Developing a Telemetry Cyber Security Testbed

Authors: **Uchenna Emerson, Tobechukwu Osuzoka**

Faculty Advisors: **Dr. Mulugeta Dugda, Dr. Farzad Moazzami, Dr. Wondimu Zegeye, Dr. Richard Dean**

Abstract

Networking is a very important concept today. It is a concept that keeps advancing as new technology is discovered. We access the network throughout our daily lives, whether it is by our phone, television, computers, WIFI, radios, cars, or any other technological devices that are used on a daily basis. The two most common networks that are used are the Local Area Network (LAN) and the Wide Area Network (WAN). A LAN is usually used for one specific area in which it has a distance limit and a limited number of computers the network can be accessible to. It is usually used for the workplace or at home. Unlike a LAN, a WAN is able to be used in large geographic areas. It usually consists of multiple LANs across a large area. These networks are created to the cloud in which it can be configured with virtual machines and hosts.

When it comes to VMware, it operates as a network in the cloud where people or businesses can operate from. Users can use a physical server to initiate the virtualization of machines that can be used for applications such as excel, word, DNS, NTP ERP, etc. and operating systems such as windows and Linux devices. Many people and companies prefer virtualization because it is cost efficient, it uses electricity, it is easy to manage, it is fast to initiate the deployment of the machines, and it is better for testing and performs greatly.

Introduction

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 enhancements to the performance and efficiency of telemetry operations. The challenge associated with this initiative is the increased vulnerability of telemetry networks to cyber security attacks. Foreign adversaries such as China have notable cyber-attack capabilities, a history of active engagement, and a record of success in penetrating and exfiltrating data from US government and industry networks. It is reasonable to assume that such adversaries have successfully penetrated our networks!

Telemetry networks share many of the challenges associated with cyber-attacks as do most enterprise networks. Telemetry networks however have several unique properties that make the threats and vulnerabilities more relevant, and structures that can be insightful to security solutions. Telemetry networks are a form of Supervisory Control and Data Acquisition (SCADA) enterprises such as the power grid. Work in this area can enlighten our work. Further the network architectures identified in the iNET standards can narrow the focus in our approach. The proposed effort is focused on cyber security solutions that are tailored specifically to the nature and structure of telemetry networks and the threats and vulnerabilities associated with these.

In modeling a telemetry network, we consider the ground station to comprise traditional enterprise network and Supervisory Command and Data Acquisition (SCADA) systems. This allows us to build on the many studies of cyber vulnerabilities in SCADA networks. SCADA systems are among the most widely used industrial control systems (ICSs) that enable the controlling and monitoring of process equipment on multiple sites that spread over large distances. SCADA systems are cyber-physical systems with communication networks interfacing the monitoring and

control system with the hardware and these could have multiple supervisory systems, programmable logic units (PLCs), remote terminal units (RTUs), human–machine interfaces (HMIs), process and control instrumentation, sensors, and actuator devices over a large geographical area. SCADA systems make use of both new and legacy systems, including traditional information systems. SCADA systems are not only as vulnerable as any other networked computer systems, but their legacy systems create another layer of threat. Since many of these systems have existed for decades, their cybersecurity risks are unknown and challenging to analyze as well. These SCADA systems resemble much of the networked telemetry systems that we intend to model and therefore represent a good starting point.

In our concurrent study, we have captured a network-enhanced telemetry architecture for the purpose of modeling and analysis for cybersecurity risks. We show how telemetry systems can be modeled as an ICS-SCADA system that merges with an enterprise network. In addition, it shows how this architecture can be transformed into an IoT reference architecture to make use of cloud service capabilities. The main goal of this paper is to lay the network foundation to explore cybersecurity issues with an Integrated Network-Enhanced Telemetry architecture. This cyber domain is going to include vulnerabilities as- sociated with ICS-SCADA, enterprise networks, and cloud networks. Future work will develop a cyber telemetry test bed for vulnerability analysis. It reflects our understanding of telemetry and SCADA and the commonalities and paves the way for our future work for the International Foundation for Telemetry (IFT). This will enable setting up and configuring a hybrid (hardware and virtual machine)-based telemetry testbed, exploring different domains of cyber vulnerability analysis, looking into different threat actors with an emphasis on insider attacks, and modeling and developing cyber defense methodologies.

