Runbook 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | IRTx Red Run 1 | Version | V1 | |
| Author | | Dylan Wondal | Date Created | 11/9/23 | |
| Attack Type | | Vulnerable services | Last Modified | 11/9/23 | |
| Staff Required | | 1 Attacker | Skills Required | Nmap, nc | |
| Document  Description | This document is to scan a server and find a vulnerable Jenkins Instance | | | | |
| 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. Look for things like ftp, smb, jenkins installs etc.  nmap -sC -sV -oN init.scan $IP | | |  |
| Step 2 | | Task | | | Complete |
| Locate jenkins | | Locate which port jenkins is running and go to webpage to see if there is any authentication. If there isn’t locate the script console under “manage jenkins” | | |  |
| Step 3 | | Task | | | Complete |
| Create Reverse shell code | | Go to revshells.com and set the reverse shell payload to groovy. Update the IP and port to desired e.g. 192.168.1.1 port 9001 | | |  |
| Step 4 | | Task | | | Complete |
| Start listener | | Start nc listener on attack box using port specified in rev shell  e.g. nc -lvnp 9001 | | |  |
| Step 5 | | Task | | | Complete |
| Run script | | Paste the code from revshells and run the script. The reverse shell should now connect with NT\AUTHORITY SYSTEM | | |  |

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, SQLmap | |
| 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 | | Go to the webpage and look for where sql can be used  e.g user information page | | |  |
| Step 3 | | Task | | | Complete |
| Capture request | | Capture request using Burpsuite of a test request with sql. Right click the request and save to file e.g. sql.req | | |  |
| Step 4 | | Task | | | Complete |
| Run SQLmap | | Run sqlmap using the file  sqlmap -r sql.req  if successful injection found, run the same command with --dump to dump the database. Also select yes when sqlmap asks if it should crack passwords | | |  |

Runbook 3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Document Name | | IRTx Red Run 3 | Version | V1 | |
| Author | | Dylan Wondal | Date Created | 9/10/23 | |
| Attack Type | | Insecure File upload | Last Modified | 9/10/23 | |
| Staff Required | | 1 Attacker | Skills Required | Burpsuite | |
| Document  Description | This is attack is to target insecure/unsanatised file uploads. A malicious file will be uploaded that will create a reverse shell on the host machine for the attacker to connect to | | | | |
| 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 |
| Locate upload page | | Locate the page where files can be uploaded and test with a test file | | |  |
| Step 3 | | Task | | | Complete |
| Upload file | | If there is no sanitisation get a php shell (ivan-sincek / php-reverse-shell) and upload | | |  |
| Step 4 | | Task | | | Complete |
| Security bypass | | If there appears to some security e.g only allow images, change the file extension to .php.jpeg. Intercept the request with burpsuite. Change the file name back to .php and send the request | | |  |
| Step 5 | | Task | | | Complete |
| Connect to shell | | Run nc to listen  e.g. nc -lvnp 9001  open location where shell is stored (output on screen)  connect to reverse shell | | |  |