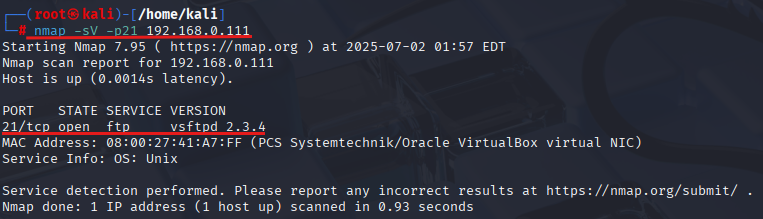
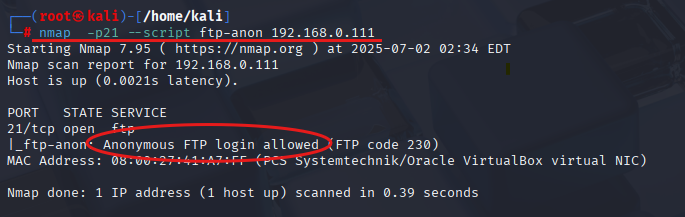
**ENUMERATION :**  The process of actively gathering detailed information about a target system or network to create a comprehensive map of target’s environment to identifies potential vulnerabilities.

**ENUMERATION - FILE TRANSFER PROTOCOL (FTP) :**

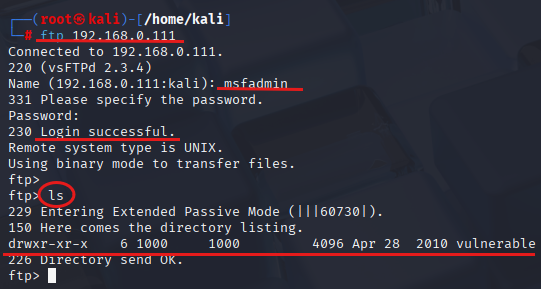
The process of identifying and gathering information about an FTP server on a target network. Using Nmap to a perform task. The basic command for performing an FTP enumeration with Nmap is: nmap -sV -p 21 [target host].



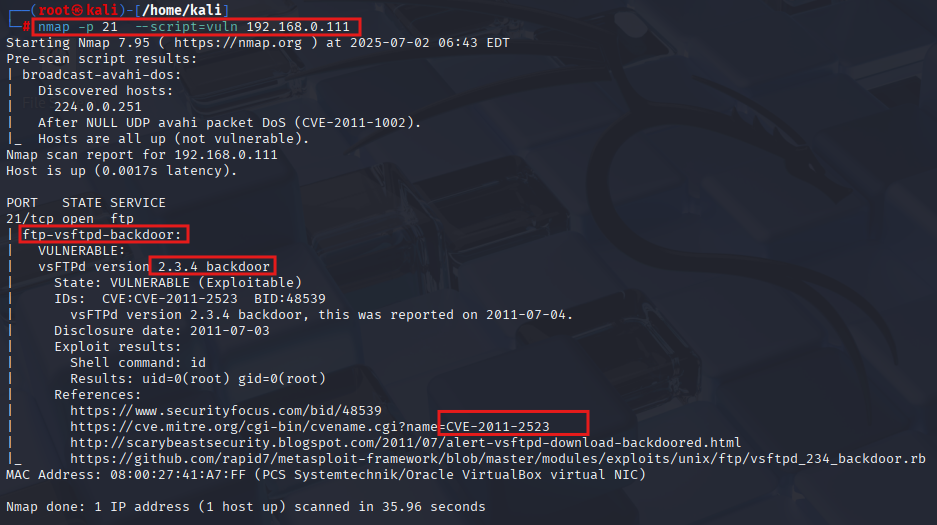
This command tells Nmap to perform a version scan (-sV) on port 21, which is the default port for FTP. The [target host] can be a host name or IP address.



Nmap also allows users to specify a specific FTP script to run during the enumeration process. To run a specific script, the -sC option can be used. For example, to run the ftp-anon script, which checks for anonymous FTP access, the following command can be used.