Problem Statement

By configuring a cloud computing network, we will be able to create a virtual database that consists of a variety of network elements. This paper describes the network elements that are used in a telemetry testbed system. There are various elements that are used in a network configuration. These components include but are not limited to routers, switches, connectors, firewalls, and LAN. By using a Vsphere software, we will be able to create these elements and through it. Each of these network elements will be taken through a series of attacks in which we will analyze and modify to be improved on. We will be reporting an in depth analysis of each element, the kind of components they consist of, and the results of each element after attacks are done.

VMware Workstation

By running several x86-based operating systems simultaneously on the same PC, VMware Workstation revolutionizes the way technical professionals build, test, demonstrate, and deploy software.

VMware Workstation, which is based on 15 years of virtualization expertise and has won more than 50 industry awards, takes desktop virtualization to the next level by providing users with unrivaled operating system support. VMware Workstation, which is based on 15 years of virtualization expertise and has won more than 50 industry awards, takes desktop virtualization to the next level by providing users with unrivaled operating system support, a dynamic customer experience, and great performance.

VMware Workstation makes use of cutting-edge hardware to create virtualized server, desktop, and tablet environments. Run apps from a variety of operating systems, such as Linux, Windows, and others, on the same PC without having to reboot. VMware Workstation enables evaluating new operating systems, software applications and fixes, and reference designs in a

secure and isolated environment. No other desktop virtualization program compares to Workstation in terms of performance, stability, and cutting-edge capabilities.

VSphere

Vsphere is the cloud computing virtualization platform for VMware. It was developed in 2009, being a full platform for deploying and managing large-scale virtual machine (VM) infrastructure. Virtual machines and the servers on which they reside are pooled into a cluster by VMware to ensure high availability. The cluster's hosts are watched, and if one fails, the virtual machines on that host are restarted on alternate hosts. ESXi, vCenter Server, vSphere Client, vCenter Orchestrator, and vSphere Update Manager are all part of the VMware vSphere software suite. Virtualization, management, resource optimization, and many other functionalities are provided by vSphere components in a virtual environment.

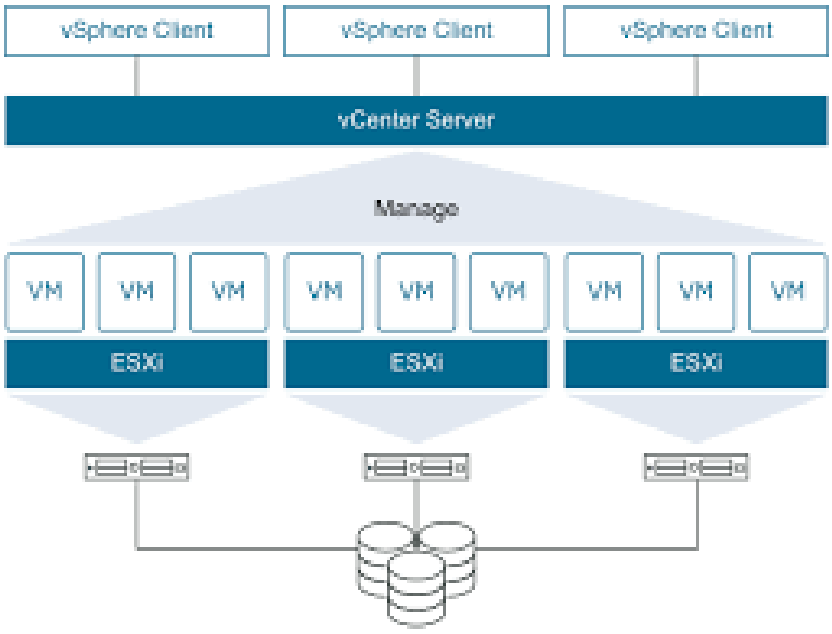

Figure 1. A diagram of VMware's vSphere platform, which composes other important features which ensure virtual servers are moving properly. This includes VMware ESXi, vCenter Server and vSphere Client

