Black Sabre Response

Observer Book

Scenario 1:

Vulnerable Service Exploitation

RED TEAM

Goals:

- Enumerate active services on target
- Determine exploit in Metasploit Framework
- Gather required information to launch exploit
- Launch exploit and get shell
    - If the MSF exploit fails, manual exploitation will be required
    - Additional research/knowledge may be required for manual exploitation

Tools:

- NMAP
- Metasploit framework
- nc

Rules of engagement:

- Do no delete any file not created by the red team
- Do not stop or modify any other services

Time Estimate: 10-30 minutes

BLUE TEAM

Goal:

- Detect any exploit attempts against services running
- Check for the suspicious process using tools such as ProcExp and Task Manager, terminate if needed
- Watch the splunk alerts console for incoming alerts.
- *Source=”WinEventLog::security” EventCode=4688 “PowerShell”*

Scenario 2

SQL injection

RED TEAM

Goals:

- Enumerate web servers
- Locate potential SQLi target
- Perform manual or automated exploitation of SQLi
- Dump tables to gather information and/or passwords/hashes

Tools:

- NMAP
- SQLmap
- Burpsuite

Rules of engagement:

- Do no delete any file not created by the red team
- Do not stop or modify any other services
- Do not delete or remove data from database
- Do not change DVWA security level

Time Estimate: 10-30 minutes

BLUE TEAM

Goal

- Detect SQLi attempts
- Watch the splunk alerts console for incoming alerts.
- On receiving a “Potential SQLi Attempt” alert, review logs in splunk to find any potentially suspicious activity.
- Look for suspicious sql queries

Scenario 3

File Upload

RED TEAM

Goals:

- Enumerate web servers
- Locate file upload location
- Determine backend
- Determine upload restrictions
  - If there is file extension checks may need to intercept request and change type before being sent to server
- Upload reverse shell
- Open shell and connect

Tools:

- NMAP
- Burpsuite

Rules of engagement:

- Do no delete any file not created by the red team
- Do not change DVWA Security level
- Do not stop or modify any other services

Time Estimate: 15-30 minutes

BLUE TEAM

Goals

- Detect malicious file uploads
- Watch the splunk alerts console for incoming alerts.
- On receiving a “Potentially Malicious Upload Access” alert, review logs in splunk to find any potentially suspicious activity.
- Flag any potential malicious files