Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Virtual Rapid Response Systems

This paper is ideal for companies that have multiple business locations but no IT support onsite; who have no budget for additional security and lack a comprehensive incident response plan. Using virtual machines deployed to problem sites as the safe workstation, one/a member of the IT security team can start to amass the pertinent information to understand the true nature of the incident and properly record it.

Copyright SANS Institute

Author Retains Full Rights

AD

Virtual Rapid Response Systems

GIAC (GCIH) Gold Certification

Author: Chris Mohan, Chris@ChrisMohan.com

Advisor: Don C. Weber

Accepted: July 7, 2008

Abstract

This paper aims to provide organizations with a quick and effective response to IT security breaches at remote locations with a virtual response platform. In a nutshell, it provides a preconfigured, standard and safe remote platform for an individual tasked with responding to a security incident. It is targeted at companies using the Windows desktop and server operating systems as their main platforms. This paper is ideal for companies that have multiple business locations but no IT support onsite; who have no budget for additional security and lack a comprehensive incident response plan. Using virtual machines deployed to problem sites as the safe workstation, one/a member of the IT security team can start to amass the pertinent information to understand the true nature of the incident and properly record it.

It is important to understand that this may not necessarily resolve the current issue. However, it will provide a much clearer picture of what has happened and should serve to prevent a reoccurrence as insight has been gained. This translates into future monetary savings for the business by avoiding potential lost productivity.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

A call comes through to the help desk. A staff member is having problems with their computer at one of your remote sites. "It's acting weird and is really slow". The call gets forwarded to the second line support group, who remotely connect to the affected machine. After some searching, they find a new tool bar on Internet Explorer, plus random pop ups advertizing online gambling sites and then notice the anti-virus service has stopped. After restarting the anti-virus and deleting the new tool bar, it's put down to a user going to unauthorized web sites during a lunch break. Half an hour goes by and two identical calls come in, all from the same location. Eventually, twenty calls have come in from the same office and even the manager has logged a call complaining that her machine is "acting weird and is really slow". It is clearly more serious than an anti-virus software issue. The calls get forwarded to you.

Dealing with a remote office where there is no IT support staff, the member of the security team has to start with the limited information contained in the call logs. With the problem growing and the threat of other sites becoming infected, a decision is typically reached to lock down the network traffic to and from the site to contain the problem.

Often, a member of IT is dispatched to fix the problem a day later, as nobody on site has been able to fix the issue under guidance. The IT support member finds a virus which has opened ports, changed system files and spawned new executables. It takes three hours to clean the first two computers. The site manager demands quicker results as twenty staff are still offline. A complete rebuild of all the infected systems only takes a few hours, so a decision is taken to do that. Valuable time as well as business is often lost in this situation.

Understandably, senior management want to know what happened, how it happened and how to stop it happening again. Are you able to provide a comprehensive analysis of the issue including relevant details from the deleted machines immediately?

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Without a road map and plan for response, simple mistakes can occur in the heat of the moment. This compounds the problem, while increasing the time, energy and cost to remedy, slowing the return to a normal operational situation.

The best solution is to use a preconfigured and tested virtual machine. Quickly deployed to the remote site it offers the capability to derive relevant information on the situation in a consistent manner. A single Remote Desktop Protocol (RDP) connection to the virtual machine onsite provides access to all the other local systems. This minimizes the wide area network (WAN) traffic overhead, and affords excellent accountability. Moreover, it provides a clear picture of what is happening on the WAN at the site and affected systems. Finally, it has the advantage of keeping records of the event stored securely, consistently, and accurately in an automated fashion.

2. The Incidence Response Charter

The six steps from the incident response model break down to: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned (Skoudis 2005). The virtual response platform is focused towards the containment and eradication stages with strong roots in the preparation and identification stages. Getting in a position to be able to respond quickly and effectively requires planning, testing and an agreed game plan.

As part of the preparation phase, brainstorm using a small, informal group to generate scenarios applicable to your unique environment. This provides the opportunity to develop an effective response plan. An important piece of any brainstorming and creative ideas mapping is to record them, clearly and concisely. They can then be objectively reviewed and implemented when necessary. These preparation documents highlight excellent locations to install the response platforms.

3. Building The Infrastructure

The virtual family: VMware and Microsoft. What makes sense in your environment? In the Windows environment VMware and MS Virtual software are easy choices. The free offerings are

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

VMware's player and server, and Microsoft's Virtual PC and server. They both have excellent features and are easy to use and install.

In this paper, we will focus on Virtual PC as the virtual response platform base. This is because in a Microsoft environment it is much simpler to get Microsoft software approved for installation to servers and PCs - it's an officially supported scenario by Microsoft (Microsoft 2009) to have Virtual PC running on top of Windows systems. One of the biggest requirements for our incident response model is that no reboot should be required after installing it. An important note is that a Microsoft XP license is needed for each of these virtual machines.

There are conversion tools that allow you to convert VMware virtual images to Microsoft virtual images. This is an advantage if you are already using a particular product, such as VMware workstation, for building testing labs. A free tool for this conversion can be downloaded (Davidb 2006).

4. Building The Response Platform

Creating the response platform is a two phase set up. Phase one is to prepare a storage area to securely hold all data recovered from examined systems. Phase two is the actual build of the response platform.

