Challenge 2 – Environment compromised

Stanislav Majzlik
06-07-2016

Summary

Bad, bad things are happening in our datacenter. Someone was able to compromise our environment. Looks like that we are not fully managing the environment and someone is heavily “helping” us. So let’s clean up.

Here are the things to do:

A. find the extent of the changes anywhere within the system, what are the prerequisites to make this happen

B. be notified of other changes, not just to files but to attack(s), what is the steps of an attack, how fast can you detect an attack and changes?

C. prevent the changes, can you prevent the attack or just detect the attack. If only detection how fast can you make this happen.

D. determine the root of the attack, can we find the culprit, is there any forensics data, where did the ‘bad actor’ leave his/her fingerprints. Is it the black market or something else?

Idea

In couple of following sentences I would like to explain the way how I approached this challenge. In order to be able to fulfill the tasks, first I am describing in high level the related security configuration of the environment with the core parts which I think are crucial in order to be able to say that we are able to detect an attack, compromised environment, or have some data to review and try to find what happened in our environment. I am also trying to describe a reasonable level of security and not fall into security through obscurity level. I will try to describe the way I would go when I would recognize that my environment was compromised.

Attacker's decision making processes and methodologies are known in advance. Every attacker would follow the defined OODA loop, which refers to decision cycle of observe, orient, decide, and act. So the administrators have huge advantage against attackers. Administrators should know their environment and it’s strong and weak parts the best and use this as their advantage.

So let’s start with the prerequisites to be able to investigate potential attack and find out what did happen in the environment. These rules will also minimize the risk of a potential attack.

Datacenter security

- Access is requested via ticket against hosting provider
- Only approved persons are able to request access for engineers (typically security officer)
- Check in at Datacenter reception is needed, Identity will be verified by official document like an ID Card, Passport or Driver License
- Onsite engineer is escorting engineers to DC floor, Onsite engineer's identity is verified with finger print sensors and personal RFID card when accessing the DC floor
- Onsite engineer opens the server room (similar controls are in place as for the DC floor)
- Onsite engineer unlocks the rack cabinets with the HW equipment (rack cabinets are locked)
- CCTV cameras are monitoring all major places from the entrance to each single rack cabinet (entrance area, reception, corridor to the DC floor, corridor to the server rooms, rack cabinets)

HW security

- Equipment is racked in locked cabinets as defined in Datacenter security part
- All devices are monitored
- All unused network interface are disabled
- All unused interconnections are removed
- Local management interfaces are disabled or password protected
-

Software security

- All software, firmware, drivers used in the environment is supported by the vendor and all related patches are applied
- Recommended configuration best practices are followed where possible
- Recommended hardening guides are followed where possible

Access control

The underlying principle is that access to all environment components (systems, services and information) is denied, unless expressly permitted to individual users or groups of users based on their job function. All access approval and access revocation requests need explicit approval from the management team and will be implemented on the appropriate environment components by the Admin team. All accounts will be assigned to a unique user ID. Initial password must be changed prior to first usage. The use of shared and\or generic accounts within the environment is strictly prohibited.

All requests for access and access revocation need to be raised via ticketing tool and must follow standard change management process.

Role definition

Standard roles are defined based on the actual environment and technology used which are then linked to defined job function. These two identities will together provide permission matrix which will be used by the Access control. This will help us to define the minimum permissions needed for the specific job role and avoid to grant too much or not enough permissions so in final it will save us a lot of time when creating new accounts.

Change management process

Every network connection, firewall or router, hardware, configuration change must be handled according to the Change management process. Every change must be tested and approved.

Logging

Central logging for the environment components is in place including the following components:

- Operating systems logs (Event Logs and su Logs)
- Antivirus logs
- IDS\IPS logs
- Firewall and Switches logs
- VMware logs
- File integrity monitoring logs

Central logging solution is set up as a Linux cluster of two servers and running on CentOS 6 with the standard clustering solution. The machines are connected via a separate LAN for the cluster communication and data mirroring.

This syslog cluster will be used as a main logs store from all components of the environment.

IDS/IPS

Combination of host based and network based IDS/IPS system will be used.

For host based IDS/IPS OSSEC will be used. OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows. OSSEC is free software and commercial support is also available.

For network based IDS/IPS we can use VMware NSX with McAfee implementation. This combination will provide us East-West traffic filtering with added functionality of IDS/IPS detection.

From my perspective, the main point of the correct IDS/IPS configuration is to be aware, how my environment behaves in normal conditions, in another words, what is the standard usage/behavior pattern. With this information's we can adjust the IDS/IPS rules to best fit in our environment.