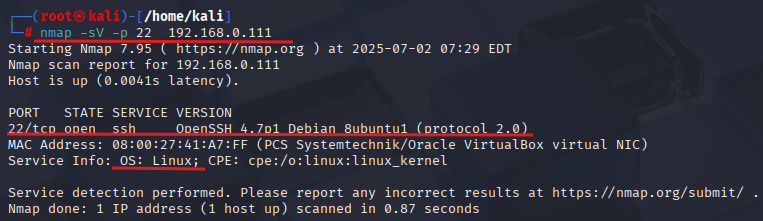
Accessing the FTP server utilizing preassigned administrative credentials. As it was improperly authorized. Where we can access the entire data of the target host.



By executing the script command, we have discerned the vulnerabilities associated with FTP version 2.3.4, as illustrated in the preceding snapshot.

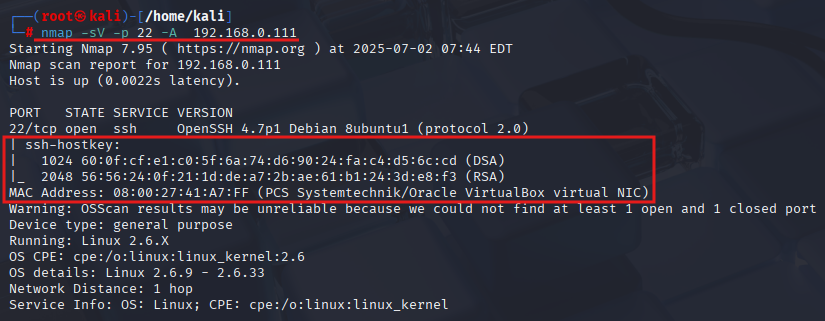
**ENUMERATION - SECURE SHELL HOST (SSH) :**

SSH enumeration is the process of identifying and gathering information about an SSH server on a target network. Using Nmap to a perform task. The basic command for performing an SSH enumeration with Nmap is: nmap -sV -p 22 [target host].

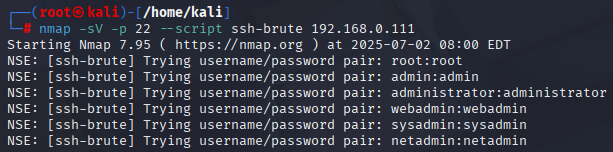


This command tells Nmap to perform a version scan (-sV) on port 22, which is the default port for SSH. The [target host] can be a host name or IP address.

The -A option, which enables OS detection, version detection, script scanning, and trace route. This option can provide more detailed information about the target host and its SSH service: nmap -sV -p 22 -A [target host].

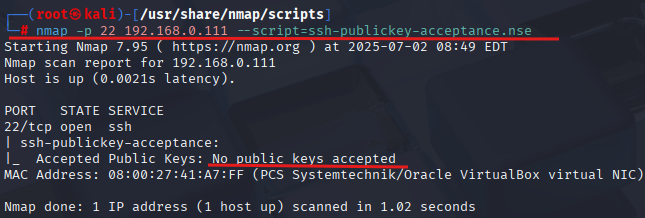


Nmap also allows users to specify a specific SSH script to run during the enumeration process. To run a specific script, the -sC option can be used. For example, to run the ssh-brute script, which checks for brute force attacks on SSH, the following command can be used : nmap -sV -p 22 --script ssh-brute [target host].

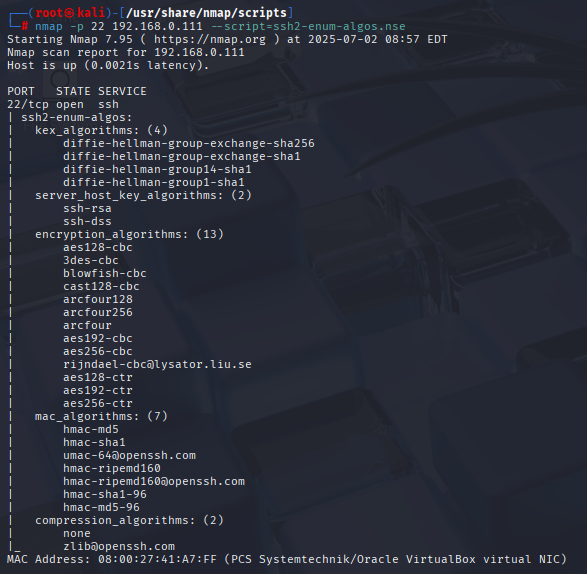


SSH brute force attack is a hacking technique that involves repeatedly trying different username and password combinations until the attacker gains access to the remote server As illustrated in the preceding snapshot.