First, build a storage location to upload copied files, data and logs. This has to be secured and under complete control against access by non-authorized staff. Never, ever, use a public location on a file server. The simple option is to create a hidden file share, in Windows, then apply very restrictive and focused Windows NT File System (NTFS) permissions to the folder. As an example, create the share Vm$ with the Group Everyone with full access to the file share. Remove all inherited permissions and apply NTFS permission explicitly for the incident responders group. To provide an additional layer of protection, enable file level auditing and limit the access to the rest of your network from that system.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

For the data storage there are multiple options, but it has to match the risk profile you believe the files may contain; how you want to preserve the information and how hard do you want to make it for someone to mistakenly attempt to access those stored files? Here are a few suggestions.

- Build another virtual machine for this purpose, with a large second drive of 30GB+ as the target location of remote captures. This adds a greater level of segregation for potentially dangerous files as you can use features of the OS to provide auditing and access.
- Buy a large data external hard drive, connect to a low value system such as a standard workstation and share out the drive. It is easy to lock away the data once the copying has been completed.
- Copy the data to a low value system on a screen segment of your network, making it accessible only to appropriate staff.

5. What Goes Into The Virtual Machine And Why

The intention of the response platform is exclusively for IR needs. With the configuration and software optimized to only what is required, the image size can be kept reasonably small. The recommended operation system is Windows XP. The following sections cover the machine, settings to provide a responsive operating system and the software to be installed.

5.1. Hardware Configuration

The virtual components should compose of two network interface cards (NIC), two virtual drives, and 512MB of RAM. The first drive is employed for the OS at 5GB. The second drive is for temporary storage of collected files and should be over 5GB. Do not install sound cards or other peripheral devices such as USB, parallel and floppy drives as they are unnecessary.

The second NIC gives you options for sniffing network traffic. There is no performance loss if both are using the same physical NIC. A machine with two physical NICs allows for each virtual NIC to be directly assigned. One can be tasked to be used by the sniffer and the other to do the normal

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

communications. This is useful if you need to span multiple network ports on a switch, as it allows you to record network traffic from a number of network sources.

5.2. Operating System Configuration

With Windows XP as the response platform operating system, format the drive as NTFS then install a base OS including service packs, currently SP3. Ensure that the system is fully patched and always install the virtual tools to get the best performance.

Place the page file (Microsoft 2007) on the C drive and set it at 1024 MB (1GB). Turn on XP firewall and only allow Remote Desktop Protocol (RDP) through the firewall, then enable RDP. Create a second, non–privileged account as the account to respond from. Never run with an administrator level account by default, but, use the "run as" option when required.

Avoid having any desktop images, but do pick an unusual background colour for easy identification. The BGinfo tool from Sysinternals (Cogswell 2009) is helpful as it can display details of the response platform, such as name, IP address and available disk space. Optimize performance of the virtual machine by stopping XP's desktop animations and visual effects. Right click on My Computer and select Properties/Advanced/Performance Settings and then select the best performance radio button.

There are dozens of other possible windows tweaks. A search for "optimizing windows XP" will bring up a couple of hundred sites with various tips. Use anything applicable in those guides; however avoid the use of any 3rd party tools to auto-optimize. It's hard to validate what they actually do unless you want to debug them and read the code. Once you've installed everything, check nothing has been additionally installed in Add/Remove programs in the control panel.

Disable services not needed such as: Windows Audio, Wireless Zero Configuration, Print Spooler, Remote Registry, Computer Browser, Alerter, Web Client, Themes, System Restore, Automatic Updates, BITS and Help and Support.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

For additional security, a number of security templates exist to lock down Windows from Microsoft (Microsoft 2006), NIST (NIST 2008), NSA (NSA 2006) and SANS. These need to fit the company's security stance so alter them to fit those needs and policies.

5.3. Recommended Software Installation For IR

What follows is a list of additional software tools to install. All of these tools are free or shareware, providing an inexpensive solution. These allow for management of other machines, gathering of information and re-distribution of the captured data.

- Microsoft Resource Kits(Microsoft 2003) for the server types 2000/3 and the workstation OS
- Robocopy: to move data upstream - /IPG switch is remarkably handy to manage bandwidth usage
- PStools (Russinovich 2007): A large number of excellent tools. When running PSExec, the password used travels in clear text over the network, so keep that in mind if you're concerned about other people monitoring the network traffic.
- Winrar (Roshal 2009): an excellent tool for compression of files and folders; this is the only shareware tool in this list. Windows XP and above offers its own built-in compression software, but this doesn't compress to the same level as Winrar.
- Windump (Windump 2006): for capturing data on the wire.
- NMap (Lyon 2008): to scan the local subnet, finger print the types of operating systems and discover all current IP addresses and open ports at the time of the scan.
- MD5deep: for creating hashes of key executables, files and directories.
- PowerShell (Microsoft 2008): Microsoft's new scripting language is an additional download for XP and Windows 2003, but is now part of the newer Microsoft operating systems.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- Putty (Tatham 2008): for connecting to switches and routers via telnet and SSH. Easy to use and configure.
- Wireshark (Combs 2009): for quick analysis of network traffic. In GUI (graphical user interface) mode, Wireshark on a 512mb RAM workstation with a big capture file will effectively hang the machine while it sorts out the data and applies your filters. Although incredibly helpful, it's better running complex analysis on a more powerful machine with plenty of resources.

5.4. Scripting Libraries Directory

Scripts can be used to gather information quickly and efficiently. Windows has numerous options for scripting; the two notable ones are visual basic scripting (VBScript) (Wilson 2004) and PowerShell (Holmes 2007). A number of excellent forensic and information detail gathering scripts exist for windows systems.

