infiltrator squad

PENETRATION TESTING

DC-1

infiltrator squad

ABOUT DC-1

DC-1 is a purposely built vulnerable lab to gain experience in the world of penetration testing.

It was designed to be a challenge for beginners, but just how easy it is will depend on your skills and knowledge, and your ability to learn.

To complete this challenge, you will require Linux skills, familiarity with the Linux command line, and experience with basic penetration testing tools, such as the tools that can be found on Kali Linux, or Parrot Security OS.

There are multiple ways of gaining root, however, I have included some flags which contain clues for beginners.

There are five flags in total, but the ultimate goal is to find and read the flag in the root's home directory. You don't even need to be root to do this, however, you will require root privileges.

Depending on your skill level, you may be able to skip finding most of these flags and go straight for root.

Beginners may encounter challenges that they have never come across previously, but a Google search should be all that is required to obtain the information required to complete this challenge

PLANNING & RECONNAISSANCE

This phase involves gathering information about the target to understand what vulnerabilities might exist.

Tools:Nmap

Description: Nmap (Network Mapper) is a popular open-source tool used for network discovery and security auditing. It helps in identifying hosts, open ports, services, operating systems, and more.
Role in Reconnaissance: Nmap is often used during this phase to discover live hosts on a network, identify open ports, and gather service and version information. This information is critical for planning the next steps of the penetration test.

Tools:Droopescan

Droopescan:

Description: Droopescan is a CMS scanner that focuses on Drupal, SilverStripe, WordPress, and other CMS platforms to identify potential vulnerabilities.
Role in Reconnaissance: Droopescan can be used to enumerate installed components, versions, and potential misconfigurations in a CMS, providing useful insight for later exploitation.
Phase 2: Scanning & Enumeration
This phase involves scanning the target for vulnerabilities and identifying entry points.

SCANNING & ENUMERATION

This phase involves scanning the target for vulnerabilities and identifying entry points.

Tools:Nmap(again)

Description: As mentioned, Nmap can also be used for more specific scanning and enumeration purposes, such as version scanning and script-based vulnerability detection.
Role in Scanning: During this phase, more aggressive scans can be run, including service version detection, OS fingerprinting, and specific vulnerability scans (e.g., using Nmap scripts for known vulnerabilities)

Tools:Droopescan(again)

Description: As mentioned earlier, Droopescan provides information about the CMS components, versions, and any vulnerabilities.
Role in Enumeration: After identifying a CMS, Droopescan will enumerate all the installed plugins and themes, check for outdated versions, and list any known vulnerabilities that could be exploited.
Phase 3: Exploitation & Gaining Access
This phase focuses on exploiting vulnerabilities to gain access to the target system.

EXPLOITATION&GAINING ACCESS

This phase focuses on exploiting vulnerabilities to gain access to the target system.

Tools:Metasploit

Description: Metasploit is a comprehensive exploitation framework that simplifies the process of developing and executing exploits against targets. It contains a database of pre-built exploits for various vulnerabilities.
Role in Exploitation: Metasploit is commonly used to exploit vulnerabilities discovered during earlier phases. You can select an exploit based on the information gathered (e.g., open ports, services, or CMS vulnerabilities), configure it, and launch the attack.

Tools:Searchsploit

Description: Searchsploit is part of the Exploit-DB project and provides access to a repository of publicly available exploits and proofs of concept. It allows you to search for specific exploits directly from your terminal.
Role in Exploitation: After identifying a vulnerable service, you can use Searchsploit to find an appropriate exploit for it. You can download the exploit code from Exploit-DB and manually execute it or import it into a tool like Metasploit.

Tools:Exploit

Description: An exploit is any code or method that takes advantage of a vulnerability to gain unauthorized access to a system.
Role in Exploitation: Once a vulnerability is identified, an exploit tailored for that vulnerability can be used to gain access to the target. Exploits can be found manually, developed custom for a target, or sourced from databases like Searchsploit.

MAINTAININGACCESS &PRIVILEGE ESCALATION

After gaining access, the next goal is to maintain persistence and potentially escalate privileges to gain deeper control over the system.

Tools:Meterpreter

Description: Meterpreter is a payload within the Metasploit Framework that provides an interactive shell, allowing an attacker to execute commands and scripts remotely. It also supports features like pivoting, persistence, and privilege escalation.
Role in Maintaining Access: After exploitation, Meterpreter can be used to maintain control over the target system. It allows an attacker to hide their presence, maintain access (through persistence techniques), and escalate privileges (using available scripts).
Privilege Escalation: Meterpreter has built-in tools that help to escalate privileges, such as exploiting sudo misconfigurations, kernel vulnerabilities, or weak file permissions.

Tools:Metasploit (again)

Description: Metasploit's post-exploitation modules can be used to establish persistence (e.g., adding a backdoor), escalate privileges, or pivot to other systems.
Role in Privilege Escalation: It provides various post-exploitation modules that can help to escalate privileges or maintain access to the compromised system.

