Global Information Assurance Certification Paper

Shoestring Virtualization – Reducing the Risk to Small Business Data from Compromised Remote Networks

GIAC (GSEC) Gold Certification

Author: Christopher Jarko, csjarko@yahoo.com
Advisor: Stephen Northcutt
Accepted: August 27, 2015

Template Version September 2014

Abstract

Many organizations with significant amounts of data worth protecting also have robust security awareness programs and clear, detailed security policies. When employees from these companies remote in from an infected network, what happens then? A user can be fully compliant with all organizational policies and procedures and be up to date on all security awareness training, but the networks used to remotely access corporate data are populated by users beyond the scope of organizational policy. The use of Virtual Private Networks (VPNs) to remotely access organizational networks has become commonplace, but this may not be enough. This paper will examine different technical approaches to mitigate the problem. Companies can restrict remote access to company-issued hardware, which has benefits but also carries significant costs. Another option is to provide enterprise virtual desktop infrastructure, but this is cost-prohibitive for many small businesses. Local desktop virtualization provides the best solution. Using software such as VMware Player and a custom-built, restricted image provides the company full control of the desktop environment and can restrict data storage to company-controlled servers.

1. Introduction

1.1. Introducing risk from compromised networks

Mobility and remote access is a necessity for many companies; salespeople, technicians, and executives must often travel as part of their jobs. While on the road, these employees often cannot afford to lose touch with their main offices, and telephone connectivity may not be sufficient. Invoices and purchase orders need to be filed, employees need to send and receive E-mail, and company files, such as technical documents, need to be accessed and possibly even modified. Remote connections to corporate IT infrastructure are typically originate from networks beyond the company's control, circumventing even the most well thought out and rigorously enforced information security programs.

Some networks are more notorious than others; open Wi-Fi access is a well-known risk. The very nature of an open wireless network means any data transmitted over the network is vulnerable to packet capture and protocol analysis tools such as Wireshark (Chappell, 2013). Wired Ethernet connections reduce the attack surface, but they are not always safe. In 2014, the U.S. Secret Service and Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) issued a non-public advisory to the hospitality industry warning of keylogger malware discovered on computers in hotel business centers in the Dallas-Fort Worth area (Krebs, 2014).

Home networks are also a source of risk to corporate data. While the numbers vary, a sampling of reports and white papers would indicate infected home networks are not uncommon. On his personal blog, Eugene Kaspersky put the number of infected (Windows) home computers at 5 percent worldwide (Kaspersky, 2013). On the other hand, Alcatel-Lucent's Motive Security Labs placed the number of infected home networks at 14 percent (Alcatel-Lucent Motive Security Labs, 2015).

1.2. Caveats

Publicly available data breach reports do not contain sufficient detail to attribute the source of the breach to a particular compromised network. Instead, reports often stop at categorizing a breach as "hacking" or "malware" (Privacy Enforcement and Protection

Unit, California Department of Justice, 2014). This may be due to an inability to attribute the attack, as was the case in the 2014 breach of the University of California, Davis Health System (University of California, Davis, 2015). In any case, there are no references in this paper which will draw a straight line from one specific infected remote network to a corporate data breach.

1.3. Relating the threat to risk: an example

In the absence of such a concrete reference, the following scenario is provided as a plausible example of how a compromised remote network could lead to a corporate data breach:

An employee has a home network used by his wife and teenage son. One afternoon, the employee's wife opens a phishing E-mail purporting to be from the family's bank and clicks on an attached document, downloading keylogger malware known as Dynasty onto the home computer. Dynasty malware gives the attacker access to anything typed on the computer, as well as the ability to capture screenshots of the victim's desktop (Ilascu, 2014). That evening, the employee uses the same home computer to access his company's E-mail and database servers with his login and password. Later that night, the attacker directly logs into the corporate servers using the employee's valid credentials and a target IP address obtained via Dynasty.

An employee may comply with all policies at work, but not at home. On the other hand, an employee might observe sound security practices at home as well as at work, but as shown in the above example, the employee's family members might engage in poor security behaviors. According to a paper presented at the 2012 Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy, home computer users generally do not accurately perceive the risks of their behavior; even when the users are aware of the risks, their behavior does not necessarily align with their knowledge (Howe, Ray, Roberts, Urbanska, & Byrne, 20-23 May 2012). In any case, the data suggests home computer users represent a vulnerability to corporate data.

1.4. Scope

This paper will look at solutions within the reach of small companies with limited financial and IT resources. The reasoning behind this approach is to make it applicable to more organizations.

For the purpose of this paper, our exemplar company has no more than 20 employees and a small IT team with two or three IT specialists, who are only available during normal business hours. (The requirement for multiple IT specialists will be explained later.) This paper assumes remote access is required for specific duties, such as traveling sales or technical support and senior management travel, but not telecommuting, which would require a complete desktop rather than a customized version with fewer applications. Finally, this paper assumes the employees' home computers use a variety of Operating Systems (OS), including Mac and Linux in addition to Windows.

1.5. Virtualization

This paper will focus heavily on virtualization. In the broadest sense, virtualization refers to the use of software to create a logical representation of a computer, separating the OS from the physical hardware (IBM Systems and Technology Group, 2007). Each virtual machine (VM) is referred to as a "guest," while the OS installed permanently on the physical computer is called the "host OS," and the physical computer itself is the "host" (Golden, 2007). The guest OS accesses the host computer's physical resources through a software application known as a virtual machine monitor, more commonly called a hypervisor (Portnoy, 2012). For a more comprehensive overview of virtualization, please see *Virtualization Essentials* by Matthew Portnoy.

1.5.1. Virtualization vendors

There are several prominent third-party vendors of virtualization software. VMware, Oracle, and Citrix are the most popular, and all of them make products capable of isolating corporate data from infected home networks. The main difference between these products is price. A few specific price differences are given later, but in general, VMware is more cost-effective and is the software used in this paper.

This begs the question: "What about Microsoft Hyper-V?" According to Microsoft TechNet, Hyper-V is a role in recent versions of Windows Server (2008 and later) which allows for provisioning of virtualized networks (Microsoft, 2013). Windows 8 or 8.1 can also act as a Hyper-V host, but Mac OS, Linux, and older versions of Windows cannot (Microsoft, 2014). Therefore, Hyper-V is not a suitable solution for the purposes of this paper.

1.5.2. Why virtualization?

Containerization of computer environments – the essence of virtualization – creates an opportunity to provide a clean guest OS running in a VM on a compromised host. This is the means by which this paper will demonstrate how to build and distribute VMs for remote access.

2. Technical Solution: Isolating the corporate network from the remote network

2.1. Less than ideal solutions

There are a number of strategies to mitigate the risk from infected remote networks. For a company with a large budget and a robust IT department (as well as the willingness to use the former for the latter), there is a wide range of options. Unfortunately, most companies need to find a solution that is economical in terms of cost and labor. This section of the paper will begin by examining three options *not* suitable for the target company.

2.1.1. Company-issued hardware

The simplest means of isolating the two networks is to have employees use only company-issued hardware to connect to company servers via secure means. Company laptops can be issued with whatever desktop configuration the company chooses, allowing for standardization. The employees can customize minor features, such as the choice of desktop wallpaper or which applications have desktop shortcuts, but other configuration aspects, such as software load or disk mapping, could be "locked down" to maintain compliance with company policies and standards. While this option may be feasible for a small company if remote access is infrequent and limited to a few

employees, the costs grow quickly if this option is widely used. In addition to the initial purchase cost, there is the cost of maintaining the laptops. This falls under the total cost of ownership (TCO), which is defined by Gartner Research as, "…a comprehensive assessment of information technology (IT) or other costs across enterprise boundaries over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses." (Gartner, Inc., 2014). Even if the company reliably uses TCO when making IT decisions, adjustments might need to be made to account for additional wear and tear on the laptops for being packed up and moved on a daily basis if the laptops are not physically robust. Finally, issuing laptops must make sense within the company's business model and IT architecture.