Jason Fossen, author of the SANS windows track, has a number of scripts (Fossen 2009) which are freely available on his web site. Further, there are many sources on other web sites which cover most administrative needs. With some slight modifications this allows the user to select key files to be extracted from the target system. For example, find a script that gets the basic details of the remote computer. Then add in a section to grab the web browser cache and history files for Internet Explorer, local ARP details, the host file and certain registry keys. Once the data has been gathered, the various created files can be added to a compressed file with the name of the system as a reference. A hash of the compressed file can be generated to validate it.

It is best to test and understand these scripts (Microsoft 2009) before using them on production systems. When the scripts operate as expected, copy them to the virtual machine and clearly mark them for what they do. It is worthwhile creating a text file with explanations of each script.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

5.5. Time

Select a time source on your network (Microsoft 2007), such as a core router or primary domain controller, which all systems use. The virtual machine and the system the data is being copied to must both be using the same time source as the rest of your network. They must be synchronized perfectly with the environment in order to produce a continuous time line of the events which can be cross-referenced, accurately, and precisely. This allows for cross referencing against other logs such as firewalls, intrusion detection systems and other reporting tools. Microsoft has a number of guides on how to do this (Microsoft 2006).

6. Securing The Machine

A number of open source and commercial security tools can be used to test the integrity of response platform such as NMap and Nessus. Running scans against the virtual system may provide some further options to secure the platform. Insecure.org has a top 100 list of security tools (Lyon 2006), select whichever tool you feel most comfortable with, scan the system and make changes as you see fit.

It's worthwhile to make hashes of the critical windows files and programs on the response platform. This provides a documented record and a reference sheet should you ever need to confirm that the system itself hasn't been compromised. A useful tool is md5deep (Kornblum 2009). It is a cross-platform set of programs to compute MD5, SHA-1, SHA-256, Tiger, or Whirlpool message digests on an arbitrary number of files.

Educate other administrators on what the purpose is of these machines. Limit the access to the platform to a minimum. Domain Administrators and all the other standard Active Directory (AD) groups should NOT have access to the response platform VM. Neither should your regular IT support staff, so have the local administrator account password stored securely.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

7. Should The Response Platforms Be Part The Windows Domain?

Without a well managed and controlled AD environment (Microsoft 2009) the machines should not be part of the domain. Without strong Windows skill sets backed up with solid change management, avoid joining the response platforms to AD. The control of the machine is given completely to AD, so it dictates to how the machine is configured. Skilled and knowledgeable Windows administrators can use the features and tools of the AD environment to be a boon to the management of the IR machines; the opposite is equally true with poorly planned or misunderstood changes. Ultimately, the decision can be business or security policy driven, but, how AD is managed has to be the first consideration.

8. Selecting Deployment Points On The WAN

Review your own network diagrams and where to place response systems should become reasonably obvious. Candidates include:

- Links with poor bandwidth or high network latency times making management of multiple machines slow and unreliable
- Geographically remote offices with no IT support on site
- At the location of previous serious incidents at remote sites

These could be ideal candidates for the first round of deployments. The host system should have enough ram, processing power and disk space to run the response platform VM. Copy the files over out of hours using the robocopy tool from the windows 2003 resource kit with the /IPG switch to prevent overloading the network bandwidth. It may be easier to post a DVD or USB drive to the site and copy the file directly. The virtual machine should be compressed into a .rar file for performance reasons when copying over the WAN.

Deploying the software and virtual machine on a site server always seems to be the best place and provides everything in the check list. However, one of two problems may be present:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1) No server at the remote site

2) Software cannot be installed on the server

To counter for these restrictions, another system has to be used; two suggestions are the receptionist's machine or the site's ad-hoc file/print server desktop. They tend to be in better shape than most other machines at site and people know where they are physically located.

For accessing the other machines in a domain, leverage the power of Active Directory group policy objects (GPO). This works even if the virtual machine is not part of the domain. Create a group for the IR team and add in the AD accounts. Link a Restricted Groups (Melber 2004) policy to your workstation's organization unit (OU). Add the IR team group as one of the permitted groups for the local administrator group. This will give the IR team local administrator rights and access to all machines in that OU.

Never apply this to the entire domain and ALWAYS test GPO's before deploying to live systems. The assumption is that a structured active directory exists and workstations and laptops machine accounts have been moved in to their own OU's. If you have not, then this may be a good reason to rethink your AD structure.

9. Preparing The Routers

When trouble strikes, it is helpful to have a couple of quick responses ready in order to isolate a remote site from the rest of your network.

A number of pre-created access lists, for Cisco routers, provides the instant application of a highly restrictive access control lists. Such an access list would block all outbound traffic from the site, while still allowing you to work with the site, via RDP, to the virtual machine and copy files to your secure file storage system.

If there is a network team at the company, make them aware of the IP addresses the response platform use and talk over the options and solutions that fit in to your environment. For more suggestions on access lists, read some of the papers in the SANS Reading Room (SANS 2009).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

10. Keeping The Platform Updated And Current

To keep response platforms up to date, avoid manual installs. Create an installation script to deploy updates, remove old software and install new software. This maintains consistency and minimizes human error. AD's Group policy can also deploy software, if the platform is part of the AD domain. Remember that software updates will require the re-hashing of the files and executables as it may modify them.