To Identify the public key of SSH we used the nmap scripting as illustrated in the preceding snapshot. Command used for public key nmap -p 22 192.168.0.111 --script=ssh-publickey-acceptance.nse



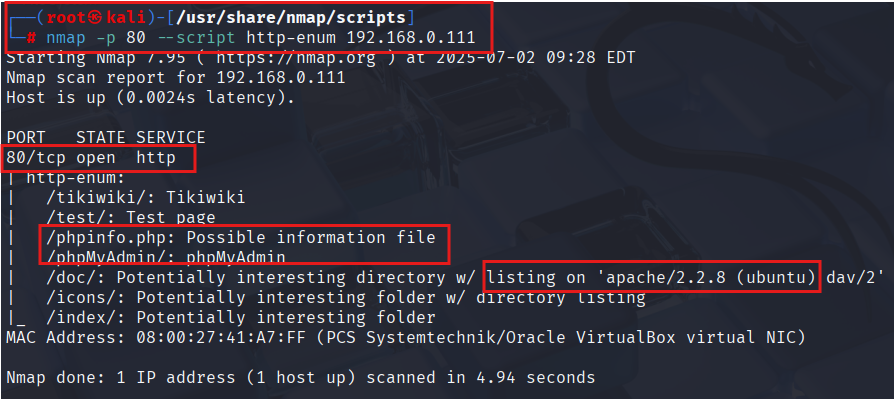
The target SSH2 server offers. If verbosity is set, the offered algorithms are each listed by type.If the "client to server" and "server to client" algorithm lists are identical (order specifies preference) then the list is shown only once under a combined type. Command : nmap -p 22 192.168.0.111 --script=ssh2-enum-algos.nse



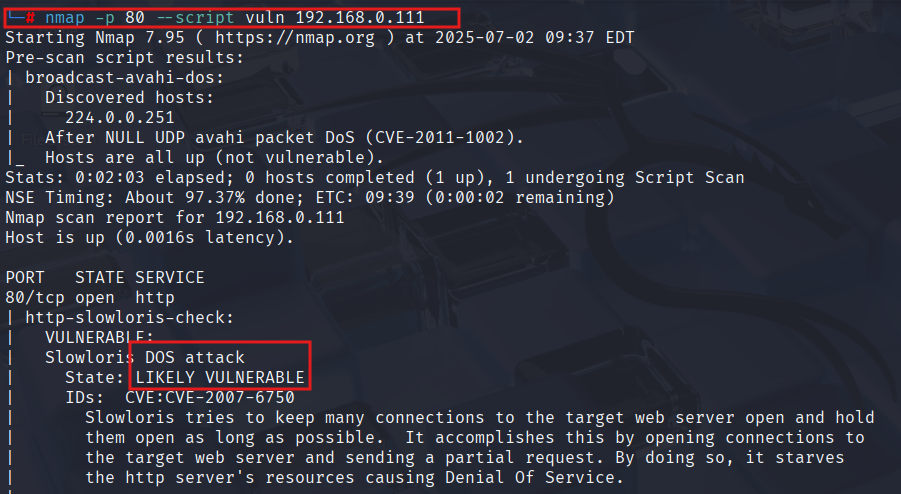
**ENUMERATION - HYPER TEXT TRASFER PROTOCOL (HTTP) :**