2.1.2. Enterprise-level virtualization

In an unconstrained environment, perhaps the ideal solution is to provide full Virtual Desktop Infrastructure (VDI). VMware offers Horizon FLEX, which allows users to access restricted, containerized Windows-based desktops from either Windows or Mac computers (VMware, 2014). Naturally, this does not come cheaply; Horizon FLEX is priced at $3,025 per package of ten licenses (VMware, 2015). Citrix makes a comparable product called XenDesktop which is less expensive ($1,020 for 10 licenses), but like Horizon FLEX, licenses for the virtualized Windows applications are not included (Citrix Systems, Inc., 2015). Also, VDI implementation requires a fairly robust data center (Citrix Systems, Inc., 2014). This puts VDI out of the price range of many small companies; since this paper is intended to provide a solution for more financially constrained organizations, the paper will use virtualization on a smaller scale.

2.1.3. Live boot

A specific implementation of virtualization known as "live boot" allows a user to boot a computer using an OS stored on specially configured removable media such as a CD-ROM disk or USB drive (Notenboom, 2012). This option is very user friendly; simply load the CD or plug in the USB drive, reboot the computer, and use the provided desktop. From a cost perspective, this solution is the cheapest, especially if the company opts to use an open source Linux distribution ("distro") for the VM. What makes this

method unsuitable is that while the guest OS resides entirely in the host computer's RAM, the VM can still map directly to the host's hard disk drive (Notenboom, 2012). This creates a vector for data loss from the corporate server to the remote host. It is possible to eliminate this risk either by using non-rewritable optical disks or by configuring the live boot media to operate in "non-persistent" or "live mode" (Lauzière, 2013). These last two options are unsuitable for this paper because the lack of persistence means software updates are not retained after shutting down the VM, either forcing the user to manually update every time the VM is used, or forcing the company to reissue live boot media every time an update is available.

2.2. Recommended solution: Local (client hosted) desktop virtualization

Another approach to separation of personal and work data and resources is to minimize the company footprint on the end-user client as much as possible by employing local desktop virtualization. Local desktop virtualization allows a company to deploy a managed desktop environment to nearly any compatible device independent of the network on which that device operates and is different from VDI, which uses servers to provision desktop environments. VDI requires a greater financial commitment, a robust IT infrastructure, and places higher demands on sysadmin staff than local desktop virtualization (Olavsrud, 2014). This paper will demonstrate implementation of local desktop virtualization by installing hypervisor software and a customized, encrypted, and restricted virtual machine (VM) on the employee's hardware.

2.2.1. Custom desktop images

Corporate IT departments often build and maintain custom desktop images. This is particularly true if the company is large, utilizes multiple hardware configurations, or operates within specific security environments (Tulloch, 2010).

As discussed earlier in this paper, a company *could* deploy a desktop identical to what the employee sees at the office, but there are reasons not to do so. According to Microsoft field engineer Jeff Stokes, "In building an image, careful consideration needs to be made on how the image will ultimately be deployed" (Tulloch, 2010). Since this paper scopes the problem as remote access during travel or "tying up loose ends" from

home rather than telecommuting or Bring Your Own Device (BYOD), it will be assumed that users do not require every driver and application available to them at the office. For this paper, E-mail, a web browser, office productivity software (word processor, spreadsheet program, slide show builder, database, etc.), one or two applications specific to the company or business unit, and the requisite drivers will make up the VM desktop. Deploying a custom image could improve corporate security by restricting access to certain data, especially if that data requires software not available on the image used for remote access. This can be useful in mitigating the insider threat; for example, an employee who maliciously accesses whatever confidential data they can get their hands on with the intent of selling it for profit or publishing it to cause embarrassment or financial harm to the company. This is done by employees disgruntled by current working conditions or pending layoffs, and by those intent on "career building with company data," stealing intellectual property in advance of leaving the company (Symantec Corporation, 2009).

2.2.2. Hypervisor software

In order to install a guest OS as a VM on a computer without changing the host OS, a specific type of virtualization hypervisor known as a "hosted hypervisor" must be installed. A hosted hypervisor depends on a host OS to access the computer's hardware, as opposed to a "bare metal hypervisor," which essentially acts as an OS in and of itself (Siebert, 2011).

Hosted virtualization hypervisors are more appropriate for personal desktop virtualization, and several of the most popular hosted hypervisors are produced by VMware, which is available in several versions: Fusion, designed to allow Windows applications to run on Mac computers; Fusion Pro, a much more robust version of Fusion; Player Pro, which allows hosting of VMs on Windows or Linux machines; and Workstation, a more robust hypervisor for Windows or Linux with many additional features, such as the ability to create secure VMs to run under Player Pro (VMware, 2015). All of these VMware products offer many features and have minimum hardware and OS requirements; some employees running older systems at home would not be able to run the required hypervisor, but this should not be common. Installing the hypervisor

and loading the VM image should be within the abilities of most employees, but there may be some who are incapable or unwilling, especially since they will now need to learn how to use the hypervisor software.

The hypervisor cost is not tremendous, certainly when compared to an enterprise-wide solution such as VDI, but at the higher end it approaches the cost of issuing a laptop. VMware hypervisors range in price per license from approximately $70 (for Fusion Pro 7) to $150 (for Player Pro 7) to $250 (for Workstation 11) for the initial purchase; upgrading earlier versions is less expensive (VMware, 2015). By contrast, Oracle's VM VirtualBox Enterprise costs $50 per named user, but the minimum purchase is 100 licenses for a total cost of $5000 (Oracle, Inc., 2015). The implementation proposed in this paper requires one copy of Workstation 11 for the IT specialist and one copy of Fusion Pro 7 or Player Pro 7 (as applicable) for each remote desktop user. If need be, the Workstation machine can also be used for remote access.

2.2.3. Advantages of this approach

By using virtualization, the corporate network will be isolated from the remote network. Hosting each VM locally will save the company at least $1400 over using a client-server approach such as Horizon FLEX for each 10 licenses (VMware, 2015). Encrypting and setting expiration dates for each VM will mitigate risks introduced by loss or high employee turnover, and restricting the VMs will prevent unauthorized changes to the desktop. Customizing each VM and desktop will enhance security and reduce data loss by preventing users from printing or saving files on the local host or network. Finally, this solution is fairly easy to implement, and will not require maintenance of a VDI server.

2.3. Implementation

The custom desktop deployed in this paper was built from Ubuntu Desktop 14.0.4 LTS (Long Term Support) and created as a virtual machine using VMware Workstation 11. Ubuntu is an open-source distro of Linux, and was chosen to interact with an Ubuntu Server 14.0.4, also hosted on VMware Workstation 11. While Linux is not widely known outside of the IT community, it bears consideration by organizations needing to provide a remote desktop. The main benefit is cost – most Linux distros are open source;

providing a commercial OS such as Windows (loaded with other commercial applications) requires a license for each instance of the software, whether used as a virtual machine or on a host system, potentially exceeding the initial cost of simply providing a company-owned laptop.

