




# YOU'VE BEEN PWND BY N1CKC@63

Virtual Design Master Season 4  
Challenge 2



Paul Woodward  
@EXPLOREVM Paul.Woodward.Jr@Gmail.com

## Contents

Executive Summary.....	2
Scope.....	2
Requirements, Constraints, Assumptions, and Risks.....	2
Requirements.....	2
Constraints .....	2
Assumptions.....	3
Risks .....	3
What we know .....	3
Locating the Changes .....	3
FireGen.....	4
ManageEngine EventLog Analyzer .....	4
vSphere Replication .....	4
Log Analysis Results .....	4
Determining the Root of the Attack .....	4
Detecting Future Changes.....	5
Splunk.....	5
Cisco FireSITE Management Center .....	5
Preventing Future Attacks .....	5
ASA Configuration Changes .....	5
Data Protection .....	6
Retention & Backup Policies .....	6
Endpoint Protection .....	6
Environmental Documentation .....	6
Other Changes .....	6
Operational Plan of Attack.....	6
Appendix and References .....	8
Challenge 1 – Datacenter Design Document .....	8
Reference Links .....	8

## Executive Summary

Thanks to the actions of the EARTH team, we now have a thriving, multi-planetary datacenter infrastructure. Shipping and receiving between Earth, Mars, and the Moon has begun to support the rebuilding process on Earth. While inspecting the day's shipping manifests, our shipping manager has discovered some discrepancies. It appears that someone made changes to his final order of supplies for the day to be delivered to the moon; additional supplies have been added, as well as the destination has been changed to Earth. All of these actions occurred under his name / account.

Immediately sensing an emergency, the shipping manager brings the issue to the EARTH team. The NOC officer says that all three datacenters appear to be alive and healthy. Attempting to access the shipping management system on Earth, he is unable to log in. Acting on his suspicions, NOC Officer Jones attempts to access the shipping database server and is again unable to gain entry. It's now clear that someone's infiltrated the Earth CHIDC01 datacenter.

The EARTH team Security Officer declares an all hands on deck emergency. Unfortunately, the EARTH team consists of 5 members, and other teams from the Earth repopulation group cannot spare any resources to assist. The early indication is that someone survived the zombie apocalypse on Earth, and has managed to create satellite communications.

## Scope

With time and limited resources against them, it is up to the EARTH team to find the culprit, restore access to CHIDC01, and secure the datacenters against future attacks. Building off the base infrastructure, additional resources, both hardware and software, may be added to detect and secure.

## Requirements, Constraints, Assumptions, and Risks

### Requirements

- Find the extent of the changes anywhere within the system
  - What are the prerequisites to make this happen?
- Be notified of other changes; not just files but attacks as well.
  - How fast can you detect an attack and changes
- Prevent the changes – Can you prevent the attack or just detect the attack?
  - If only detection, how fast can you make this happen?
- Determine the root of the attack
  - Can we find the culprit?
  - Is there any forensic data?
  - Where did the "Bad Actor" leave their mark?

### Constraints

- Limited manpower is available
- Life critical supplies are being diverted from their final destination – Time is of the up most importance
- As resources and time are short, we are unable to completely "blow away" the Earth datacenter VMs and configurations and start over fresh.

## Assumptions

- There is an assumption, within reason, of best practices being used in the initial datacenter installation from challenge 1 – However, human error can exist
- A Windows Active Directory environment is in place for user and role management. This would have been completed by the Ops team upon completion of the Datacenter infrastructure
- Humanity Link software does NOT originate on Earth
- There is not enough people anywhere to do this by hand in any timely fashion. Incident response should not take decades
- People overlook security issues all the time
- There exists some data that MAY help us
- The bad actor does not know they were detected, yet. However, could easily see something if you are foolish in your response.
- You personally detected them as the person placing an order
- You have NOT lost Control of all aspects of communication
- You have lost CONTROL yet not monitoring capability of the earth bound datacenter, yet to continue to function you can perform most control operations
- The black market is operational between earth-moon-mars

## Risks

- We must not let the “Bad Actor” (BA) know we are on to them
- If access and full control are not restored, the entire Earth repopulation project is at risk of failure

## What we know

In our installation of the datacenter, our Networking Officer implemented Cisco Advanced Security Appliance (ASA) 5555 with FirePOWER services capability at each datacenter to act as a firewall and a VPN connection between each site.

Remote Syslog was configured for the Cisco gear to send all administrative changes to a log server at the main Mars datacenter. This Syslog server resides on a separate VLAN than the Production or HumanityLink VLAN. Remote Syslog collection was also configured in a similar fashion for Windows Active Directory as well. Kiwi Syslog server is used for log collection.

As the internet does not exist as it did in the time before zombies (BZ), we only have 2 connections to each site:

- Earth -> Mars & Moon
- Mars -> Earth & Moon
- Moon -> Earth & Mars

## Locating the Changes

In discovering the location of the breach, and extent of the damage done by BA, our historical logs will be an amazing asset. As our logs are located in the Mars datacenter, where our hacker does not have access, we can safely analyze these logs without arousing the suspicion that we are on to them. Due to the team's limited manpower, and the size of the historical logs, automated log analyzation tools will be utilized for quick analysis and root cause analysis.

