Morgan State University, Electrical and Computer Engineering Department
Virtualization for Telemetry Network

Authors: Perry Jordan, Favour Okonkwo

Advisors: Dr. Farzad Moazzami, Dr. Richard Dean, Dr. Wondimu Zegeye, Dr.Mulugeta Dugda, Daryl Morten.

Abstract:

Our world is changing fast and many companies have graduated to task automations, Artificial Intelligence and Machine learning, virtual and Augmented Reality, Blockchain, IoT, and many more. To aid this progression, more intensive and complex computing has been undeniably pivotal, more data has been generated and stored, and above all, more measures have been required to protect both data and functionalities of these advancements.

Really, how relevant or advanced is a system if any unauthorized or unqualified person has access to its database, networks or functionality?

This paper breaks down the use of hardware virtualization tools to develop testbed systems that test for vulnerabilities in a telemetry network. Put simply, we are developing a testbed that will model an enterprise of telemetry networks. We will then launch attacks on these networks and test the vulnerabilities of the client machines to ascertain the level of vulnerability of the client machines.

There are a number of components included in the Testbed such as routers, switches, LANs, Virtual machines, connectors, firewalls, etc. The virtual machine here is a VMware workstation.

Introduction:

The use of Telemetric systems was first recorded in the 19^{th} Century. These systems consisted of automated communication models that were designed to allow data to be collected and shared remotely, and with some degree of accuracy and ease. The data or information shared can then be used for any type of computing or mere review. One advanced, yet typical application of advanced telemetry is cloud computing. Others include Radio networks and various wireless communications.

Visualizing the Concept of a Telemetry System

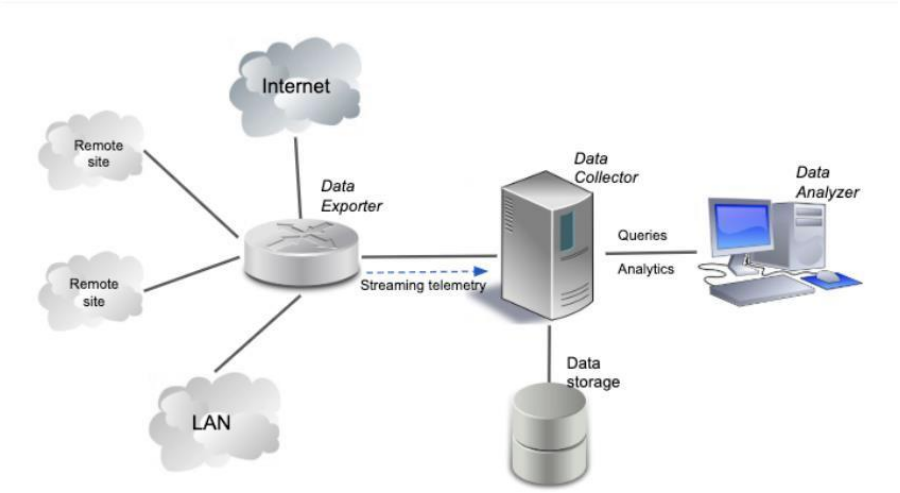


Image credit: https://www.netreo.com/blog/network-telemetry-it-executive-guide/

However, networked telemetry has come a long way and with more advancements have come new threats and vulnerabilities that the conventional telemetry systems may not have possessed. We plan to exploit these vulnerabilities, analyze the results from the exploitations, and implement rigid defense strategies to combat these vulnerabilities.

MSU and the Telemetry System:

Morgan State University Wireless Networks and Security Lab (WiNetS), team is building a telemetry testbed that will model real-life telemetry structures and simulate testing of cyber-attacks and optimal defense strategies.

The telemetry community's initiative to deploy network centric solutions has been the focus of its initiatives this past decade. The development of the Integrated Network- Enhanced Telemetry (iNET) protocols and the strategy for networked operations offers improvements to both performance and efficiency of telemetric operations. One of the major setbacks that occur in operations like these is an increase in the vulnerability of telemetry networks to different attacks. These attacks can range from Intrusions, exfiltration, and unauthorized penetrations, as well as other numerous cyber security attacks.

Many telemetric networks share the same challenges and cyber-attacks as other enterprise networks. Their networks also have a number of specific attributes that cause them to be targeted and vulnerable. We already know that Telemetry networks

are similar to Supervisory Control and Data Acquisition (SCADA) enterprise systems. However, the unique network architectures identified in the iNET standards can help us to be precise in our approach.