High quality 8GB USB sticks provide an excellent delivery tool to distribute to local support staff or to the site manager. USB drives are quick to update, robust and highly portable; more so than re-writable CDs and DVDs. An added advantage is if something happen to the machine hosting the VM, a replacement machine can then quickly selected and the image reloaded from the USB stick.

11. Virus Outbreak – A Case Study

This is the way I used virtual technology to respond to a security incident with the basic problem of very poor bandwidth, no-one onsite to act as a hands-on proxy and very limited trust of any of the local machines.

One evening, as I was about to leave the office, a call came in. One of our partner sites was having problems and they thought it might be a virus. There was very little information on the environment and no one technically proficient to help out with support locally. The office was thousands of miles away.

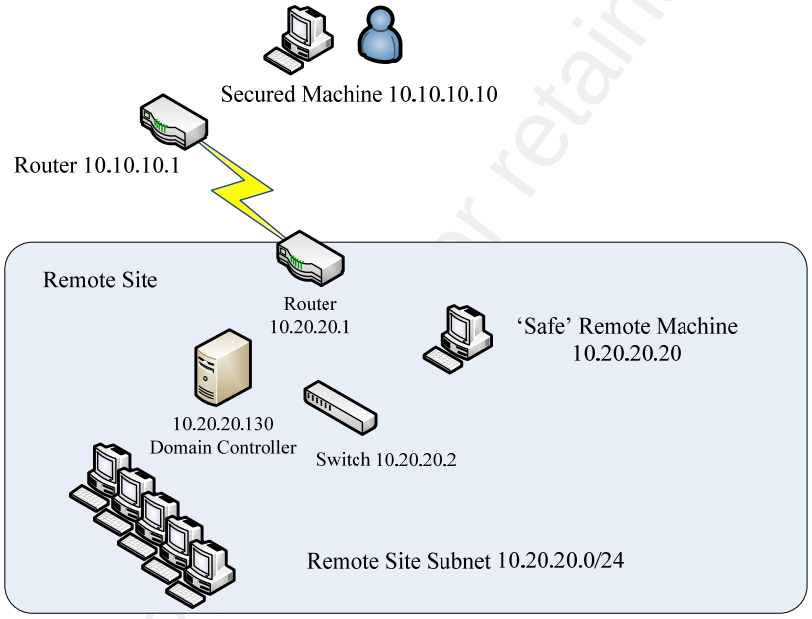
With very limited understanding of this network and its systems, I created a journal of events. I used a lined exercise book with margins, noting what I uncovered and how I responded to each event. This held all recorded events with times of each event in the margins. This was invaluable for learning how to more effectively respond the next time and what to watch out for.

I talked with the site contact, making him aware of the problem. I told him how to communicate the issue to the onsite staff and how to avoid adding to the problem. I then gathered as much useful data from the local staff, wrote it down and created a simple network map (see figure 1). The list included:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

IP addresses, subnet masks, OS types, computer types, common software (most importantly noting what anti-virus was being used), key systems and what the end user was reporting as a problem on their systems.

Figure 1 – Basic overview of the network



I locked down the site against transmitting to other remote systems and networks by placing restrictions at the infected site's router to deny any outbound connections. On the Cisco router, I added an extended inbound access list (Davis 2009) on the local interface (the one connection to the affected LAN) to block any outbound traffic from the site. With the access list set to log dropped attempts, it gave me a feel of what the level of traffic attempting to leave the site was. Note this can cause high CPU utilization on the router and significantly slow down working with the router. A further measure was to only allow access to the site from specified IP addresses, such as the machine I was connecting to the response platform via RDP (see Appendix B, list 1). The logs showed nothing obvious or unusual traffic-wise.

I requested the sole use of a machine during the incident, as it avoided any possible problems caused by someone else working on the same system. I connected with an account that has local

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

administrator access, rather than a domain account. This minimized the numbers of accounts used to manage the incident. The utility robocopy pushed Winrar, Virtual PC and the compressed response platform to the remote computer. I continued using the remote machine's IP address rather than DNS or Netbios name. Robocopy's syntax is source, destination, files to be copied and command switches.[1]

After an hour, the transfer completed and I connected to the physical system. Access to the local resources of the controlling system, such as printers and local drives have been de-selected in the options of the RDP utility. The command line MSTSC /v:10.20.20.20 /console provided local access to the system. Once the connection was made, I installed Virtual PC, uncompressed and started the response platform.[2]

From my secured work station, I accessed the response platform by its DNS name. I checked the response platform was operational; noted its IP address and that the time was correct. Windump –D identified the second interface and started up Windump on the second passive network card using Windump –I 3 –nn –s 1500 –w d:\Capture.cap –C 20. This will drop the packets in to a file on the d: drive and create a new file once it reaches 20Mb in size. [3]

---

[1] Robocopy d:\tools\install\ \\10.20.20.20\c$\install *.* /E /R:5 /W:5 /COPYALL /IPG:50 /LOG+:\tools\install. This example copies all files and folders including empty ones (/E) to a folder on the target machine 10.20.20.20, keeping the relevant information and permissions of the files (/COPYALL).
/R: is the maximum number of retries to copy the files allowed and /W: is wait time between retries. /IPG: (Inter-Packet Gap in milliseconds), provides the ability to avoid flooding the WAN bandwidth on slow lines. The /LOG+:\ switch keeps a record of the files transferred. The robocopy /? Provides an extensive list of commands as does http://www.ss64.com/nt/robocopy.html

[2] If RDP hasn't been enabled then turn on access via a GPO or connect to the remote machine with regedit, browse to HKLM\System\CurrentControlSet\Control\Terminal Server, and set or create fDenyTSConnections (a DWORD) to 0. As I was concerned about the response platform being compromised, a quick backup of the image was taken before launching. It's also possible to use commands such as PSexec to installing Virtual PC and winrar without using RDP. Microsoft has a number of VB scripts to add Virtual PC images and start them automatically.