Agility is important in discovering our changes, so the following tools will be utilized. It should be noted that they are not a long term solution for change management; that will be discussed in the “Detecting Future Changes” section.

### FireGen

FireGen 3.0 Log Analyzer is specially designed to pour through the logs created by firewalls and security appliances. This program mimics the steps taken by security administrators and presents data graphically for easy interpretation. This tool will help with the forensic analysis of the logs to locate how the Bad Actor entered the environment.

### ManageEngine EventLog Analyzer

EventLog Analyzer is a free tool which can be utilized for forensic analysis of historical Windows Syslog events. This tool can also be utilized for real time event monitoring, but the free version is only applicable for 5 sources. The ERTH team will use EventLog Analyzer only to review Active Directory events and changes which may have been made.

### vSphere Replication

Using vSphere Replication, known affected VMs will be replicated to the Moon datacenter for analysis utilizing the “Recover with latest available data” option. This allows a VM to be replicated in its last known state and without synchronizing to the existing VM. The VM will have networking disabled so it cannot communicate with the attacker and notify them that we are investigating the corrupted servers.

### Log Analysis Results

A review of the logs from the Cisco ASA 5555 have revealed the Cisco IPS Signatures 7169-0 and 7169-1, as well as the creation of an unknown administrative account. Windows Active Directory event log analysis has revealed the creation of a domain admin account and it’s addition to all security groups in the environment.

## Determining the Root of the Attack

As rogue satellite communications have been detected, the Security Officer believes our Bad Actor has gained entry through our firewalls. A VPN connection links each site, so a Man in the Middle attack is not suspected. Since there are only 2 necessary connections, IP control lists would be configured to limit the IP addresses allowed to make connection to each ASA. It is believed BA followed the satellite communications and discovered our datacenters. Log analysis has proved that the BA has created an account and created a VPN connection to the CHIDC01 ASA. The thought now is there must be a vulnerability in our ASA.

Reviewing the ASA 5555 configurations and logs, it has been discovered that the Bad Actor has utilized the IKE v1 & IKEv2 vulnerability to compromise the CHIDC01 firewall. This vulnerability allows a UDP packet to be sent specifically to a buffer overflow and allowed the Bad Actor to gain control of the ASA. Rather than completely locking out the ERTH team, the BA created their own administrative account on the ASA and created a VPN connection from their lair to the Earth datacenter.

This issue can be fixed by implementing the upgraded software provided by Cisco to address this vulnerability. The software on all Cisco ASA 5555s will be upgraded after intel and data collection on the Bad Actor has been completed, and the order given to remove the threat.

## Detecting Future Changes

To help the understaffed ERTH team monitor and secure the datacenters, additional monitoring tools will be put into place. These centralized management tools will provide real time analytics, detect any changes to configurations, and alert our NOC/ERTH staff of changes based on our configuration preferences

### Splunk

Splunk is an industry leading software suite specializing in data collection, indexing, analyzation, monitoring, and reporting for nearly all technologies utilized in a datacenter. Splunk will be linked to all networking gear, virtual machines, Active Directory Domain Controllers, Windows Servers, databases, and applications.

Splunk's proactive alerting will be configured to send notifications to the ERTH team staff via email and SMS. These proactive alerts will be for administrative changes to any hardware, Active Directory, and critical applications. Health and other metric alerting will be configured as well, and alerting channels will be set based on SLA levels.

The Splunk dashboard will be added to the NOC center and monitored by the NOC Officer. The ERTH team members will all be trained on Splunk to provide relief for the NOC Officer. The NOC Officer will subsequently train additional staff on reading the data and utilizing the dashboard as staff become available.

### Cisco FireSITE Management Center

As it was not configured with the ASA deployment, FireSITE Management Center will be deployed as a virtual appliance. FSMC offers analytics, policy management, statistics, and forensic tracking. This tool will be utilized side by side with Splunk for an additional view into our datacenter environments.

Much like Splunk, alerts will be sent to the ERTH team based on SLA requirements. The NOC center will be equipped with another dashboard to provide real time data for security and health monitoring.

## Preventing Future Attacks

With change alerting in place via Splunk, the NOC Officer now has near real time notification to potential attacks or undesirable changes to the environment. While these outlined changes will greatly reduce the potential for a future attack, there will always be a chance of a breach. The key to future success will be diligent monitoring, and rapid response to incidents.

### ASA Configuration Changes

Control Plane Access List will be configured on each ASA to restrict traffic attempting to connect to the edge devices at each datacenter.

As each 5555 ASA has only 2 required connections, and the hardware at each connection is known and static, MAC filtering will be implemented. This will restrict connections to the each firewall to only known, approved devices.

