Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

- Set alarm for when a single IP is sending an (x)amount of packets/per 1 minute intervals..

What threshold would you set to activate this alarm? **1000 packets per 1 minute interval.**

System Hardening

What configurations can be set on the host to mitigate port scans?

- Implement a IPS/IDS tool
- Firewall

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

I would set 2 separate alerts. The first would be at a Low-Normal priority for whenever someone accesses the company_folders directory. Then I would set a secondary alert with a priority of High for whenever someone attempts to interact or access the secret_folder directory.

What threshold would you set to activate this alarm? **I would set a limit (threshold) triggered after 3 events.**

System Hardening

What configuration can be set on the host to block unwanted access?

- **Reconfigure to store the secret folder on a private facing network.**
- **Add file folder encryption or encrypt the data within the folder.**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- **Set an alarm for a designated number of unsuccessful attempts reached.**

What threshold would you set to activate this alarm?

- **A threshold could be set at 3 attempts per second.**

System Hardening

What configuration can be set on the host to block brute force attacks?

- **Limit the number of user attempts.**

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- **Set an alarm for any unauthorized wireless access to the webdav; set an alarm for unauthorized access attempts occurring outside of the organization.**

What threshold would you set to activate this alarm?

- **I would set a threshold of 3 attempts per alarm per the above alarm designations.**

System Hardening

What configuration can be set on the host to control access?

- **Putting into place a firewall if it does not exist or if it is currently in place, evaluate the current configurations and reconfigure to provide stronger protection.**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

- **Set an alarm for any traffic going out of the target machine on port 4444.**

What threshold would you set to activate this alarm?

- **For this particular alarm, I would implement what I would call a “zero-tolerance” alarm in the the interim, evaluate and reconfigure at post evaluation.**

System Hardening

What configuration can be set on the host to block file uploads?

- **Block traffic inbound and outbound on port 4444 with the use of a firewall.**