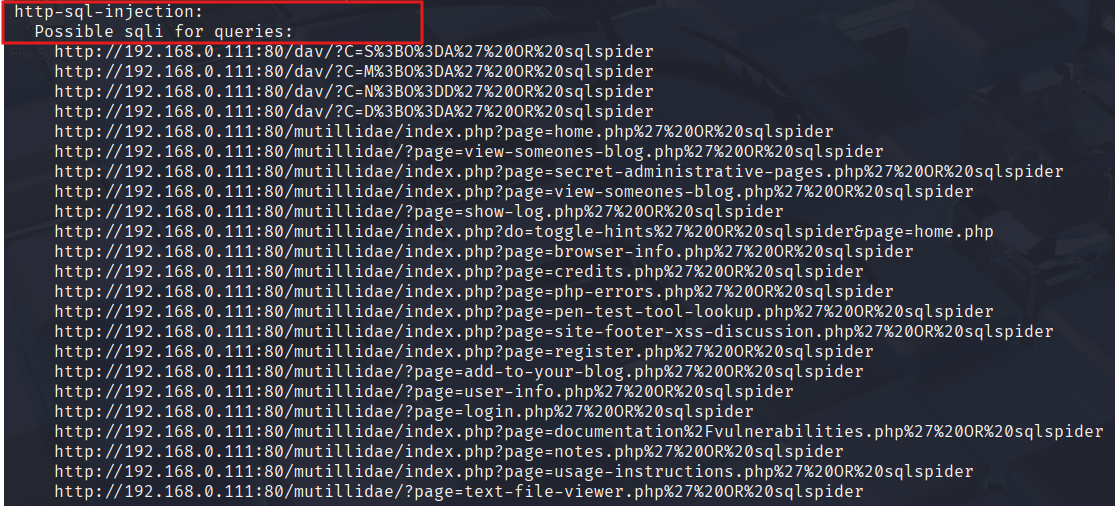
HTTP enumeration is the process of gathering information about a web server by sending specific HTTP requests and analyzing the responses. This information can reveal details about the server's configuration, applications, and potential vulnerabilities.

The nmap --script http-enum command uses the Nmap Scripting Engine (NSE) to enumerate common files, directories, and other resources on a web server. It helps identify potential vulnerabilities and misconfigurations by checking for known web application components and sensitive files. Command : nmap -p 80 --script http-enum 192.168.0.111.

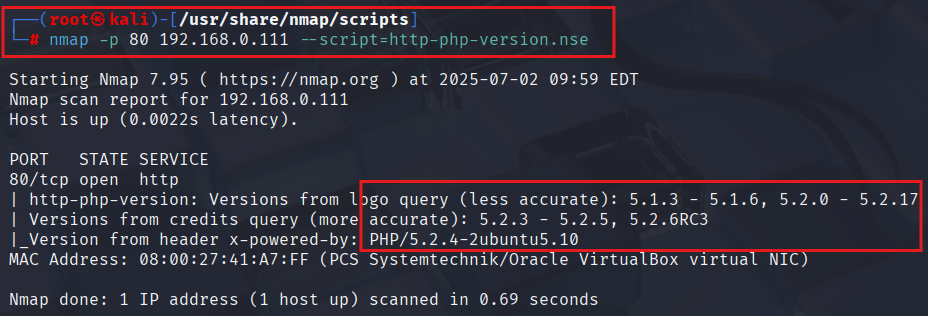


The Nmap command nmap --script vuln tells Nmap to execute all scripts categorized as "vuln" within the Nmap Scripting Engine (NSE). These scripts are designed to detect common vulnerabilities on target systems by checking for known issues like outdated software, default credentials, and misconfigurations. Command : nmap -p 80 --script vuln 192.168.0.111

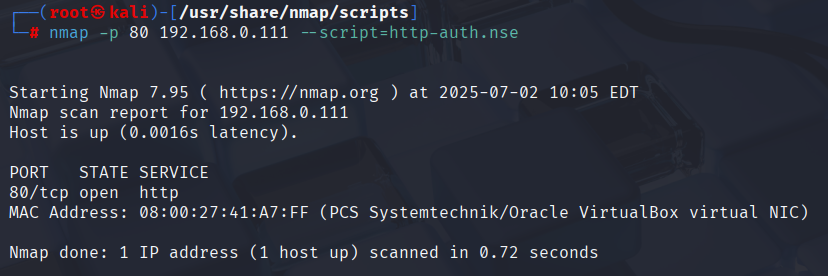




nmap --script http-php-version.nse is an Nmap command that uses the [Nmap Scripting Engine (NSE)](https://nmap.org/book/man-nse.html) to detect the version of PHP running on a web server. It does this by sending specific HTTP requests and analyzing the responses to identify the PHP version.