## Data Protection

Data protection will be implemented in the form of Veeam Enterprise Suite, which includes Veeam Backup & Recovery v9. This solution will require the following VMs:

- Veeam Enterprise Manager (placed at the Mars DC)
- Veeam Backup Server – One at each datacenter
- Veeam Backup Proxy Server – Two at each datacenter
- Veeam Repository Servers – One at each datacenters
  - Repository Servers are Windows Server 2012 R2 VMs presented with iSCSI storage for backup storage

## Retention & Backup Policies

VM Type	Full / Incremental	Schedule	Retention
Critical	Incremental	15 minutes M-Sa	4 weeks
Critical	Full	Every Sunday	4 weeks
Standard	Incremental	Every 12 hours	4 weeks
Standard	Full	Every Sunday	4 weeks

## Endpoint Protection

To secure endpoints, and as a tool to assist in change tracking, Carbon Black will be deployed. Carbon Black is a powerful end point protection software that locks down systems and only allows programs on a whitelist to execute. Carbon Black also tracks changes made to files, registry entries, and provides a step by step order of how one program may trigger another to execute.

Implementing the blacklist/whitelist solution is labor intensive, so on the initial deployment, a monitoring only mode will be utilized. After resolution of the datacenter hack, when resources become more available, the whitelist will be created and implemented.

## Environmental Documentation

Detailed information about the entire environment, from switch configurations, VM hardware resources, server roles and features, Active Directory configuration, to networking designs will be documented. This information provides a great resource for the ERT team to compare active configuration to initial healthy, functional configurations for troubleshooting purposes.

## Other Changes

As the Bad Actor may be working with someone internal to our staff, physical hardware will be hardened as well. All unused ports on the ASA and switches will be disabled, as well as all USB ports on all datacenter hardware.

## Operational Plan of Attack

Now that the 4 requirements have been answered, how do we implement them in a manner such that we do not tip our hand to Bad Actor? Below is the playbook for retaking CHIDC01.

1. Logs are analyzed and the source of the breach has been located

- a. As electronic communications may be compromised an in person meeting with Mr. Billionaire is arranged to discuss the results
  - b. We now know when the BA entered our networks and approximately how many changes they have made to the system
2. Mr. Billionaire issues an interplanetary announcement celebrating the success of our new datacenter implementations. He now requests that the ERTH Team configure centralized monitoring all sites.
  - a. Having Mr. Billionaire giving the green light for the next phase of development gives the impression that we are blissfully unaware of our Bad Actor, and that our implementation of Splunk, FireSIGHT, and other changes appear 'normal'
3. ERTH team rolls out multi-site monitoring tools outlined in our 4 requirements
  - a. These tools will provide a real time notification of any changes the BA may make, allowing us to see to what depth they have access to CHIDC01
  - b. Monitoring is managed in the Mars datacenter and is the Management VLAN, away from BA
  - c. False Splunk servers are placed in the Earth datacenter to distract the BA from our true intentions, as well as prevent them from seeing what data we are truly monitoring.
4. The ERTH Security Officer watches patiently as alerts roll in on the BA's activities. Clearly BA is interested in what we are implementing and is poking around our new systems.
  - a. Although we could cut off the BA from our systems at this point, the Security Officer allows the continued prodding as a form of pen testing and allows them to assess the BA's abilities
5. As it's too late to recall the shipment, satellite tracking is utilized to follow it to its final destination with the hopes that the BA will be on site to receive the cargo. A recovery team will follow the shipment to the site to collect the cargo once the order has been given. An armed security team will accompany the recovery team as the landing site may be a trap, and the existence of zombies is still a possibility.
6. As we know how the Bad Actor entered our systems and which VMs they've corrupted, it's time to take them back. Since our monitoring rollout went successfully, Mr. Billionaire now asks for a test of the disaster recovery system – Site Recovery Manager
7. Non-corrupted VMs are failed over to the Moon Datacenter. Simultaneously, the BA's administrative account is removed from the ASA. Should our ability to make changes on the ASA be impaired by the BA, the ERTH Security officer will hack the 5555 using the same exploit utilized by the BA. The ASA will be immediately updated so the exploit cannot be used against the datacenter in the future.
  - a. VMs which have been deemed as corrupted will be destroyed and rebuilt, if possible, otherwise they will be "cleaned" by members of the ERTH team to remove any administrative or registry changes, as well as remove any malicious software.
8. Once the ASA is deemed "repaired", all VMs will be returned to CHIDC01. Intensive monitoring of network traffic in/out of the firewall as well as security settings on the VMs will begin to verify the removal of the Bad Actor's foothold.
9. Ongoing security audits and investigations of new softwares/appliances will continue to increase security in and around the datacenter.



## Appendix and References

### Challenge 1 – Datacenter Design Document

(Double click .PDF to open)



## RETURN TO EARTH

Virtual Design Master Season 4  
Challenge 1



### Reference Links

#### Cisco

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike>  
<http://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-732251.html>

Splunk

[http://www.splunk.com/en\\_us/products/splunk-enterprise.html](http://www.splunk.com/en_us/products/splunk-enterprise.html)

[http://www.splunk.com/en\\_us/products/splunk-enterprise/features.html](http://www.splunk.com/en_us/products/splunk-enterprise/features.html)

<http://www.nutanix.com/splunk/>

Veeam

<https://www.veeam.com/data-center-availability-suite.html>

Carbon Black

<https://www.carbonblack.com/>

FireGen

<http://www.firegen.com/firegen30.html>