The ideal approach and effort is focusing on developing cyber security solutions that are tapered uniquely towards the nature and architecture of telemetry networks.

As stated earlier, the unique network architectures identified in the iNET and related standards can help us to be focused in our approach. With that knowledge, we will model the telemetry network with the presumption that the ground station will comprise traditional enterprise networks and SCADA-like systems. This presumption allows us to leverage previous extensive studies of numerous cyber vulnerabilities within SCADA networks. Due to SCADA's role in industry, as well as its need to be impenetrable, providing adequate protection and protective measures to SCADA systems is paramount. Newer systems that support SCADA are based on Internet Protocol (IP) and Ethernet.

The approach of this paper is to illustrate the foundation and explore cybersecurity issues that exist within a Network-Enhanced Telemetry architecture.

Approach

For this project, we will set up multiple virtual machines (VMs) (using VM-ware) that will serve as both the intruder and the client. We plan to utilize the Linux operating system as the attacking machine, and different versions of the windows operating system will serve as the client machine. Multiple intrusion tests will be run using Kali Linux to determine the vulnerabilities within the different Windows Operating systems in the network of systems that we will build i.e., the Testbed.

Even though we will be dealing with virtualization, we still need to make room for a physical computer that will act as the general-purpose machine to run these virtualizations. This physical component/hardware will be able to cater to multiple host machines all at once. This computer must be a high-performing workstation that can handle the demanding volume and intensity of the project. In addition, the workstation, with all its specifications, will provide excellent support for virtual machines, switches, routers, etc. that will enable our networks to run efficiently.

Why Kali?

Kali Linux is an Advanced Penetration Testing Linux Distribution that is employed for Penetration and vulnerability testing. This Linux version provides multiple penetration and intrusion applications and software that can be readily used to exploit vulnerabilities in any or most operating systems. Some of these tools include Nikto, Aircrack-NG, Nmap, and *Wireshark*.

The Testbed

As mentioned earlier, the testbed is a network of Operating systems running virtually and housed by a physical machine. It consists of sophisticated hardware (the physical host machine) and software running on the hardware. Combined, we have a cyber security testing environment where we will perform multiple intrusion detection and vulnerability tests. The test environment will all be virtual, and the attack machine will be the Kali version of the Linux Os.

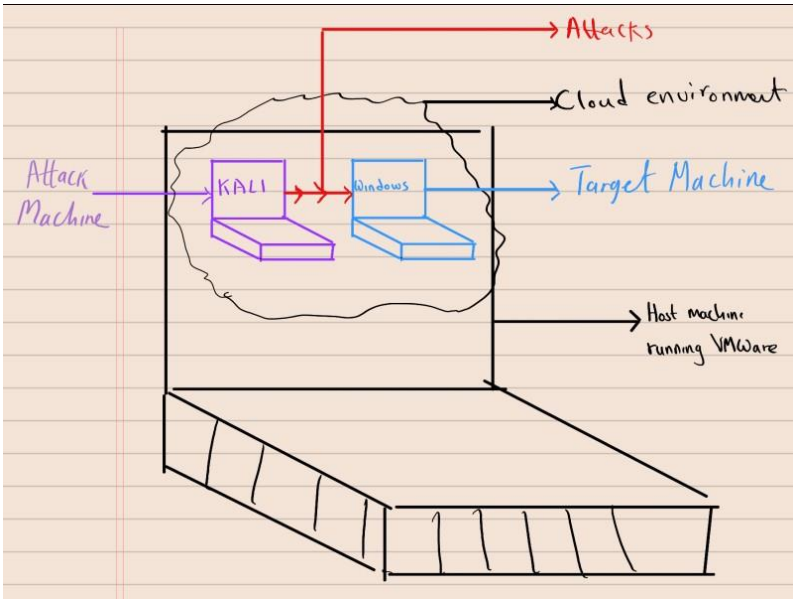
Some of the tests will include vulnerability testing, analysis of intrusion detection systems, etc. We will use a minimum of two solid state drives so keep track of the virtual data and the boot data.

VMware Workstation

Why virtual machines? Typically, a Virtual machine is a cloud environment that imitates a physical machine. We decided to use VMs as they are easy to set up and deploy. The fact that they allow users to run just about any operating system makes them very versatile and just the right environment for conducting tests on different types of OSs. Also, they are cost effective, portable, and accessible from remote locations; allowing multiple researchers to collaborate efficiently regardless of their physical locations.