2.3.1. Building a virtual machine template with a customized desktop

To begin, download the appropriate image (.iso) file from www.ubuntu.org, either 32-bit or 64-bit, depending on the employee's hardware and host operating system. To create the virtual machine, open Workstation and select "Create a New Virtual Machine" (Screenshot 1). The New Virtual Machine Wizard will open and step through the process, which is very user-friendly. To begin, select "Typical" or "Custom" configuration (Screenshot 2:); "Custom" allows more flexibility with regards to hardware selection, but "Typical" should be sufficient for most cases. Next, Workstation prompts the user to select the appropriate .iso image to serve as the OS for the virtual machine (Screenshot 3:). The next step is to specify the size and configuration of the virtual hard disk drive (Screenshot 4:). The final step is to confirm the virtual hardware configuration. Here the user is provided the opportunity to make other customization choices, such as removing the printer or configuring the USB controller so as to prevent Bluetooth devices from being shared with the VM, thereby reducing the attack surface (Screenshot 5:). Another key configuration choice is the virtual network adapter. The adapter can be either "Bridged," which connects the VM directly to the host's network, "NAT" (short for Network Address Translation), in which the VM shares the host's IP address, or "Host-only," which will only allow connections to other VMs on the same network. For remotely connecting to the company server, either NAT or Bridged will work (Screenshot 6:).

After the configuration is set, Workstation creates the VM, essentially installing the guest OS as if it were doing so on the host computer. Ubuntu installation begins with creating the first user, the user with admin rights who will configure the desktop for distribution (Screenshot 7:).

Following installation, the VM boots into Workstation, and from there, the admin user can then update the Ubuntu OS with **sudo apt-get-update** (Screenshot 8:) and **sudo**

apt-get-install. This is essential, since any Linux distro is likely to have had updates released since the image file was published for download. After the initial update, the admin should begin removing unnecessary or unwanted software such as Bluetooth Transfer (Screenshot 9:). While Ubuntu Desktop was chosen for this paper, it is not the lightest Linux distro available, and it contains many programs that are not necessary for most users. Manually removing software is very time consuming and tedious. Organizations desiring to use Linux for their remote machines should explore the various distros to find the one best suited for their needs.

2.3.2. Creating deployable VMs from the template

Once the desktop is configured as needed, the admin has a template for distributing the VM to employees. This process should be repeated as necessary if different desktop configurations are needed for different groups of employees, e.g., one for the salespeople, another for mobile technicians, etc. Workstation allows users to clone VMs (Screenshot 10:) using a Wizard much like the one to create new VMs. There are two types of clones: "linked clones," which are referenced to the original ("parent") VM (and therefore the physical hard drive used by that VM), and "full clones," which are complete copies of the parent VM (Screenshot 11:). Linked clones are smaller, but full clones can be used regardless of the status of the parent VM; therefore, full clones are required.

The admin should then create a clone for each employee. These clones will only have the admin's account; after each clone is finished, the admin must then create the user account for the employee, allowing the employee to set their passwords and create public and private key pairs for such things as encrypted and digitally signed E-mail, or secure shell (SSH), a protocol commonly used for secure data transfer (Screenshot 12:). Another critical step is to change the hostname of each cloned VM. This must be done to avoid hostname resolution errors when SSH is used. The hostname can be changed by editing **/etc/hosts** and **/etc/hostname** files (Screenshot 13:).

2.3.3. Snapshots

One of the biggest security advantages to using VMs is the ability to use snapshots. As the name implies, a snapshot freezes the state of the VM at a given time.

By taking a snapshot of the clean desktop and setting the VM to always revert to that clean state every time it boots (Screenshot 14:), the potential for persistent threat is eliminated.

Snapshots are also very useful during the desktop customization process. If an admin makes a change to the VM that leaves the machine unstable or removes a functionality required by the user, VMware allows the admin or user to revert back to a previous snapshot. This raises two points: First, snapshots should be taken frequently to reduce the amount of work that will have to be redone if you need to revert to a previous snapshot. Second, it is very important to delete all but the most recent snapshot prior to cloning or distributing a VM, since having multiple snapshots greatly increases file size.

2.3.4. Encrypting and restricting the VM

Before saving the VM to removable media and issuing it to the employee, the VM should be encrypted to prevent unauthorized use. To encrypt the VM, the employee enters a password into Workstation (Screenshot 15:); the employee will need to enter this password prior to opening the VM in Player Pro, and there is no means for recovering this password if lost (VMware, 2014). Once the VM is encrypted, the admin can then enter a password to put restrictions on the VM, such as preventing the user from changing the configuration of the VM or connecting USB drives. VMs can also be restricted by giving them an expiration date (Screenshot 16:); this is useful for companies with high employee turnover or in the event the host machine is lost or stolen, and therefore is highly recommended. Restricting a VM also prevents the user from removing encryption.

2.3.5. Distribution and use

Once the VM has been encrypted by the employee and restricted by the admin, the VM files can be copied to removable media and issued to the employee, along with a copy of VMware Player Pro and the Player Pro product key. The employee then installs and activates VMware Player Pro, then copies the VM files to their host computer. Player Pro is simple and user-friendly; the employee can open the VM after entering the encryption password, and begin using their carefully configured, locked-down desktop to remotely connect to company servers.

2.3.6. Operational validation

Security is critical, but the purpose of distributing the VMs in the first place is to enable employees to do their jobs while away from the office. For each variation of the custom desktop, the company should have an employee from the appropriate business unit attempt to conduct all "mission essential tasks" required during remote access. This will help identify omission of critical software or services before distribution, rather than discovering the error just minutes prior to giving a key sales presentation on the road.

2.3.7. Audit

Distributing the VMs is not enough to ensure the corporate network is now secure. Auditing should be performed on the VMs as well as the VPN server. Auditing the distributed VM would be the responsibility of the second IT specialist mentioned earlier. Even if the company does not choose to have a dedicated information security specialist, it is essential to have an objective party evaluate the VM for vulnerabilities or flaws in the design of the custom desktop. The security validation should be done in two phases. First, conduct an audit of the VM. The auditor should load the VM on a laptop or desktop and then attempt to execute operations intended to be prohibited by the desktop design. For the example VM built for this paper, such operations would consist of attempting to load unauthorized software or mapping to a local USB drive or printer. Next, the auditor should conduct a penetration test of the VM to validate the security of the desktop from threats originating from the remote network. Using the security control of *separation of duties* to have a second IT specialist conduct the audit and pen test decreases the risk of insider threat caused by errors in desktop design, whether inadvertent or intentional.

After distributing the VMs, the company should take steps to verify that employees are actually using their VMs to gain remote access. First, application whitelisting software should be used to limit access to programs loaded on the distributed VMs. For the Ubuntu server used in this paper, Novell AppArmor is installed by default (Ubuntu Documentation Team, 2014).

Second, VPN server firewall access control lists should be configured for Media Access Control (MAC) address filtering, restricting access to the MACs of each VM.

While MAC addresses can be spoofed with tools such as Ettercap (Ettercap Project, 2015), the intent behind MAC filtering is not so much to foil hackers as it is to validate appropriate remote access by employees.

Finally, VPN server logs should be kept and reviewed regularly in order to provide additional confirmation of authorized access. Also, reviewing logs will help establish a baseline of "normal" remote access activity. With regards to the solution proposed by this paper, baselining is not only useful to help detect attacks, it can be useful in evaluating the feasibility of requiring VMs to access the corporate network. If a log review shows few connections, it may be because too many employees are uncomfortable using the VMs, or if the VMs aren't functioning properly on certain machines.