[3] Note if the physical system had two NIC, spanning the ports on the switch to redirect traffic to allow sniffing of

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

A quick review of firewall logs on response machine in %Systemroot%\pfirelog.txt noted no failed connections from infected machines. This suggested that the infection was not searching for new targets on the LAN.

I ran a quick sweep using NMAP of the network to get a picture of what was live on the network. A basic scan swept the subnet (NMAP -PE -sP 10.20.20.0/24), (Lyon 2009) and then further scans of systems of interest (NMAP -sV -PN -O 10.20.20.130). DNS and DHCP could also be harvested for data for the Domain Controller on site; however the NMAP scans showed what was live on the network at the point of investigation. This showed 96 devices.

The network switches can provide useful details on which systems are behaving abnormally: these can appear as large transmit/receives values or suspicious MAC addresses. The following section describes an actual event of a virus outbreak. I logged on to the switch and found two more switches connected in the LAN that I had not been told about (see Appendix B), so I copied out all the MAC addresses connected to each port. I didn't see any unusual levels of network traffic or unusual events; however, it was easy to discern that three servers were connected from the high statistics on the ports. I counted 102 ports in use, although six were not transmitting.

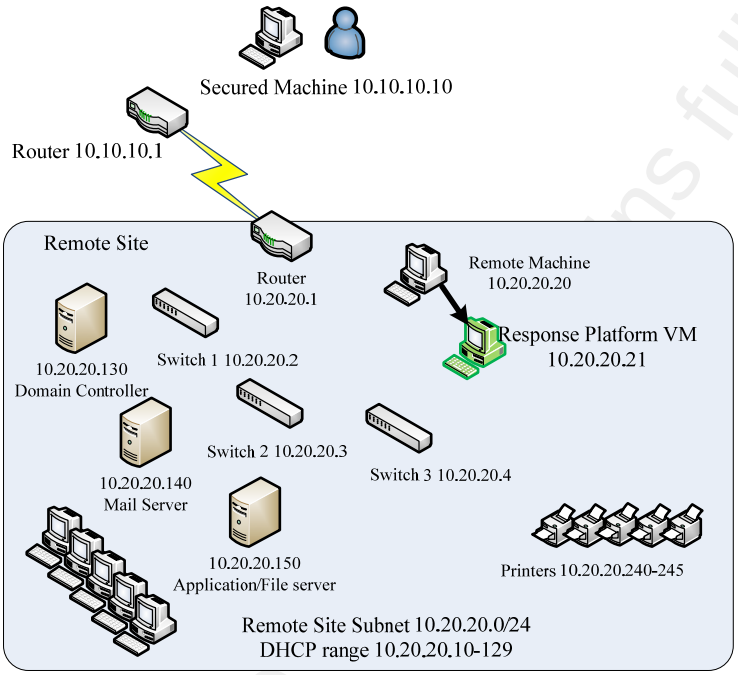
At this point I updated the notes and made a network diagram (see figure 2). I asked the site manager to confirm my findings and asked for any discrepancy in the count between the ports and NMAP scan. It appeared that some of the staff had panicked and unplugged their machines when they'd heard the word "virus". I asked the site manager to leave them unplugged and to provide me with the machine and owner's details.

---

the local LAN. This can mean packets being lost if the switch is pushing too much traffic to the VM, as the system can not keep up to capture them.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Figure 2 – A more complete layout of the network



Starting with one of the affected machines reported, I ran a script that did a number of basic checks. It looked at what services were running, queried certain registry keys, checked a number of system files and did a basic port scan report (using netstat –an dumped to a text file). I compared it to a previously created clean machine scan report. What stood out in the result was that there was a change to two registry keys, the host file had been modified and that the AV service was stopped and disabled.

This proved something was wrong, so I acquired forensic data from the target machine by the use of scripts and tools run from the response platform. WINdump was stopped to avoid adding in useless data and then, once collected, the data was hashed using md5deep for auditing reasons. I moved the files to my machine, thus avoided burdening the response platform with background analysis. An additional PERMIT rule for CIFS (TCP\UDP 445) traffic was created on the router to allow the data to be transferred from my machine to the IP address of the response platform (see Appendix B, list 2). While creating the rule and copying the data, I ran NMAP to scan the infected machine on all ports using NMAP -T5 localhost -p0-65535 -sU -sS -O2 command. The output was compared against the netstat output; just to be sure I hadn't missed anything else.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

My best option for a quick identification was to get the local AV service working, updated and then run a full scan on the suspect system. From the response platform, I replaced the host file, moved a copy of the current AV definition on the c drive, installed it, started the AV service and then ran a full scan of the machine. Almost immediately, the AV log on the infected machine filled with detections, cleaning attempts and provided a virus name. After researching the virus from my desktop and from the AV vendor's site, I had a clear understanding of what I was facing. I knew what the threat to the company was, how to detect it and how to eliminate it from the system.