As an example:

Our HumanityLink software suite is using 3tier architecture. Web – App – DB communication. Let's say that our number of average TCP sessions from public network to our Web server is 100 per second with peaks up to 120 TCP sessions per second, with maximum of 10 sessions from single public IP, then It would make sense to have alarm set on 150 TCP sessions per second and 20 sessions from single public IP. IPS rules could step in by denying connections from public IPs with more than 20 sessions from single IP and drop all connections from that public IP.

Let's say that during singe TCP session the average transferred data is few kilobytes before the session is closed. So in case a single session already transferred couple of megabytes, it is a suspicious connection (attacked is dumping our database or getting some files) so again, connection can be dropped and new connections banned from the same public IP.

Similar alarms and rules can be implemented for communication between Web and App servers, and as well between App and DB servers.

What I am trying to say is that I would recommend to spend the time of monitoring the behavior to be able to fully understand the usual patterns. If the IDS/IPS rules are adjusted correctly, then these systems would be beneficial for us in order to stop an attack immediately and to be able to see what is happening in our environment.

Log analysis

For log analysis I would recommend to use VMware Log Insight as the tool has a great possibilities of log management, sophisticated analytics, extensibility and fast troubleshooting. There are two ways how to get the syslog messages to VMware Log Insight. The syslog server can send a copy of received messages to Log Insight, or all systems can send the syslog messages to two destinations.

All of these will apply in a case of manual analysis with the standard troubleshooting approach but as we look more on automated solution we have to implement different tool.

As the right tool for the job I have chosen Flowmon. The software is able to detect anomalies and undesirable behavior as attacks, anomalies in data traffic, anomalies in device behavior, undesired applications, security issues (viruses, spyware, botnets), email traffic, operations problems and potential data leakage. This was one of the reasons why I selected this software. Software can be implemented as a Virtual Appliance as well as a SaaS which is beneficial as there is no need for a dedicated HW. Flowmon is using standard protocols (NetFlow, IPFIX, NetStream, jFlow) which are implemented in most of the network devices. Software can detect security incidents in real-time and give us possibility to investigate and proved them. Its also possible to eliminate illegal software and services or abuse of the network by employees.

Flowmon will be implemented on physical network devices as well as on vSphere networking. Physical network devices will provide us traffic monitoring on the North-South traffic, vSphere networking on the East-West traffic. So we will be able to monitor the traffic patterns coming from public networks as well as traffic between virtual machines in our environment.

DDoS attacks

Flowmon ADS is able to detect and block DDoS attacks with the FlowMon DDoS Defender. The attack can be detected in sub 60 seconds timeframe. Mitigation of the attack can be triggered automatically when attack is detected with use of the BGP Flowspec protocol. Once the attack has been detected Flowmon will send a BGP Flowspec advertisement to BGP Flowspec aware router/firewall to block certain source-destination connection. So instead of dropping all traffic to our server, we will drop a specific data flow. So the service will be available for regular users and the DDoS attack will be mitigated.

Traffic recording

To prove or deeply investigate the compromised network traffic, we will use Flowmon Traffic recorder. This tool will provide us with on-demand full packet capture and recording or a complete packet trace and analysis to provide an effective network problem identification and resolution. Network capture criteria can be based on IP addresses, MAC address, port number, etc.

All what was described so far is providing us with the functionality of finding the changes anywhere within the system so it covers the task A: find the extend of the change anywhere within the system.

Task B: be notified of other changes, not just to files but to attack(s), what is the steps of an attack, how fast can you detect an attack and changes?

We have static IDS rules in place, which will notify us if something suspicious has been detected. We have also automated Network Behavior Anomaly detection tool is place. Flowmon is able to detect anomalies in real-time so we can detect an attack instantly.

Task C: prevent the changes, can you prevent the attack or just detect the attack. If only detection how fast can you make this happen.

Well known attack patterns can be blocked immediately with the use of IPS. DDoS attacks can be blocked in less then 60 seconds with the use of Flowmon DDoS Defender. More sophisticated attacks will be monitored with Flowmon ADS.

Task D: determine the root of the attack, can we find the culprit, is there any forensics data, where did the 'bad actor' leave his/her fingerprints. Is it the black market or something else?

Once we will be notified about anomaly (intrusion, infection) in our network we can use Flowmon Traffic recorder to capture the related data for deep analysis. We will use these tools to deeply investigate the range of the intrusion and then create a mitigation plan to cleanup our environment. We can use our IPS to stop the intrusion and adjust the environment configuration to avoid similar attack in the future.