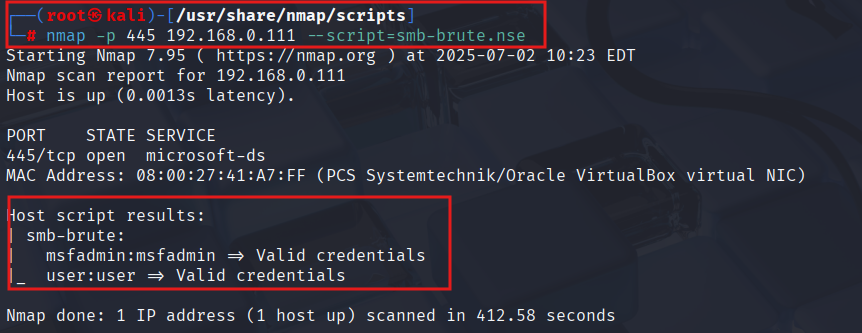
Nmap test for common authentication bypass vulnerabilities on HTTP servers. Specifically, this script attempts to identify weak or missing authentication mechanisms by sending various HTTP requests with different authentication challenges and evaluating the responses. Command : nmap -p 80 192.168.0.111 --script http-auth.nse We didn’t find any authentications because its an open port and insecure one.



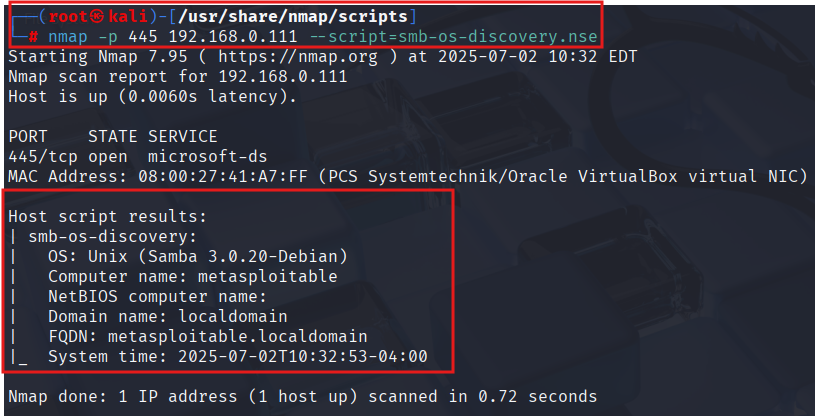
**ENUMERATION - SEVER MESSAGE BLOCK (SMB) :**

SMB enumeration is the process of gathering information about a target system that uses the Server Message Block (SMB) protocol, specifically focusing on identifying shared resources, user accounts, and potential vulnerabilities.

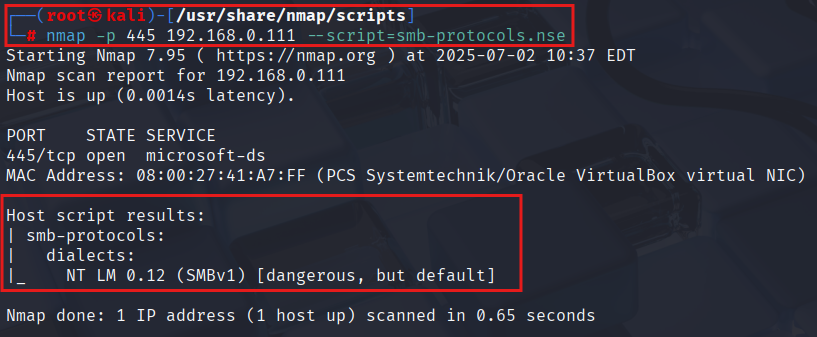
Attempts to guess username/password combinations over SMB, storing discovered combinations for use in other scripts. Every attempt will be made to get a valid list of users and to verify each username before actually using them. When a username is discovered, besides being printed, it is also saved in the Nmap registry so other Nmap scripts can use it. Command : nmap -p 445 192.168.0.111 --script=smb-brute.nse



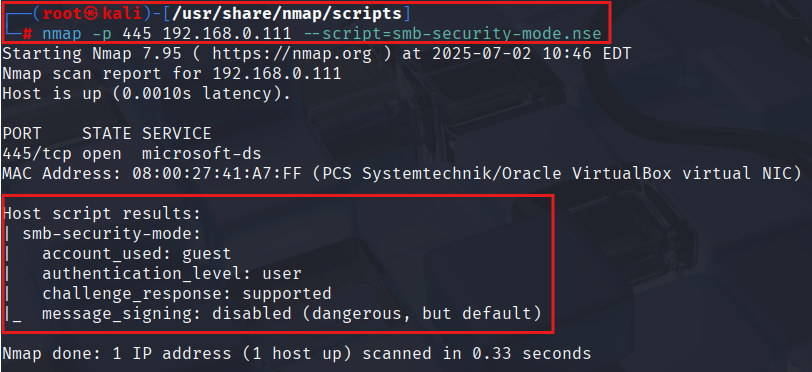
The nmap --script smb-os-discovery.nse command uses Nmap's Scripting Engine (NSE) to identify the operating system and other information of a target machine via the Server Message Block (SMB) protocol. It attempts to determine the OS, computer name, domain, work group, and system time by initiating an SMB session, typically with an anonymous account, and analyzing the server's response. Command :nmap -p 445 192.168.0.111 --script smb-os-discovery.nse