The infection was a simple virus. The virus set the AV service to disabled, replaced the host file with a new one filled with 127.0.0.1 addresses for most AV vendors web sites, created itself as a service and added a couple of registry keys. It also infected any .exe file. It would then try to contact one of a dozen web sites to download updates and other malware.

Selecting another reported machine, confirming the same infected symptoms was simple. Following the same cleanup process removed all traces of the virus. A working AV would fix the infected files and blocking the web sites at the firewall would stop new malware being downloaded to the infected machines. The key problem was that users were local administrators and could re-infect themselves if they ran an infected .exe file.

I cleaned up my notes, to organize my thoughts and informed management of the situation. I put forward the two standard options of a quick fix or the full format and rebuild option[4].

Given the infection was a virus and was relatively easy to find and fix, the decision was reached to have all the local staff stop using their machines and purge the virus from all systems and files.

[4] In a number of situations, it may just be safer, more cost effective and faster to format and rebuild the machine. Taking the path of rebuilds, it is important to note the base build must be unaffected by the infection. Otherwise the machine will be re-infected. An area that may get forgotten is mapped network shares and redirected folders for user profiles and my documents. These need to be scan or even deleted to avoid having infected files located there.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

12. Case Study - The Clean Up

I'd already mapped out the environment; had an account that has privileges on the local systems, knew what the issue was and the symptoms from the investigation. I asked the site manager to plug in the six machines that had been disconnected by their users and collect up all USB storage devices so they could be scanned at a later point.

The virus created an extra process, registry keys and files. This enabled me to search for those common features. This highlights another excellent reason to have a baseline of a standard, non-infected system for reference.

From the response machine, I started a script which systematically connected to each target machine and ran the data collection scripts to acquiring the basic information. This list of machines was taken from the information generated by the NMAP scan. This had a list of all the live systems on the network with passed the data into a file using the –oN switch. Once a reasonable size group of machines have been interrogated, batches of twenty in this case, the script compressed the data and pushed it back up to the storage location of my workstation. A hash of the compressed files was taken to maintain integrity and a level of accountability.

I moved and decompressed files to a more powerful system to speed up the analysis; this left the response machine to continue on with gathering information. From there I ran a search on the data, looking for those key indicators that pointed to a compromised system.[5] I used a simple PowerShell (Wilson 2007) search string script to quickly parse data from files and output it in to a .csv format. Imported .csv or text files in to Excel makes a very simple, yet effective, analysis option.

An effective method to identify infected machines, once you know what the symptoms are, is to pick a number of those key identifiers and scan for them. In my case, if the system's host-file last

[5] Built-in Windows tools such as FC.exe or find.exe have their uses, but the windows ported version of GREP.exe is remarkably useful to pull out data.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

modified date was within 1 week, the AV definition file was older than a week and the AV services were set to stopped and disable, then this was a solid sign of infection.[6]

Using PowerShell, or any other scripting language, a script can quickly scan the target machine for these symptoms from the response VM. Basically, if service x equal stopped and host file equal or less than date and AV file equal or greater than date then output to file. These results were fed in to a .csv, opened in Excel and showing me 87 infected systems. I then placed the host names of those systems in to a text file and copied the list back to my response platform machine.

On the response platform, I created a simple batch script. It used robocopy to copy the current AV update and replace host file to the machines in the infected hosts' text file. Another script used PSexec and the SC.exe command (Laurie 2007) to update all the machines' AV definitions, start the AV service and run a full scan. This avoided additional WAN traffic of downloading the AV definitions to each machine and allowed the router filters in place until the all clear was called.

To wrap up the incident, the exported data and files showed what was the first machine to be infected (from the time stamp on the host file) and who was logged on to that machine (from the event logs). This was put in to a time line of when the other machines got infected and how quickly it spread. The response machine VM was deleted, only after all the data had been moved and the site had received the all clear. The captured data was compressed and burnt to CD for our records and training purposes.

My notes were then typed up and presented to management, with supporting evidence from the captured files. There were a number of other key factors why the infection spread so quickly. These factors were:

- poorly maintained antivirus definitions, unpatched systems
- no personal firewalls

[6] Taking Conficker.b as another example, search for the 5 to 6 windows services being disabled, the creation of a schedule task, deletion of a registry key and listening on port 80. This information is easily discovered on any one of the major AV vendor's sites such as http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?ID=76852

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- everyone was a local administrator to their machine
- a number of non-technical staff's accounts were in the Domain Administrator group.

This report provided the IT group a way to help the business understand the risks and make changes to they way they use technology to prevent this happening again. The report focused on the unnecessary use of administrator privileges for non-IT staff on their computers and keeping systems up to date with operating system and anti-virus software. A clear timeline, with the man hours of effort from the IT group required, was provided. This was balanced against the down time and revenue lost by the business for the incident. Technical details were kept to a minimum, however, a note was add how some staff may misperceive the lost of administrator rights. A reference to an internal document on how similar business units function without issue or impact from the removal of administrator rights was included.

The technical changes were straight forward, and quick to implement. A new organizational unit was created for the office's machines with two further sub OU's for laptop and desktop computers. The AD computer objects were moved to the appropriate OU. A group policy object for restricted groups was applied to the new OU. This removed all non-approved users from the local administrator group on all machines automatically.