The machines will employ scalable Intel CPUs that support multi-core functionality, thus maximizing the efficiency and ability of the testbeds. Typically, we will attack the testbed networks with multiple intrusion methods and then conduct result analysis in order to figure out how best to edify it so that it can better self-protect itself.

Simulation of Host machine and attacks



VSphere Computing:

VSphere was developed and launched in May 21, 2009. It virtualization platform that provided extra support for cloud computing. VSphere has increased the efficiency and scalability of virtual machines, allowing them to in turn provide more support to users.

VMware vSphere is VMware's virtualization platform, which transforms data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. vSphere manages these infrastructures as a unified operating environment, and provides you with the tools to administer the data centers that participate in that environment(https://docs.vmware.com/en/VMware-vSphere/index.html). With VSphere, virtualization is smooth and expected outcomes are reliable. It also allows applications to be transferred from one host to another with no downtime in between.

VSphere working architecture model

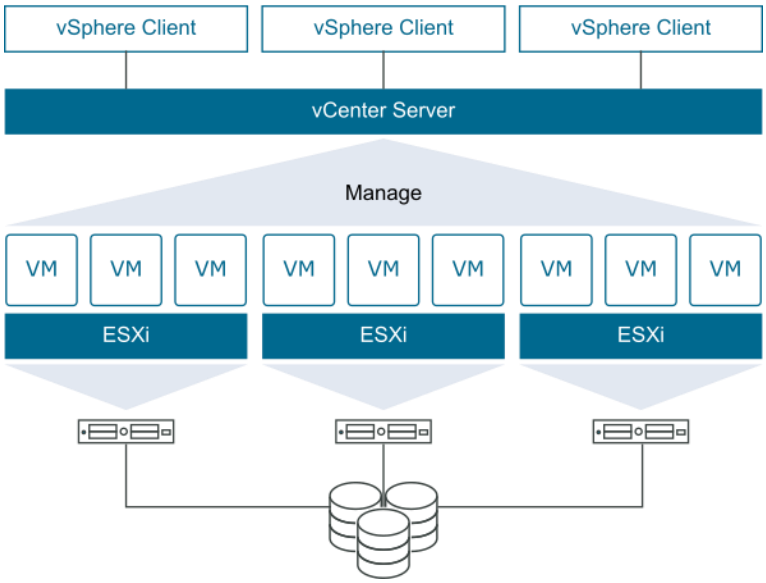


Image credit: https://docs.vmware.com/en/VMware-vSphere/index.html

VSphere ESXI

One of the core components of VSphere, ESXI, is the virtualization platform that allows users to run virtual machines as well as other virtual appliances. VMware ESXi is a next-generation hypervisor the foundation for an optimal virtual infrastructure. This ingenious architecture operates on its own, not needing or depending on any general-purpose operating system, thus providing enhanced security, reliability, and simplified management. The architecture is compact and is designed for it to be directly integrated into any virtualization-optimized server hardware. This compact design enables easy installation, configuration, and deployment of the software.

Conclusion

We are developing a system using the concept and knowledge of Telemetry networks. This system will be built with a workstation that will run a high-performance virtual machine. The Virtual machine will host two unique and independently yet simultaneously running Operating systems, namely Kali Linux and Windows XX. The former will serve as the attacking machine, while the latter, the target machine.

We look to employ results from our tests to develop enhanced defense strategies for telemetry networks in total.

REFERENCES

1. https://www.hcr-llc.com/blog/telemetry-systems-what-are-they-and-how-do-we-use-them

2. https://www.netreo.com/blog/network-telemetry-it-executive-guide/

3. https://www.kali.org/tools/

4. https://docs.vmware.com/en/VMware-vSphere/index.html

5. vSphere 4.1 - ESX and vCenter, Overhead Memory on Virtual Machines. http://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphereresourcemanagement.doc_41/managing_memory_resources/r_overhead_memory_on_virtual_machines.html

6. vSphere Hypervisor; http://www.vmware.com/uk/products/vsphere-hypervisor/

7. ESXi and vCenter Server 5.5 Documentation, CPU Compatibility and EVC; https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.vcenterhost.doc%2FGUID-03E7E5F9-06D9-463F-A64F-D4EC20DAF22E.html