2.4. Shortfalls of this approach and lessons learned

There is no "silver bullet" solution to the problem of accessing company resources from compromised hosts and networks. This paper has offered a solution weighed against factors such as cost, ease of use, and ease of administration. The following paragraphs discuss some of the threats left unmitigated by local desktop virtualization as well as some potential problems created by the solution itself.

2.4.1. Data transmission vulnerabilities

Abstracting the logical layer from the physical hardware does nothing in and of itself to protect the data in motion between the corporate and remote hosts. Data sent clear text can still be read if captured by Wireshark or another packet capture program. Therefore, encrypting the data in transit is essential. Even so, various protocols used for secure connectivity have themselves been compromised, such as was the case with the "Heartbleed" vulnerability in certain implementations of OpenSSL (US-CERT, 2014).

2.4.2. Compatibility issues

The implementation used in this paper does not support Android, Apple iOS, or Chrome OS (VMware, 2015); employees cannot remotely access company servers from smartphones or tablets using these operating systems. This is noteworthy now and could

become significant if tablet computers grow in market share, or if BYOD becomes more prevalent.

2.4.3. Employee frustration caused by change

To reduce implementation costs, the solution proposed in this paper used Ubuntu Linux. Like many Linux distros, Ubuntu uses a fairly intuitive Graphical User Interface not unlike Windows or Mac OS X, but nevertheless, Linux is a different system and will likely be unfamiliar to most employees, especially those who are not technically inclined. Moreover, Linux does not use the same application software as Windows or Mac, adding an additional source of stress and frustration for some. For that matter, the proposed solution assumes a certain degree of familiarity and proficiency with Ubuntu on the part of the company IT team, which might not be the case. If the IT team struggles, this implementation is likely to fail.

2.4.4. Configuration Control

Since the company is issuing multiple VMs with different configurations, diligent configuration control is necessary. Failure to do so may result in VMs not receiving critical patches, thereby introducing vulnerability to corporate data rather than protection. Configuration control can be administratively intensive if the VMs are sufficiently different, and for a small company such as the one in this paper, this may pose an undue burden on the IT team.

3. Conclusion

Access to corporate IT resources from remote locations exposes corporate data to risk from malware or other vulnerabilities present on the remote network. To mitigate this, we must isolate the remote host from its network. Tunneling connections such as VPNs provide some protection from eavesdropping and packet capture, but do nothing to prevent malware from transiting the VPN to infect the corporate servers.

To better protect the corporate network, we need an additional layer of isolation, which we provide through local desktop virtualization. This is a better choice for smaller companies with limited budgets and less robust IT support, since it has a lower TCO than company-issued devices, and a significantly lower price than enterprise-wide VDI,

especially if the company uses an open-source OS such as Ubuntu for the remote desktop. The company can further enhance security by customizing the remote desktop to remove unnecessary hardware and software, which reduces the number of potential vulnerabilities and makes data theft from an insider threat more difficult.

There are some potential shortfalls, however. Virtualization does not inherently protect data in transit, employee hardware may be incompatible with the chosen hypervisor, and the employees themselves might be resistant to learning new software. That being said, this solution should be well within the reach of most companies, and provides concrete security benefits at a reasonable cost.

Christopher Jarko, csjarko@yahoo.com

References

Alcatel-Lucent Motive Security Labs. (2015). *Motive Security Labs Malware Report - H2 2014.* Boulogne-Billancourt: Alcatel-Lucent.

Chappell, L. (2013). *Wireshark 101: Essential Skills for Network Analysis.* San Jose: Protocol Analysis Institute.

Citrix Systems, Inc. (2014). *Remote Access to Desktop PCs - XenDesktop 7.5 Design Guide.* Retrieved from Citrix Systems, Inc. Web site: http://www.citrix.com/products/xendesktop/go/tech-info.html

Citrix Systems, Inc. (2015, July 18). *Store*. Retrieved from Citrix Systems, Inc. Web site: http://store.citrix.com/store/citrix/en_US/buy/productID.315219300/ThemeID.37713000

Ettercap Project. (2015). *Manual Reference Pages - ETTERCAP (8).* Retrieved from IronGeek.com: http://www.irongeek.com/i.php?page=backtrack-3-man/ettercap

Gartner, Inc. (2014). *Gartner IT Glossary - Total Cost of Ownership (TCO)*. Retrieved April 18, 2015, from Gartner.com: http://www.gartner.com/it-glossary/total-cost-of-ownership-tco/

Golden, B. (2007). *Basics of Network Virtualization - For Dummies*. Retrieved from Dummies.com: http://www.dummies.com/how-to/content/basics-of-network-virtualization.html

Howe, A., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (20-23 May 2012). "The Psychology of Security for the Home Computer User". *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 209, 223). San Francisco: Institute of electrical and Electronic Engineers (IEEE).

IBM Systems and Technology Group. (2007). *Virtualization in Education.* Research Triangle Park: IBM Corporation.

Ilascu, I. (2014, Oct 20). *Keylogger in Phishing Email Also Takes Screenshots*. Retrieved from Softpedia News:

Christopher Jarko, csjarko@yahoo.com

http://news.softpedia.com/news/Keylogger-In-Phishing-Email-Also-Takes-Screenshots-462607.shtml

Kaspersky, E. (2013, March 25). *One in Twenty is the Sad Truth.* Retrieved from Eugene Kaspersky's official blog: https://eugene.kaspersky.com/2013/03/25/one-in-twenty-is-the-sad-truth/

Krebs, B. (2014, July 14). *Beware Keyloggers at Hotel Business Centers*. Retrieved from Krebs on Security: http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/

Lauzière, T. (2013). *User Manual.* Retrieved from Linux Live USB Creator Web site: http://www.linuxliveusb.com/en/help/guide

Microsoft. (2013, January 17). *Hyper-V Getting Started Guide*. Retrieved from Microsoft TechNet: https://technet.microsoft.com/en-us/library/cc732470%28d=printer,v=ws.10%29.aspx

Microsoft. (2014, August 19). *Install Hyper-V and Create a Virtual Machine*. Retrieved from Microsoft TechNet: https://technet.microsoft.com/en-us/library/hh846766%28d=printer%29.aspx

Notenboom, L. (2012). *What's a "live" CD? And why would I want one?* Retrieved from Ask Leo: http://ask-leo.com/whats_a_live_cd_and_why_would_i_want_one.html

Olavsrud, T. (2014, October 2). *Local virtual desktops may be the (old) new thing in BYOD*. Retrieved April 20, 2015, from www.cio.com: http://www.cio.com/article/2689606/byod/local-virtual-desktops-may-be-the-old-new-thing-in-byod.html

Oracle, Inc. (2015, July 18). *Store*. Retrieved from Oracle corporate Web site: https://shop.oracle.com/pls/ostore/product?p1=OracleVMVirtualBoxEnterprise&p2=&p3=&p4=&p5=&intcmp=ocom_virtualization_vmvirtualboxenterprise

Portnoy, M. (2012). *Virtualization Essentials.* Indianapolis: John Wiley & Sons, Inc.

Privacy Enforcement and Protection Unit, California Department of Justice. (2014). *California Data Breach Report.* Sacramento: California Department of Justice.

Christopher Jarko, csjarko@yahoo.com

Siebert, E. (2011, August). *Understanding hosted and bare-metal virtualization hypervisor types*. Retrieved April 19, 2015, from TechTarget: http://searchservervirtualization.techtarget.com/tip/Understanding-hosted-and-bare-metal-virtualization-hypervisor-types

Symantec Corporation. (2009). *Anatomy of a Data Breach - Why Breaches Happen and What to Do About It.* Mountain View: Symantec Corporation.