One of the local site servers was configured as an antivirus update server for the local machines to retrieve the virus definitions from. This server got updates streamed from one of the internal AV server; reducing WAN traffic and provided a consistent AV version. A new AV policy enforce twice daily definition updates from the server to the local computers, quick virus scans at 12 pm daily and a full scan once a week at 4 pm on Fridays on all machines. Additionally, any detected viruses triggered a email alert to the help desk team. The email contained the machine name, file name, logged in user account and name of the virus discovered.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

13. Appendix A Cisco Commands

13.1. Find a Mac address on a switch

Connect to the switch, get to the enabled mode and type:

show mac-address-table

This displays all the MAC addresses of devices connected to the switch. If you have the MAC address of the device, type:

show mac-address-table address 0011.2233.4455

The port address is displayed :

Mac Address Table
Vlan Mac Address Type Ports
10 0011.2233.4455 DYNAMIC Fa0/21
Total Mac Addresses for this criterion: 1

The port is a FastEthernet port (Fa0/nn), as the example shows, the machine is connected to FastEthernet port 0/21

When there are multiple switches , this is displayed:

Mac Address Table
Vlan Mac Address Type Ports
10 0011.2233.4455 DYNAMIC Gi0/1
Total Mac Addresses for this criterion: 1

The Gi0/n indicates the MAC address is pointed to a gigabit port and since the gigabit ports usually only links to other switches, it is an indication that the MAC you are looking for is on another switch.

Use CDP (Cisco Discovery Protocol), to find out what the neighboring switches are, if it has been enabled.

Cisco_Test1# show cdp neighbor Gi0/1 detail

The response should be something similar to this:

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Device ID: Cisco_Test2
Entry address(es):
IP address: 10.20.20.3
Platform: cisco WS-C3550-24-PWR, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): GigabitEthernet0/1
[rest of section removed]

Now go back to the telnet step above and run through it again except this time use the 10.20.20.3 IP address from the show cdp neighbor output. Repeat until you find the switch and port with the MAC address.

Copy the MAC tables to a text file as it helps keep a clear record of what ports are being used by what MAC addresses. This provides excellent references when reviewing computers ARP tables.

13.2. Applying a restrict access list

13.3. List 1

```
CiscoRouter# config t
CiscoRouter(config)#access-list 110 permit tcp host 10.10.10.10 255.255.255.0 any eq 3389
CiscoRouter(config)#access-list 110 deny IP any any log
CiscoRouter(config)#interface Ethernet 1
CiscoRouter(config-if)#IP access-group 110 out
CiscoRouter(config-if)#exit
CiscoRouter(config)#exit
```

© SANS Institute 2009, Author retains full rights.

13.4. Allowing CIFS traffic

13.5. List 2

Access-list 110 permit tcp host 10.10.10.10 255.255.255.0 host 10.20.20.21 eq 445

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

14. References

Skoudis, Ed and others. (2005). SANS courseware, SEC 504 Hacker

Techniques, Exploits & Incident Handling. SANS Institute.

Microsoft "Virtual PC 2007." 2009. Microsoft. Retrieved May 9, 2009, from Web site: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=04d26402-3199-48a3-afa2-2dc0b40a73b6.

davidb "VMDK(VMWare) to VHD Converter." 26 November 2006. Retrieved May 9, 2009, from Web site: http://vmtoolkit.com/files/folders/converters/entry8.aspx

Microsoft "How to configure paging files for optimization and recovery in Windows XP." 12 July 2007. Microsoft. Retrieved May 9, 2009, from Web site: http://support.microsoft.com/kb/314482

Cogswell, Bryce. "BgInfo v4.15." 30 March 2009. Microsoft. Retrieved May 9, 2009, from Web site: http://technet.microsoft.com/en-us/sysinternals/bb897557.aspx

Microsoft "How to Create a Custom Security Template." 18 October 2006. Microsoft. Retrieved May 9, 2009, from Web site: http://msdn.microsoft.com/en-us/library/ms940857(WinEmbedded.5).aspx

NIST "Guidance for Securing Microsoft Windows XP Systems for IT Professionals." 10 October 2008. NIST. 10 October 2008 <http://csrc.nist.gov/itsec/guidance_WinXP.html

NSA "Microsoft Windows Operating System." 12 September 2006. NSA. Retrieved May 9, 2009, from Web site: https://www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems/microsoft_windows.shtml

© SANS Institute 2009, Author retains full rights.

Microsoft "Windows Server 2003 Resource Kit Tools." 28 April 2003. Microsoft. Retrieved May 9, 2009, from Web site: http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd&displaylang=en

Russinovich, Mark "PsTools v2.44." 5 November 2007. Microsoft. Retrieved May 9, 2009, from Web site: http://technet.microsoft.com/en-us/sysinternals/bb896649.aspx

Roshal,Alexander "WinRAR." 30 April 2009. RARLAB. Retrieved May 9, 2009, from Web site: http://www.rarlab.com/

Windump "WinDump: tcpdump for Windows." 01 December 2006. Windump Team. Retrieved May 9, 2009, from Web site: http://www.winpcap.org/windump/default.htm

Lyon, Gordon "Fyodor" "Nmap - Free Security Scanner For Network Exploration & Security Audits." 30 April 2008. Retrieved May 9, 2009, from Web site: http://nmap.org/

Microsoft "How to Download Windows PowerShell 1.0." 17 January 2008. Microsoft. Retrieved May 9, 2009, from Web site: http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx

Tatham, Simon "PuTTY Download Page." 12 August 2008. Retrieved May 9, 2009, from Web site: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Combs, Gerald "Wireshark." 01 May 2009. Retrieved May 9, 2009, from Web site: http://www.wireshark.org/

