WinRM 5985 Exploitation Cheat Sheet

🔎 **Step 1: Detect if Port 5985 is Open**

bash

CopyEdit

nmap -p 5985 --open -sV <IP>

If it shows:

arduino

CopyEdit

5985/tcp open http

👉 Likely WinRM is running.

🔐 Optional: Verify it's WinRM

bash

CopyEdit

nmap --script=http-winrm-info -p 5985 <IP>

Look for output like:

yaml

CopyEdit

WinRM Service

OS: Windows Server

Authentication Methods: Basic, NTLM

🔑 Step 2: If You Have Credentials

Try logging in using evil-winrm:

bash

CopyEdit

evil-winrm -i <IP> -u <username> -p <password>

If you have a **.pfx or cert**:

bash

CopyEdit

evil-winrm -i <IP> -u <username> -p <password> --ssl

⚠ Troubleshooting Tips

Symptom	Fix
Error: Authentication failed	Try other creds / check case sensitivity
SSL/TLS required	Try --ssl or test port 5986
Can't connect	Port may be firewalled — scan again

Example Scenario

You got webadmin:Summer2024 from a web.config file?
5985 is open? You try:

bash

CopyEdit

evil-winrm -i <ip> -u webadmin -p 'password'