If SMBv1 is found to be enabled, it will be flagged as insecure, as it is considered outdated and vulnerable. Command : nmap -p 445 192.168.0.111 --script smb-protocols.nse

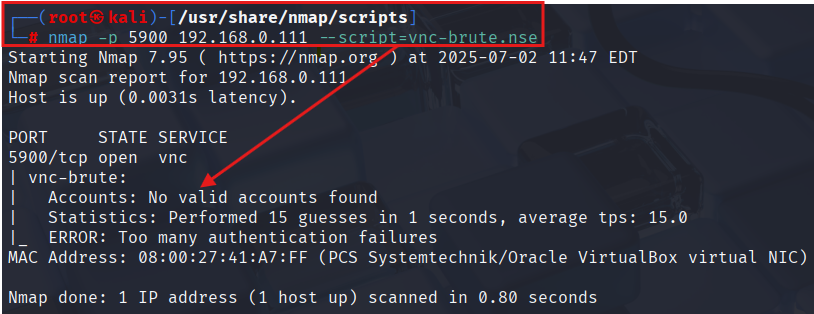


Returns information about the SMB security level determined by SMB. Here is how to interpret the output: User-level authentication: Each user has a separate username/password that is used to log into the system. Command : nmap -p 445 192.168.0.111 --script=smb-security-mode.nse



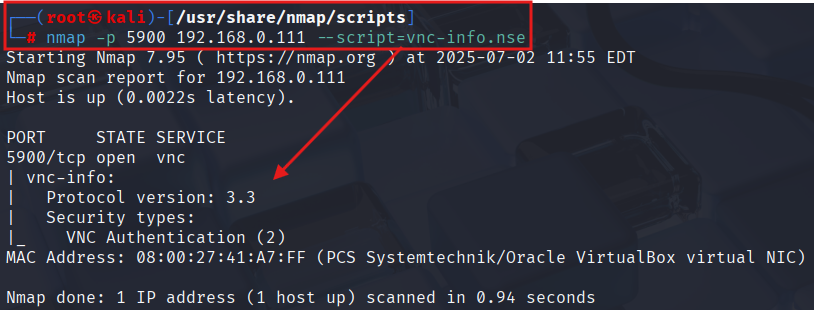
**ENUMERATION - VIRTUAL NETWORK COMPUTING (VNC) :**

Involves identifying and gathering information about VNC servers and their configurations on a network. This process helps attackers understand the environment and potentially exploit vulnerabilities.

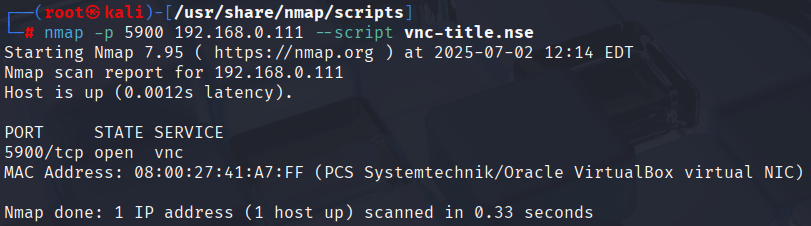


Vnc brute force attack is a hacking technique that involves repeatedly trying different username and password combinations until the attacker gains access to the remote server As illustrated in the preceding snapshot.Command : nmap -p 5900 192.168.0.111 --script=vnc-brute.nse

Queries a VNC server for its protocol version and identifies supported security types used by the server.Command : nmap -p 5900 192.168.0.111 --script=vnc-info.nse



Attempts to log into a VNC server and Extracts the desktop title (the name of the remote desktop session). command : nmap -p 5900 192.168.0.111 --script vnc-title.nse



The script only runs if it detects a VNC service on the specified port. If the service is on a different port or not running, the script’s rule function returns false and skips execution.