Fossen, Jason "Sample Scripts." 01 May 2009. Enclave Consulting. Retrieved May 9, 2009, from Web site: http://www.isascripts.org/scripts.zip

Microsoft "Script Center." 17 January 2009. Microsoft. Retrieved May 9, 2009, from Web site: http://www.microsoft.com/technet/scriptcenter/default.mspx

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Microsoft "How to configure an authoritative time server in Windows Server 2003" 15 May 2007. Microsoft. Retrieved May 9, 2009, from Web site: http://support.microsoft.com/kb/816042

Microsoft Support, (2006). How to configure an authoritative time server in Windows XP . Retrieved May 9, 2009, from How to configure an authoritative time server in Windows XP Web site: http://support.microsoft.com/kb/314054

Lyon, Gordon "Fyodor" "Top 100 Network Security Tools." 17 January 2006. Insecure.Org. Retrieved May 9, 2009, from Web site: http://sectools.org/

Kornblum, Jesse "md5deep." 04 April 2009. Retrieved May 9, 2009, from Web site: http://md5deep.sourceforge.net/

Microsoft "Windows Server 2003 Active Directory." 17 March 2009. Microsoft. Retrieved May 9, 2009, from Web site: http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

Melber, Derek "Using Restricted Groups." 25 November 2004. windowsecurity.com. Retrieved May 9, 2009, from Web site: http://www.windowsecurity.com/articles/Using-Restricted-Groups.html

SANS "SANS' Information Security Reading Room." 04 May 2009. SANS. Retrieved May 9, 2009, from Web site: http://www.sans.org/reading_room/

Laurie, Vic "Managing Windows XP Services with the Service Controller Command SC." 14 May 2007. Retrieved May 9, 2009, from Web site: http://commandwindows.com/sc.htm

Holmes, Lee (2007) Windows PowerShell Cookbook: O'Reilly

Wilson, Ed (2004) Microsoft Windows Scripting Self-Paced Learning Guide: Microsoft Press

Wilson, Ed (2007) Microsoft Windows PowerShell Step By Step: Microsoft Press

© SANS Institute 2009, Author retains full rights.

Armstrong, Ben (2009) Virtual PC Tips. Retrieved May 9, 2009, from Web site: http://blogs.msdn.com/virtual_pc_guy/

Davis, David (2009) Understanding Cisco Access Lists. Retrieved May 9, 2009, from Web site: http://www.petri.co.il/csc_how_to_use_cisco_ios_access_lists_01.htm

Lyon, Gordon "Fyodor" (2009) Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning: Nmap Project

Orebaugh, Angela and Pinkard, Becky (2008) Nmap in the Enterprise: Your Guide to Network Scanning: Syngress

© SANS Institute 2009, Author retains full rights.

Last Updated: April 16th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Abu Dhabi 2014	**Abu Dhabi, AE**	**Apr 26, 2014 - May 04, 2014**	**Live Event**
US Cyber Crime Conference	**Leesburg, VAUS**	**Apr 27, 2014 - Apr 28, 2014**	**Live Event**
SANS Austin 2014	**Austin, TXUS**	**Apr 28, 2014 - May 03, 2014**	**Live Event**
Security Leadership Summit	**Boston, MAUS**	**Apr 29, 2014 - May 07, 2014**	**Live Event**
SANS Security West 2014	**San Diego, CAUS**	**May 08, 2014 - May 17, 2014**	**Live Event**
SANS Secure Europe 2014	**Amsterdam, NL**	**May 10, 2014 - May 24, 2014**	**Live Event**
SANS ICS410 London 2014	**London, GB**	**May 12, 2014 - May 16, 2014**	**Live Event**
SANS Melbourne 2014	**Melbourne, AU**	**May 12, 2014 - May 17, 2014**	**Live Event**
SANS Malaysia @MCMC 2014	**Cyberjaya, MY**	**May 12, 2014 - May 24, 2014**	**Live Event**
SANS Bahrain May 2014	**Manama, BH**	**May 17, 2014 - May 22, 2014**	**Live Event**
AUD307: Foundations of Auditing Security and Controls of IT Systems	**Oklahoma City, OKUS**	**May 21, 2014 - May 23, 2014**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**May 26, 2014 - May 31, 2014**	**Live Event**
Digital Forensics & Incident Response Summit	**Austin, TXUS**	**Jun 03, 2014 - Jun 10, 2014**	**Live Event**
SANS Rocky Mountain 2014	**Denver, COUS**	**Jun 09, 2014 - Jun 14, 2014**	**Live Event**
SANS Pen Test Berlin 2014	**Berlin, DE**	**Jun 15, 2014 - Jun 21, 2014**	**Live Event**
SEC511 Continuous Monitoring and Security Operations	**Washington, DCUS**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANS Milan 2014	**Milan, IT**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANSFIRE 2014	**Baltimore, MDUS**	**Jun 21, 2014 - Jun 30, 2014**	**Live Event**
SANS Canberra 2014	**Canberra, AU**	**Jun 30, 2014 - Jul 12, 2014**	**Live Event**
SANS Capital City 2014	**Washington, DCUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**San Jose, CAUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
SANS San Francisco 2014	**San Francisco, CAUS**	**Jul 14, 2014 - Jul 19, 2014**	**Live Event**
SANS London Summer 2014	**London, GB**	**Jul 14, 2014 - Jul 21, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**OnlineVAUS**	**Apr 22, 2014 - Apr 27, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**