ESXI

The VMware ESXi Server is a more powerful, smaller version of VMware's enterprise-level computer virtualization software product, the VMware ESX Server. ESXi, which is part of the VMware Infrastructure, allows for centralized control of enterprise desktops and data center applications. "ESX integrated" is the abbreviation for "ESX integrated." VMware ESXi began as a smaller version of VMware ESX that required only 32 MB of disk space on the host. The hypervisor ESXi is at the heart of the vSphere product suite. A hypervisor is software that allows you to create and run virtual machines. There are two types of hypervisors:

- Type 1 hypervisors, commonly known as bare metal hypervisors, run on the system's hardware directly. A guest operating system runs above the hypervisor on a different level. VMware ESXi is a Type 1 hypervisor that runs without an underlying operating system on the host server hardware.
- Hypervisors of type 2 run within a traditional operating system environment, with the host operating system providing I/O device support and memory management. VMware Workstation and Oracle VirtualBox are examples of Type 2 hypervisors.

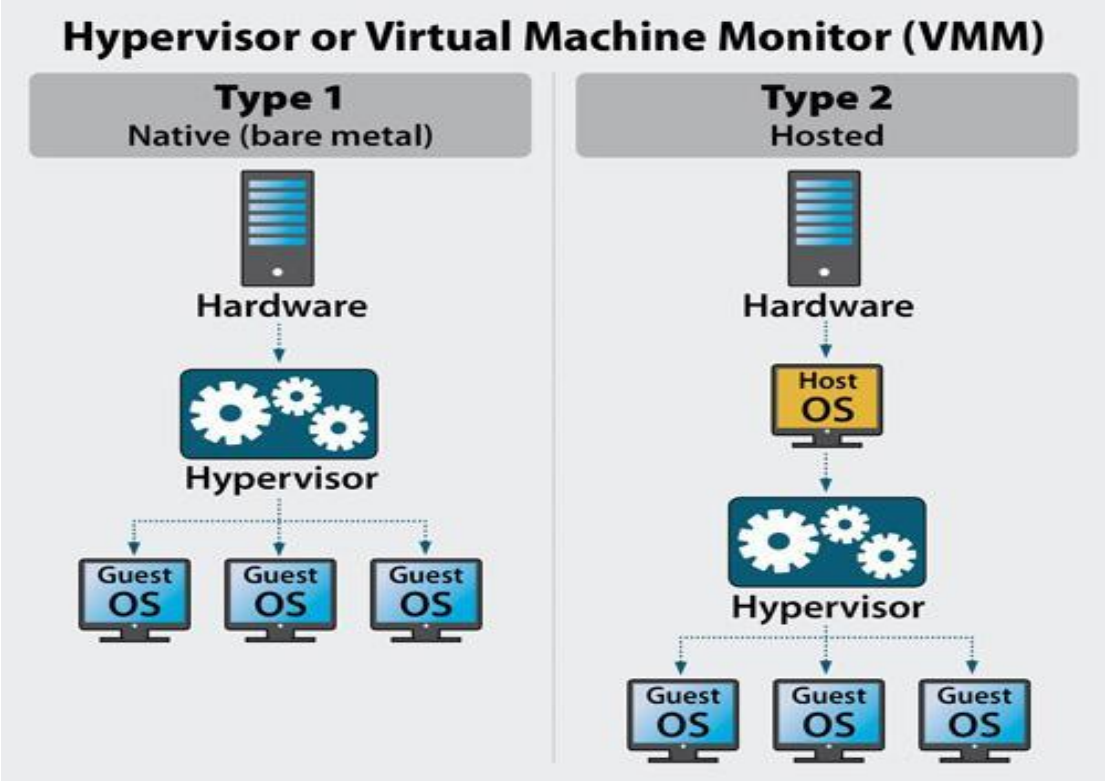

Figure 2. ***Type 1 and Type 2 hypervisors. Type 1 hypervisors are also referred to as "bare metal" because they are usually installed, running VM's on the computer's hardware, as Type 2 hypervisors are referred to as "hosted" since they run as normal applications on operating systems.***

The virtualization layer in ESXi isolates the actual host's CPU, storage, memory, and networking resources into numerous virtual machines. This implies virtual machine programs can utilize these resources without having direct access to the underlying hardware. The hypervisor utilized by VMware ESXi is referred to as vmkernel by VMware. Virtual machines send requests to vmkernel.