Tulloch, M. (2010, June). *Desktop Image Management: Build a Better Desktop Image*. Retrieved April 19, 2015, from TechNet Magazine: https://technet.microsoft.com/en-us/magazine/ff721826.aspx

Ubuntu Documentation Team, e. a. (2014). *Ubuntu Server Guide.* wiki.ubuntu.com.

University of California, Davis. (2015, October 13). *Privacy Rights Clearinghouse.* Retrieved from Data breach search results: http://www.privacyrights.org/data-breach-asc/268/262%2B259%2B257%2B258/1153%2B1473%2B2122?title=Davis&=Apply

US-CERT. (2014, April 8). *OpenSSL "Heartbleed" Vulnerability*. Retrieved from US-CERT Alerts and Tips: https://www.us-cert.gov/ncas/current-activity/2014/04/08/OpenSSL-Heartbleed-Vulnerability

VMware. (2014). *Using VMware Workstation 11.* Palo Alto: VMware, Inc.

VMware. (2014). VMware Horizon FLEX Datasheet. Palo Alto, CA.

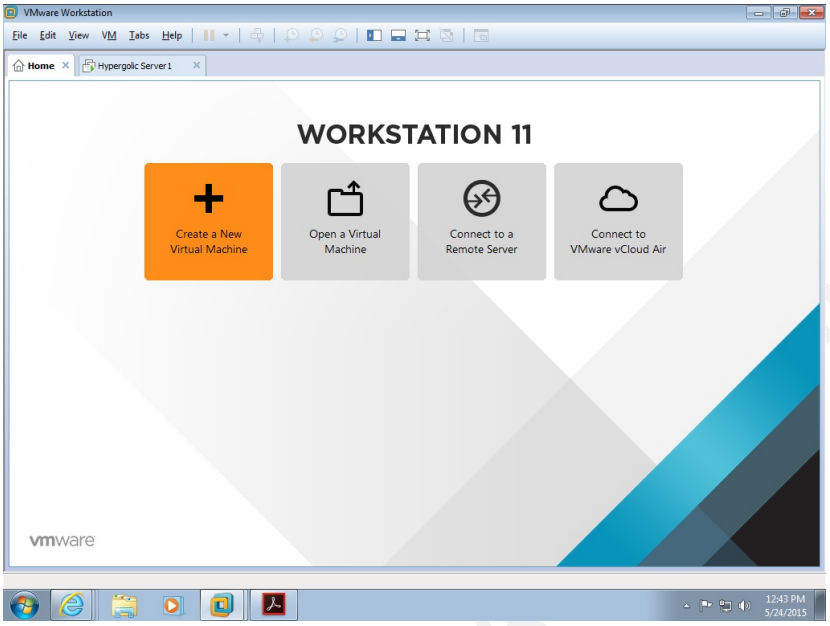
VMware. (2015). *Store*. Retrieved April 20, 2015, from www.vmware.com: http://store.vmware.com/store/vmware/en_US/home

Christopher Jarko, csjarko@yahoo.com

Appendix

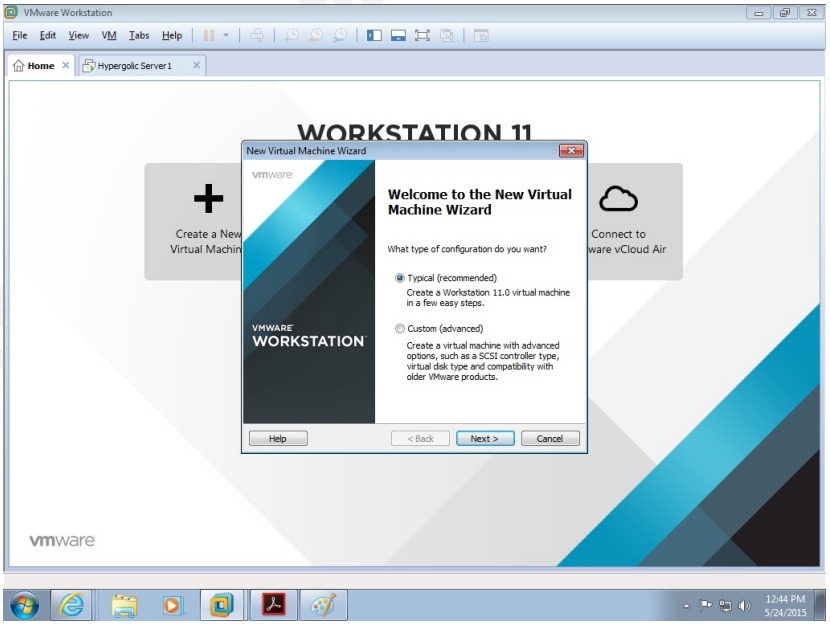
Screenshots

Screenshot 1:



Creating a new virtual machine

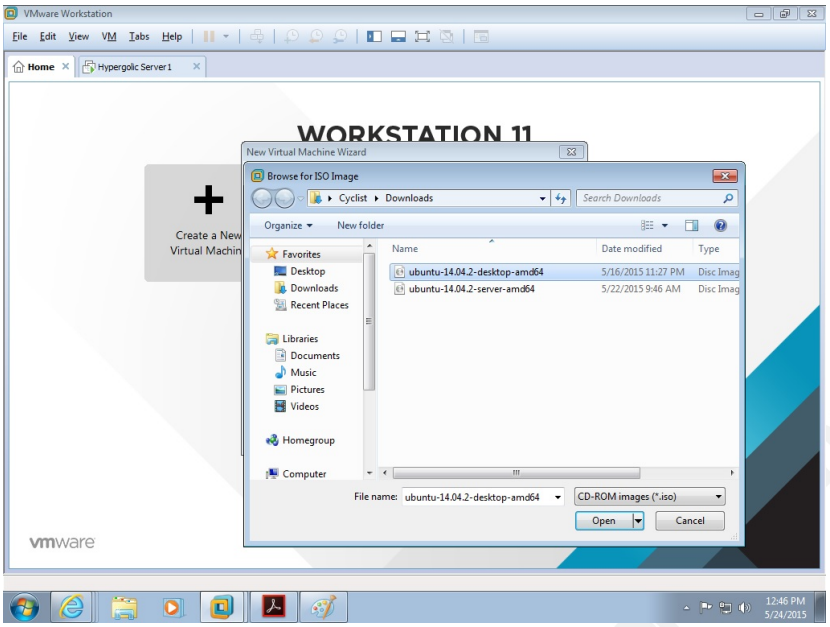
Screenshot 2:



Selecting the configuration type

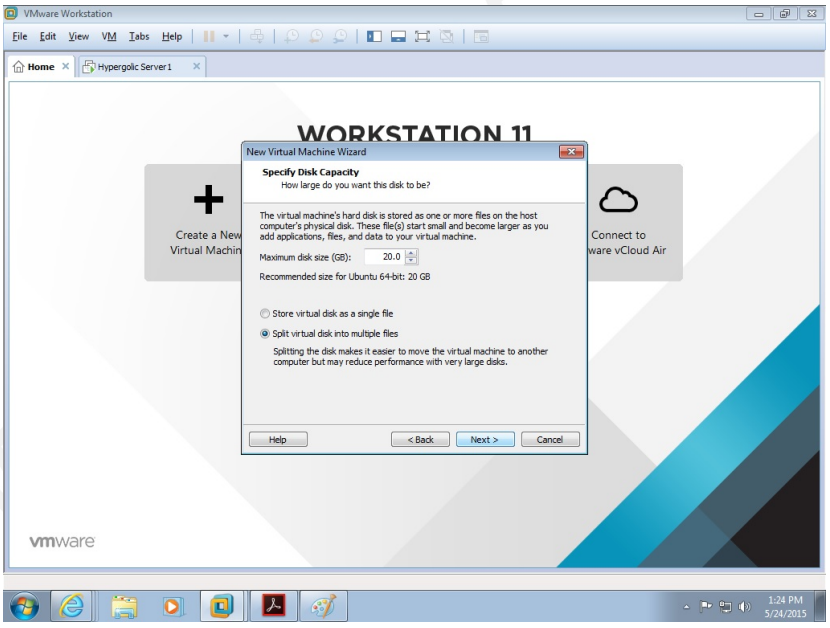
Christopher Jarko, csjarko@yahoo.com

Screenshot 3:



