP tables from compromised hosts..
Tactic: Gather network information for further analysis.

Reporting:

Command: `db_export -f [format] -a [path]`
Description: Exports scan results and exploit data from the Metasploit database.
Tactic: Prepare comprehensive reports for stakeholders.

DNS Spoofing:

Command: `use auxiliary/spoof/dns/nbns_response`
Description: Spoofs NetBIOS Name Service (NBNS) responses.
Tactic: Redirect traffic for credential theft or man-in-the-middle attacks.

Web Application Testing:

Command: `use auxiliary/scanner/http/dir_scanner`
Description: Scans for directories on a web server.
Tactic: Identify hidden paths and potential vulnerabilities in web applications.

Database Exploitation:

Command: `use auxiliary/scanner/mssql/mssql_login`
Description: Brute force MS SQL Server credentials.
Tactic: Exploit weaknesses in database security.

Social Engineering Toolkit Integration:

Command: `use auxiliary/spoof/phishing_set`
Description: Integrates with the Social Engineering Toolkit for phishing campaigns.
Tactic: Simulate real-world social engineering attacks.

Wireless Network Exploitation:

Command: `use auxiliary/scanner/wifi/wifi_login`
Description: Attempts to crack Wi-Fi passwords.
Tactic: Gain unauthorized access to wireless networks.

File Format Exploitation:

Command: `use exploit/windows/fileformat/[exploit_name]`
Description: Exploits vulnerabilities in file formats (e.g., PDF, Office documents).
Tactic: Target users through malicious files.

Credential Sniffing:

Command: `use post/windows/gather/credentials/gpp`
Description: Extracts plaintext passwords from Group Policy Preferences (GPP).
Tactic: Retrieve stored credentials for lateral movement.

Meterpreter Scripting:

Command: `meterpreter > run post/windows/manage/killav`
Description: Executes Meterpreter scripts for specific tasks (e.g., disabling antivirus).
Tactic: Automate post-exploitation actions.

PowerShell Payloads:

Command: `use exploit/windows/local/payload`
Description: Generates payloads for PowerShell exploitation.
Tactic: Exploit Windows systems using PowerShell.

Exploiting IoT Devices:

Command: `use exploit/linux/iot/[exploit_name]`
Description: Targets vulnerabilities in Internet of Things (IoT) devices.
Tactic: Exploit weak security in IoT ecosystems.

Automated Target Reconnaissance:

Command: `use auxiliary/scanner/http/ssl_certificate`
Description: Collects SSL certificate information from web servers.
Tactic: Automate reconnaissance for SSL/TLS vulnerabilities.

Anti-Forensics:

Command: `use post/windows/manage/timestomp`
Description: Modifies file timestamps to evade forensic analysis.
Tactic: Cover tracks during and after exploitation.

Bypassing UAC (User Account Control):

Command: `use exploit/windows/local/bypassuac`
Description: Exploits vulnerabilities to bypass UAC on Windows systems.
Tactic: Elevate privileges and execute code with higher permissions.

Token Impersonation:

Command: `use incognito`
Description: Provides commands for token manipulation and privilege escalation.
Tactic: Mimic higher-privileged users for lateral movement.

Exploiting MS17-010 (EternalBlue):

Command: `use exploit/windows/smb/ms17_010_eternalblue`
Description: Exploits the EternalBlue vulnerability for remote code execution on Windows systems.
Tactic: Target unpatched Windows systems for rapid compromise.

Fingerprinting Services:

Command: `use auxiliary/scanner/fingerprint/[service]`
Description: Fingerprinting services to gather information about their versions and configurations.
Tactic: Understand target services for precise exploitation.

Automated Credential Harvesting:

Command: `use post/windows/gather/credentials`
Description: Collects credentials from compromised Windows systems.
Tactic: Harvest passwords for lateral movement and privilege escalation.

Automated Password Cracking:

Command: `use auxiliary/analyze/jtr_crack_fast`
Description: Analyzes John the Ripper output to crack password hashes.
Tactic: Crack password hashes for credential access.

Exploiting Web Application Vulnerabilities:

Command: `use exploit/multi/http/[exploit_name]`
Description: Targets vulnerabilities in web applications.
Tactic: Exploit weaknesses in web services for unauthorized access.

AV Evasion with Veil-Framework:

Command: `use evasion/windows/`
Description: Generates payloads with the Veil-Framework to evade antivirus detection.
Tactic: Enhance payload obfuscation for better success rates.

SNMP Enumeration:

Command: `use auxiliary/scanner/snmp/snmp_enum`
Description: Enumerates information from SNMP-enabled devices.
Tactic: Gather details for network mapping and potential vulnerabilities.

WiFi Pineapple Integration:

Command: `use auxiliary/gather/wifi/pineapple`
Description: Integrates with the WiFi Pineapple for wireless network reconnaissance.
Tactic: Gather information about WiFi networks and connected devices.

VoIP Exploitation:

Command: `use auxiliary/voip/`
Description: Exploits vulnerabilities in Voice over IP (VoIP) systems.
Tactic: Target weaknesses in communication infrastructure.

Windows Management Instrumentation (WMI) Exploitation:

Command: `use exploit/windows/wmi/`
Description: Exploits vulnerabilities using Windows Management Instrumentation.
Tactic: Leverage WMI for post-exploitation activities.