Intel (Xeon and above) and AMD Opteron CPUs are both supported by ESXi. The VMkernel in ESXi is 64-bit, thus hosts with 32-bit CPUs aren't supported. Guest operating systems

are supported in both 32-bit and 64-bit versions. Up to 4,096 virtual processors, 320 logical CPUs, 512 virtual machines, and up to 4 TB of RAM per host are supported by ESXi.

VCenter

VCenter Server is a program that allows you to manage your VMware vSphere infrastructure from a single location. It serves as a single point of administration for all ESXi hosts and virtual machines. You may install vCenter Server on a compatible version of Windows or utilize the vCenter Server Appliance, which is a preset Linux version. Advanced vSphere capabilities include vSphere High Availability, vSphere Fault Tolerance, vSphere Distributed Resource Scheduler, VMware vSphere vMotion, and VMware vSphere Storage vMotion all need vCenter Server. A single vCenter Server instance can support up to 1,000 hosts, 10,000 virtual machines that are switched on, and 15,000 virtual machines that are registered.

Both the vSphere Client and the vSphere Web Client may be used to administer your vCenter Server. When an ESXi host is managed by vCenter Server, the vSphere Web Client is the recommended way to manage it. The inventory items, resource pools, performance statistics, and other information are stored in the vCenter Server database. vSphere administrators may use vCenter server to manage numerous ESXi hosts and virtual machines (VMs) from a single interface. You gain better insight into vSphere's setup of your essential components via a single console. The VCenter server is responsible for resource provisioning, workflow automation, performance monitoring, and user administration, among other things. You may, for example, manage hundreds of tasks, boosting productivity that would otherwise be impossible to do with physical infrastructure.

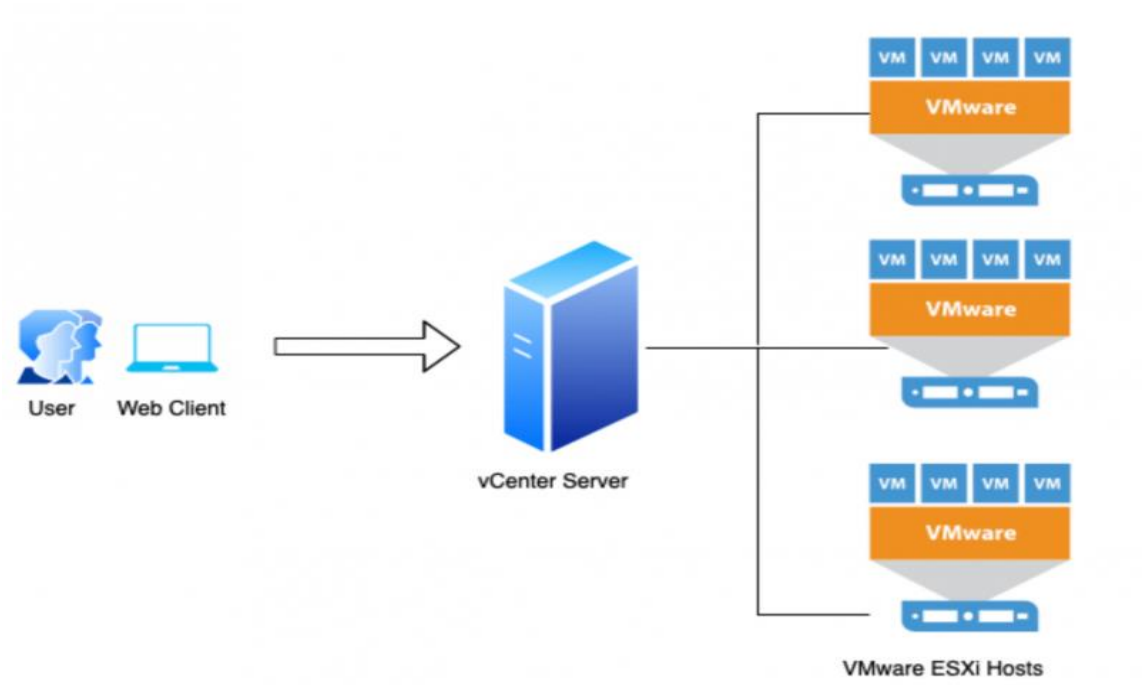

Figure 3. A diagram showing interaction between a user using vSphere Web client to connect to a vCenter Server. Doing so allows the user to manage the vSphere deployment.