Selecting the .iso file

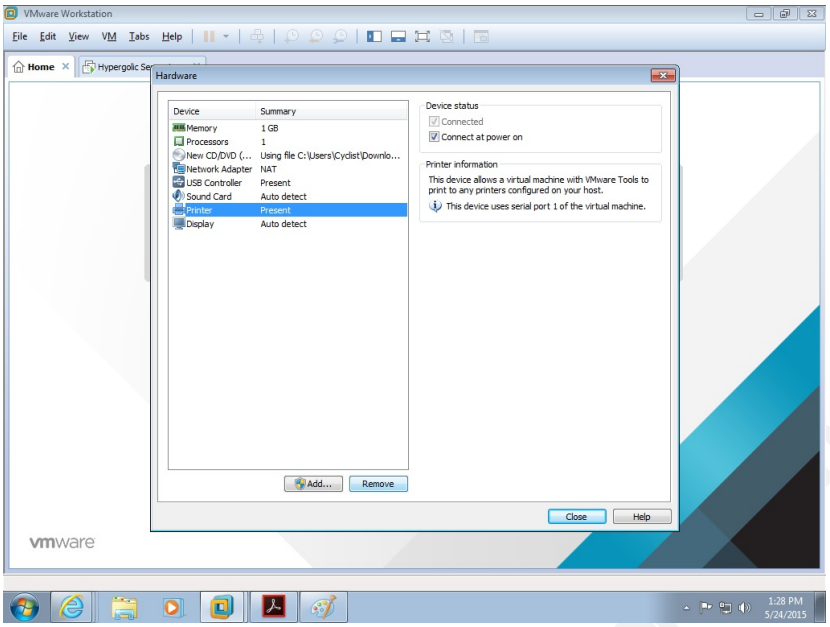
Screenshot 4:



Configuring the virtual hard drive

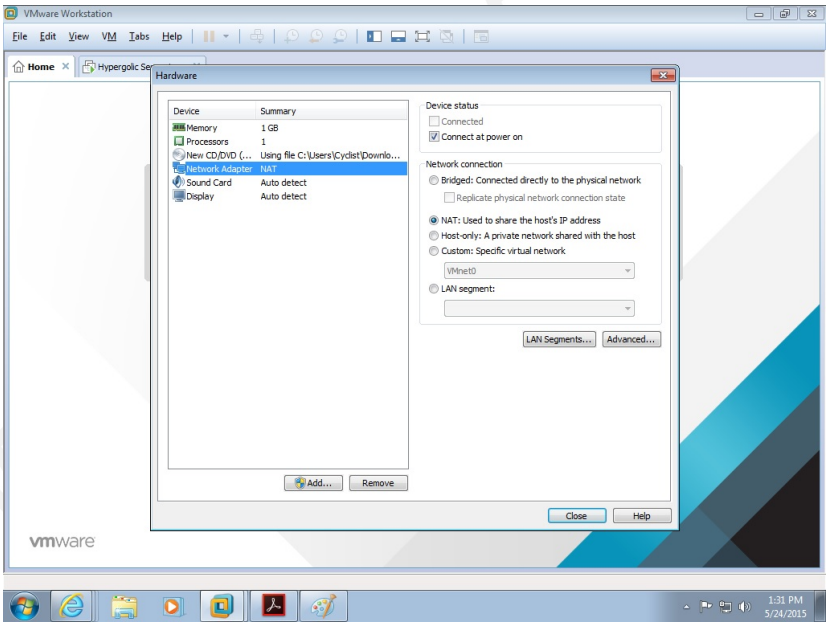
Christopher Jarko, csjarko@yahoo.com

Screenshot 5:



Removing unwanted or unnecessary hardware

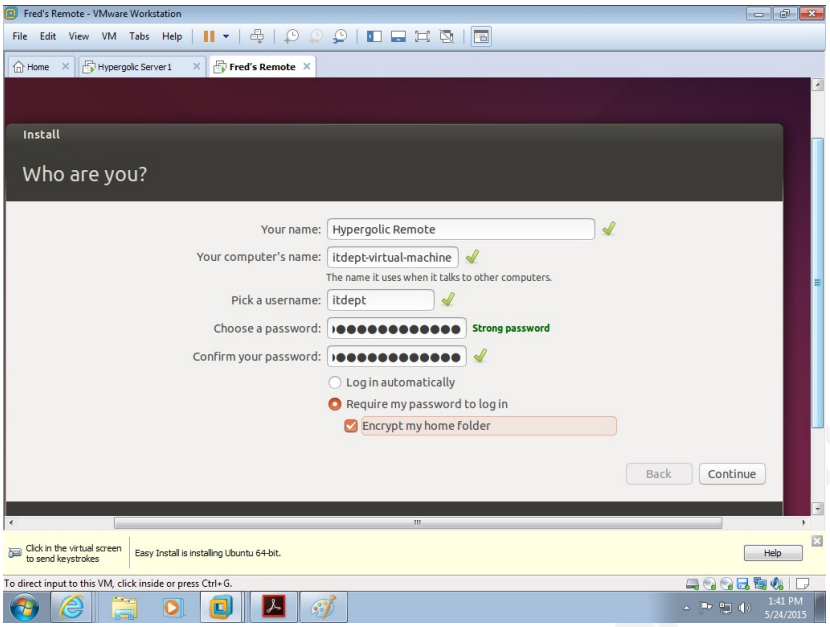
Screenshot 6:



Selecting the network adapter

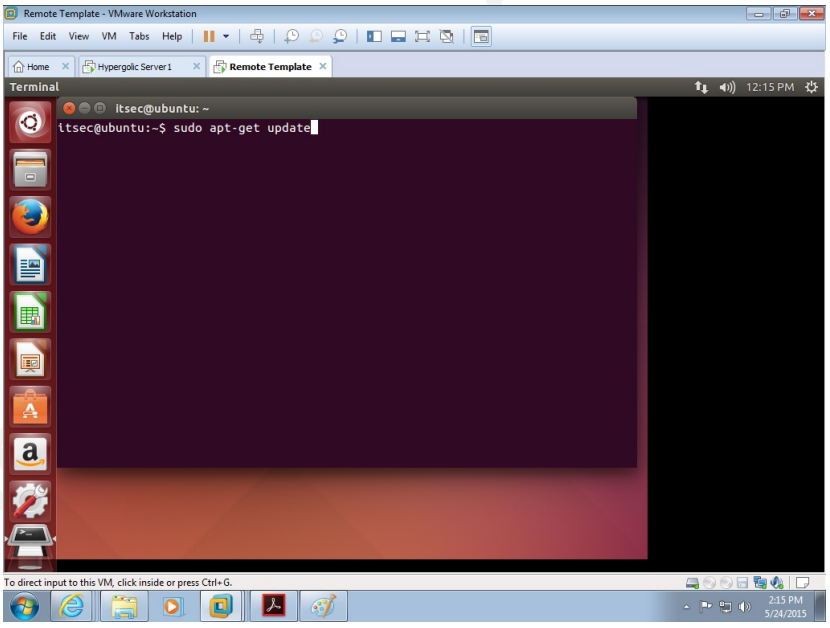
Christopher Jarko, csjarko@yahoo.com

Screenshot 7:



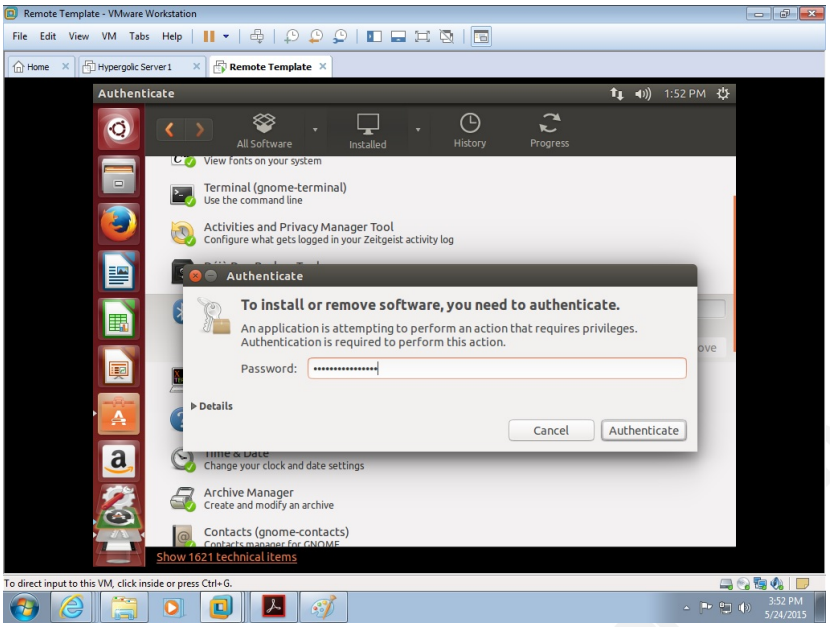
Creating the first user account

Screenshot 8:



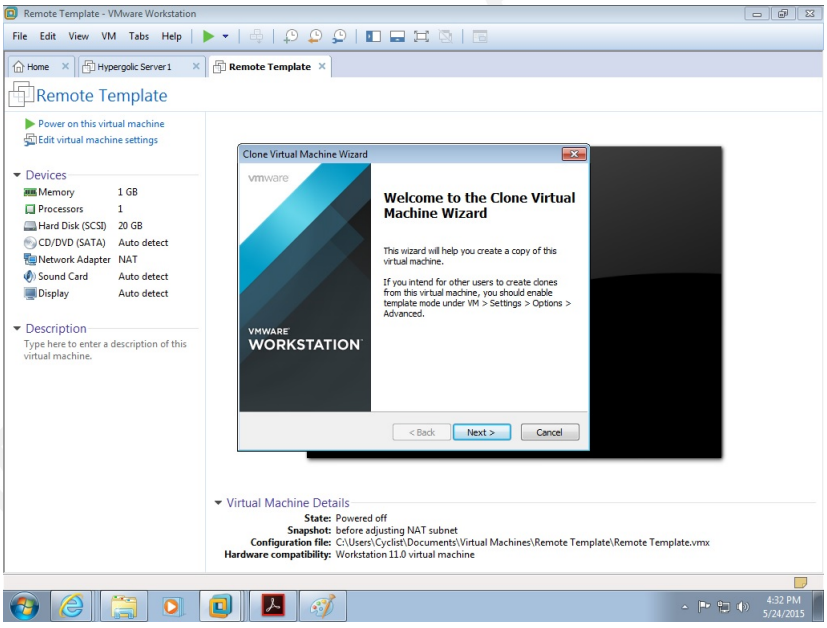
Performing the initial update with **sudo apt-get update**

Screenshot 9:



Removing unwanted software from the VM

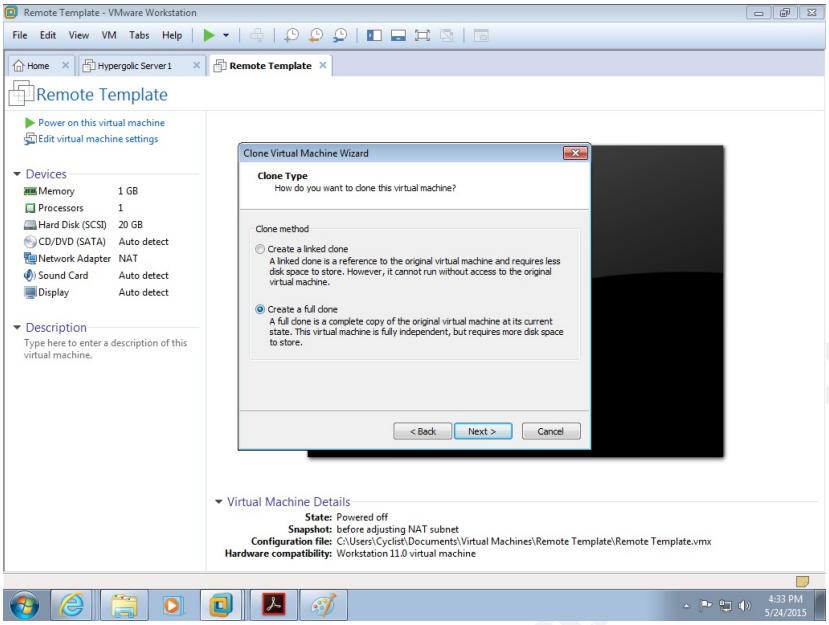
Screenshot 10:



The Clone Virtual Machine Wizard

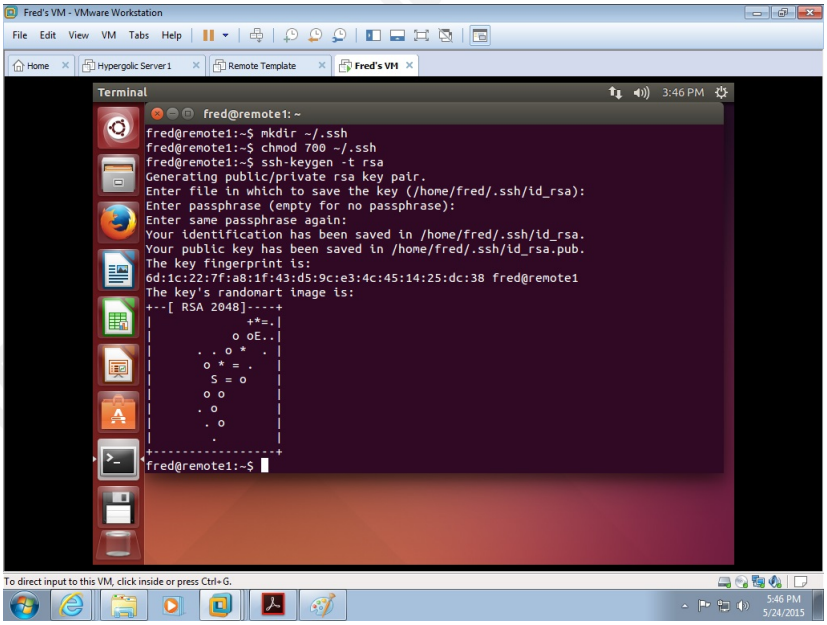
Christopher Jarko, csjarko@yahoo.com

Screenshot 11:



Select "Create a full clone"

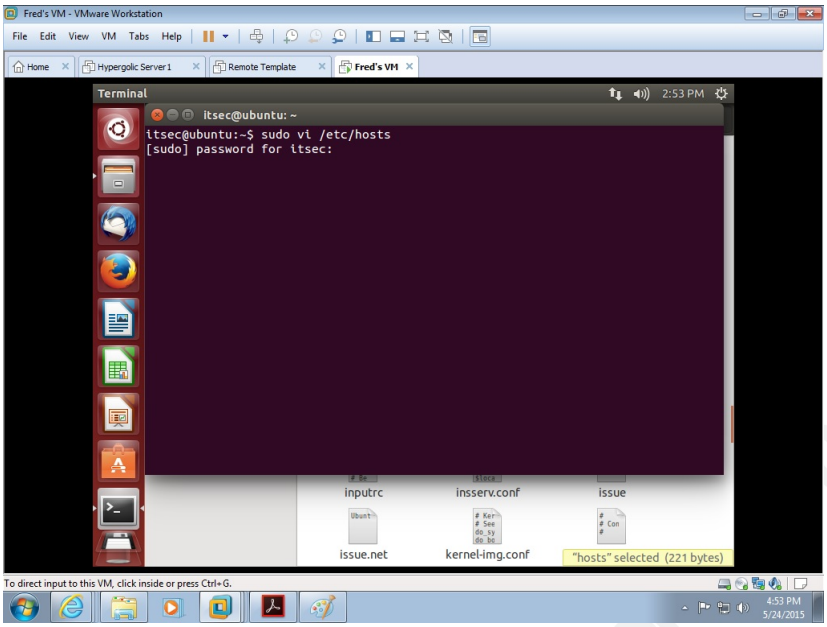
Screenshot 12:



Generating RSA keys for Secure Shell (SSH)

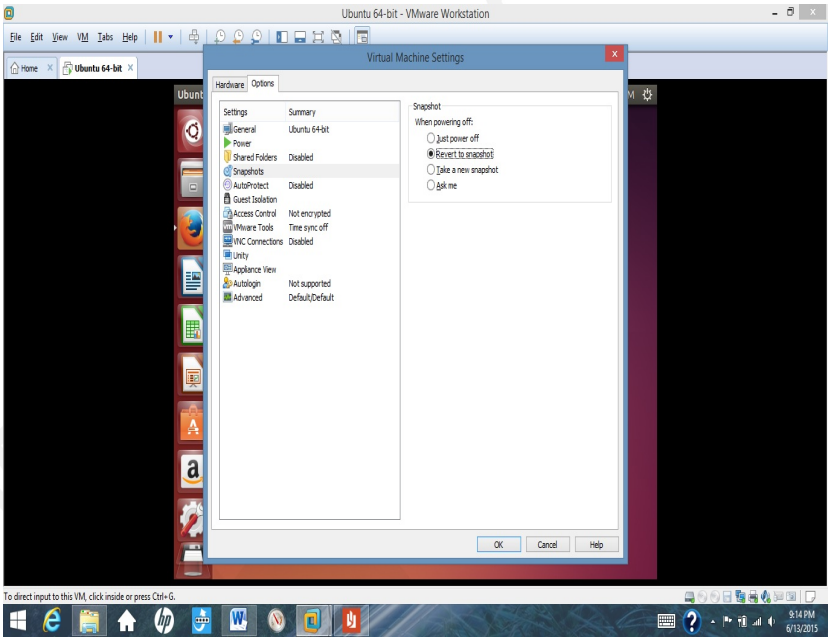
Christopher Jarko, csjarko@yahoo.com

Screenshot 13:



Editing the hostname using **sudo vi /etc/hosts**

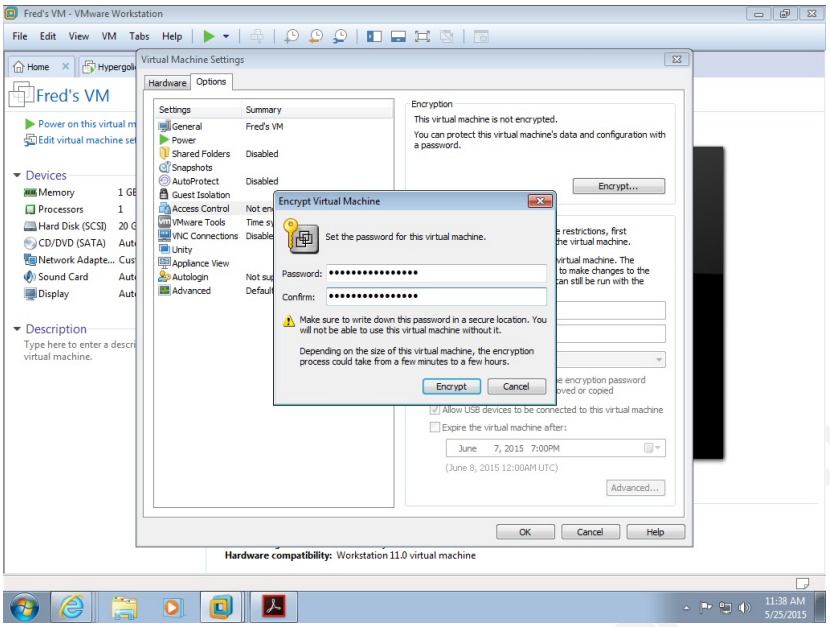
Screenshot 14:



Configuring the VM to always revert to the clean snapshot

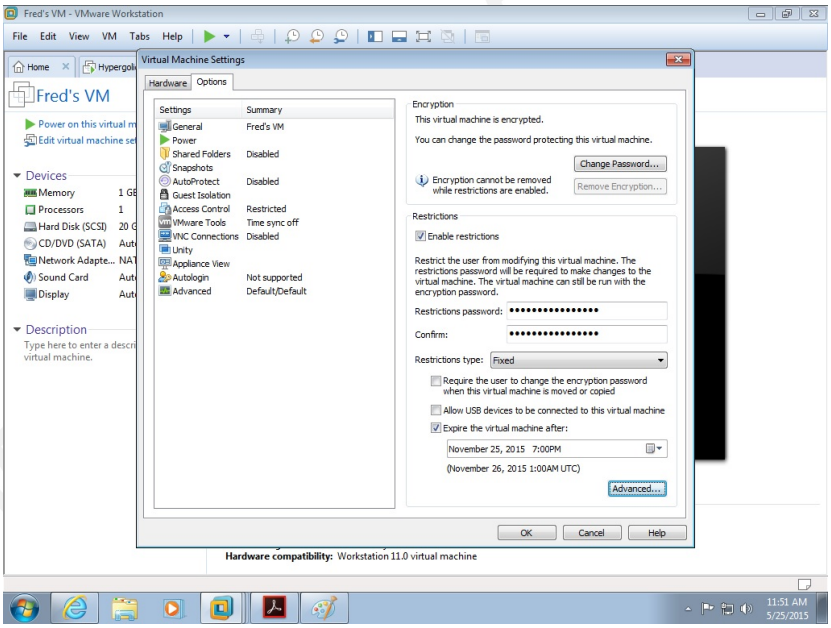
Christopher Jarko, csjarko@yahoo.com

Screenshot 15:



Encrypting the VM

Screenshot 16:



Restricting the VM with an expiration date

Christopher Jarko, csjarko@yahoo.com