POST-EXPLOITATION & REPORTING

In this phase, you gather information from the target system to understand the impact of the breach and report your findings.

Tools:Meterpreter (again)

Description: Once you have access via Meterpreter, it allows you to collect valuable information such as password hashes, sensitive files, and system logs.
Role in Post-Exploitation: You can use Meterpreter to dump credentials, exfiltrate data, or analyze the internal network. These activities help demonstrate the impact of the attack for reporting purposes.

Tools:Metasploit(again)

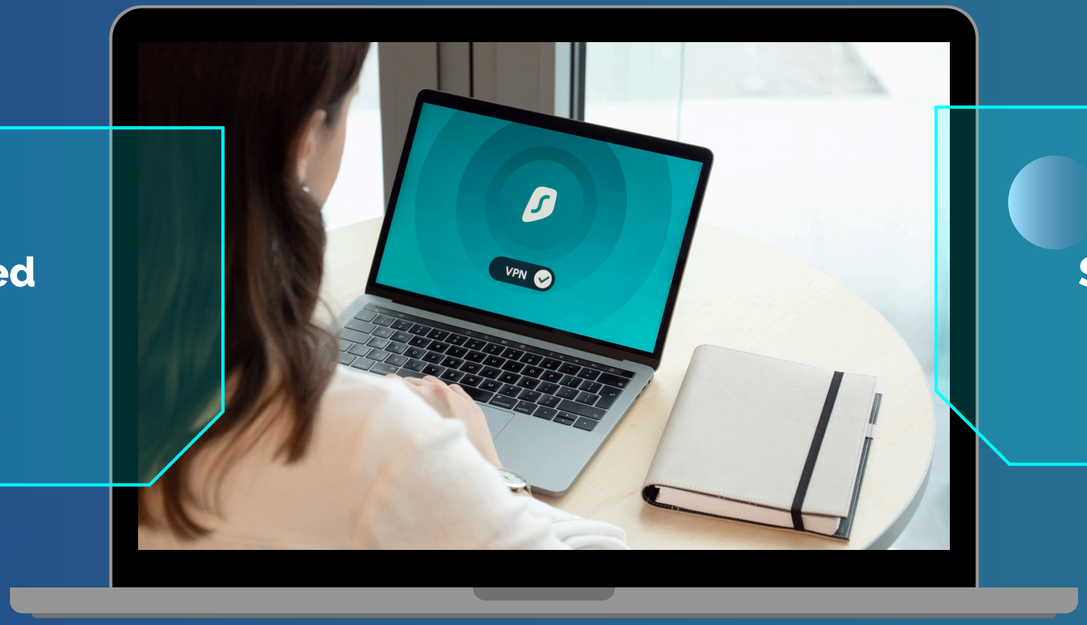
Description: Metasploit contains several post-exploitation modules that can be used to extract sensitive data, pivot to other machines, or clean up traces.
Role in Reporting: After a successful penetration test, Metasploit allows you to document the impact of your attack by running post-exploitation modules, gathering evidence, and reporting on what sensitive information could be stolen.

Phase	Tool	Description	Role
Phase 1: Planning & Reconnaissance	**Nmap**	Network discovery tool to find hosts, ports, services, and OS versions.	Gathers information on the network topology and services.
	Droopescan	CMS scanner focused on Drupal, WordPress, etc.	Identifies CMS versions and vulnerable plugins/themes.
Phase 2: Scanning & Enumeration	**Nmap**	Used for more detailed scans like service versioning and vulnerability detection.	Identifies specific services, vulnerabilities, and open ports for exploitation.
	Droopescan	CMS enumeration tool.	Enumerates plugins, themes, and CMS details to identify potential attack vectors.
Phase 3: Exploitation & Gaining Access	**Metasploit**	Comprehensive exploitation framework with a large database of exploits.	Used to exploit discovered vulnerabilities and gain unauthorized access.
	Searchsploit	Tool to search for exploits from Exploit-DB.	Finds public exploits for known vulnerabilities discovered in earlier phases.
	Exploit	Code or method that leverages a vulnerability to gain access.	Executes the exploit to gain initial access to the target system.
Phase 4: Maintaining Access & Privilege Escalation	**Meterpreter**	Payload within Metasploit providing a remote shell with various post-exploitation features.	Used to maintain access, hide presence, and escalate privileges on the target system.
	Metasploit	Post-exploitation modules for privilege escalation and persistence.	Provides tools for escalating privileges and adding persistence.

Phase 5: Post-Exploitation & Reporting	**Meterpreter**	Shell that allows data extraction and interaction with the target.	Used for gathering evidence (passwords, files, etc.) and documenting the impact of the breach.
	Metasploit	Post-exploitation modules for gathering data, pivoting, and cleaning up.	Used for reporting, collecting sensitive information, and documenting attack impact.

PERSONAL TIPS

Keep Software Updated



Secure Home Networks

infiltrator squad

THANK YOU!