The OSI Networking Model

The OSI model was created to improve portability by establishing a standard for network data transfer across computers and components with varying hardware, software, operating systems, and protocols. The OSI Reference Model's goal is to offer a framework for both developing and describing networking systems. The presence of the model makes it easier to study, create, build, and reorganize networks by allowing them to be thought of as parts that work in controlled situations.

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

- Application Layer - Layer 7 of the OSI Model enables application and end-user operations. Communication partners are identified, service quality is assessed, user authentication and privacy are taken into account, and any data syntactic limitations are recognized. At this layer, everything is application-specific. Application services like file transfers, e-mail, and other network software services are provided by this layer.
- Presentation Layer - By translating from application to network format and vice versa, this layer enables independence from variations in data representation (e.g., encryption). The presentation layer is responsible for converting data into a format that the application layer can understand. This layer formats and encrypts data before sending it across a network, ensuring that there are no compatibility issues.
- Session Layer- Connections between applications are established, managed, and terminated by this layer. Conversations, exchanges, and dialogues between the apps at either end are set up, coordinated, and terminated by the session layer. It is responsible for the organization of sessions and connections.

- Transport Layer- Layer 4 of the OSI Model is responsible for end-to-end error recovery and flow management, as well as providing transparent data transport between end systems or hosts. It guarantees that all data is sent completely.
- Network Layer- Layer 3 includes switching and routing technologies, allowing data to be sent from one node to another via logical routes known as virtual circuits. Routing and forwarding, and also addressing, debugging, congestion control, and routing protocol, are all functions of this layer.
- Data Link Layer- The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer are two sublayers of the data link layer.
- The MAC sublayer governs how a networked computer obtains access to data and authorization to send it. Frame synchronization, flow management, and error checking are all handled by the LLC layer.
- Physical Layer- At the electrical and mechanical levels, Layer 1 of the OSI Model transports the bit stream – electrical impulse, light, or radio signal – over the network. It defines cables, cards, and physical elements, as well as the hardware for delivering and receiving data on a carrier.

Network Telemetry

Telemetry is the automatic transfer of measurements or other data from remote or inaccessible locations to receiving equipment for monitoring. Network equipment such as routers, firewalls, and switches provide real-time data to one or more centralized sites for storage, processing, and analysis in network telemetry. Network Telemetry is an important part of any modern data center operation. The foundation for effective network automation and analytics is

insight into what a network is doing and how it is being used. Telemetry, or more precisely streaming telemetry, has the potential to speed up network troubleshooting, predict network capacity expansion, and establish baseline network performance.

The Cybersecurity Testbed

A cybersecurity testbed will be created with VMware. Testing, vulnerability analysis, intrusion detection systems, and network analysis are just a few of the cyber security disciplines that can be explored on the test bed. It will be using two solid state drives to separate the virtual data from the boot data, keeping data organized in the testbed. It will be using 2 scalable Intel CPU that has ten cores for each unit. This will make the testbed to contain 20 cores in which each can be used to their maximum efficiency. The Video Card that would be used is a GIGABYTE GeForce GTX 1050 ti. It would be preferred to provide the full capability of the testbed with the 4GB of space and the speed in running the VMware software on the testbed. We will be testing the vulnerability of the testbed by sending attacks through a software. Once analysis has been conducted, we will improve on the durability of the testbed in order to increase it strength of protecting itself against virtual attacks.

Conclusion

Workstation provides technical experts complete control over how virtual machines are set up and interacted with. Cyber-attacks are prevalent today and there is increasing consciousness across all industries to combat this menace. This paper demonstrated by example the vulnerability of future networked telemetry to cyber-attacks. To save time, it helps with the choosing from a range of choices for installing, protecting, connecting, sharing, and observing virtual machines.

By configuring this network, we will be able to connect a well suitable network environment for people or companies in which provides top-notch security in the virtual environment.

References

[1] 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

[2] 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

[3] vSphere Hypervisor; http://www.vmware.com/uk/products/vsphere-hypervisor/