**1) 504.1 - SEC504 Notes Introduction**

https://www.sans.org/score/incident-forms/  
  
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf  
  
The Internet Storm Center  
isc.sans.edu  
  
Phishing Frameworks: sptoolkit and Phishme  
  
SANS 550 - Active Defense   
look it up  
  
False attribution - making your malware seem like it belongs or was created by someone else.  
For instance, the US government making it seem as if their tools were created by the Chinese government.  
  
  
Federal Reserve's Suspicious Activity Report at  
www.federalreserve.gov/boarddocs/press/general/2000/20000619/form.pdf  
  
PII - personal identifiable information  
PHI - personal health information  
  
Lookup GRR - google rapid response  
  
Binary image - creationg software:  
dd, Netcat, and ncat for moving data across the network, Safeback and so on.  
  
Forensic software:  
Sleuth Kit and Autopsy (free at sleuthkit.org)  
EnCase (commercial software from Guidance Software)  
Forensics Toolkit (commercial software from AccessData)  
X-Ways Forensics software (commercial)  
Others  
  
Diagnosis software you can trust:  
Statically linked binary executables from a write-once media (CD or DVD)  
Attackers often change built-in programs to lie to system admins and hide the attackers' tracks  
  
Rootkits by definition alter the trusted components of OS software to give an attacker stealthy control:  
- we advise against the use of bootable Windows PE environments  
- most of them change the hard drive and contaminate evidence  
- instead, use a good bootable Linux environment, such as SIFT  
  
The SANS Investigative Forensics ToolKit (SIFT) image can be helpful:  
http://computer-forensics.sans.org/community/downloads  
- this VMware appliance includes numerous analysis tools:  
Sleuth Kit  
log2timeline  
Wireshark  
Volatility  
ssdeep and md5deep  
Numerous others!!!  
  
Get USB Token RAM device (at least 16 Gig)  
External hard drive USB2/3 and possibly Firewire and Thunderbolt  
Ethernet TAP (4-8 ports preferable, 100/1000 Mbps), don't get a switch, taps are preferred (NetOptics are popular)  
Patch cables (2 straight-through, and one crossover)  
USB cables and serial cables for routers and other network equipment  
Laptop with multiple operating systems  
  
CheatSheets:  
http://pen-testing.sans.org/resources/downloads  
  
Have the system administrators look for unusual:  
Processes and services  
Files  
Network usage  
Scheduled tasks  
Accounts  
Log Entries  
Other unusual items  
Additional supporting (third-party) tools  
  
Show autostart program with WMIC:  
wmic startup list full  
  
look for unexpected accounts in the Administrators group:  
lusrmgr.msc  
  
check for very large files:  
FOR /R c:\ %i in (\*) do @if %~zi gtr 10000000 echo %i %~zi  
  
Scheduled tasks:  
better to check with:  
schtasks  
, because it will show also jobs created with other programs such as 'at' and not just with Scheduled Tasks.  
check logs:  
eventvwr.msc  
  
  
  
eventquery.vbs /L security  
  
wevtutil qe security /f:text  
  
Tools for mapping listening TCP/UDP ports with:  
TCPView: Free  
  
Use WINDOWS 10 for the virtual machine to run the commands!!!  
  
Check processes on your computer:  
taskmgr.exe  
tasklist /v  
wmic process list full  
  
services.msc  
sc query | more  
tasklist /svc  
  
schtasks | more  
  
net localgroup administrators  
  
Log Entries with:  
secpol.msc  
  
Local Policies - Audit Policy - Audit Logon Events - select Failure  
  
and then generate a security event  
  
- run the Event Viewer - check the Security log or Windows logs and Security  
- generate an avent running 'runas /user:administror cmd.exe", type a bogus password in when asked for a password.  
- look at your Event Viewer and Hit refresh (F5 key)  
  
There's a challenge .exe script in the C:\Tools Directory called 504lab.exe, that will emulate a compromised system.  
  
Unusual Network Usage:  
net view \\127.0.0.1  
net session  
net use  
nbtstat -S  
netstat -na  
netstat -na 5  
netstat -nao 5  
  
netsh firewall show config  
netsh advfirewall show currentprofile  
  
Unusual Processes:  
tasklist  
wmic process list full  
wmic process get name,parentprocessid,processid  
  
tasklist /m /fi "pid eq [pid]"   
wmic process where processid=[pid] get commandline  
  
- beware of base64 decoding tools online!  
  
Unusual Services:  
services.msc  
net start  
sc query | more  
tasklist /svc  
  
Unusual Reg Key Entries:  
reg query hklm\software\microsoft\windows\currentversion\run  
  
Check Startup Items:  
dir /s /b "c:\documents and settings\[username]\Start Menu\"  
dir /s /b "c:\users\[user\_name]\Start Menu\"  
  
- show autostartup programs:  
wmic startup list full  
  
  
Find Parent ID of process:  
C:\> wmic process get processid,parentprocessid,executablepath|find "process id goes here"  
  
Kill process with WMIC:  
wmic process [pid] delete  
  
Find the PID of a powershell like process, with no open port:  
wmic process where (name like "powershell%") list brief  
  
disable your firewall:  
netsh advfirewall set allprofiles state off  
  
Efficient handling of errors is part of the process!  
  
When looking at the situation, you need to determine how much damage could be caused:  
How widely deployed is the affected platform or applications?  
What is the effect of vulnerability exploitation, if a vulnerability is present?  
What is the value of the systems impacted so far? What is the value of the data on those systems?  
Can the vulnerability be exploited remotely (via a network connection)?  
Is a public exploit available? Was one recently released?  
  
Ask yourself:  
what level of skill and prerequisites are required by an attacker to exploit the vulnerability?  
Is the vulnerability present in a default configuration?   
Is a fix available for the vuln?  
Do other factors exist that reduce or increase the vuln's risk or potential impact, such as the possibility it is a worm?  
  
Letty Zeltser has prepared an Initial Security Incident Questionnaire for Responders:  
http://zeltser.com/network-os-security/security-incident-questionnaire-cheat-sheet.html  
  
BE CAREFUL:  
Do NOT delete ANY files until the case is closed out, and even then if you have storage space, save them for a document retention timeframe approved by your legal team.   
Identify every piece of evidence in your notebook.  
Control access to evidence.  
  
Each piece of evidence must be under the control of one identified person at all times:  
Include a lined page with the evidence to record all hands-offs: who an when!   
Record when you lock it up in storage.  
  
When turning over evidence to law enforcement, have the sign for it!  
  
###################  
504.1 - Incident Handling Step-by Step & Comp Crime Investigation/1.5 Incident Handling Phase Three Containment/  
  
CyberCPR - tool - free up to 3 users!  
  
Local handlers should keep making reports to the command center as they gather and analyze evidence!  
  
WordWebBugs to track the attacker!  
  
1.6 Incident Handling Phase Four Eradication:  
  
Malware on a system is a sympthom, but how the attacker got in the system in the first place, is the root cause!  
  
The business unit decides whether to keep the compromised system on or not! you can only recommend!  
  
  
1.7 Incident Handling Phase Five Recovery:  
The window to recover and ask for money after an incident is for 3 months!  
  
To and when to restore from backup and to restore operations, put that decision into the hands of the business and system owners.  
Provide your advice, but they make the final call! Document your advice in a signed memo!  
  
Monitor the system when is back online. Continue to monitor for backdoors that escaped detection!  
Utilize network and host-based IDS and IPS.  
Carefully check operating system and application logs!  
  
Look for the attacker's artifacts that helped the attacker get in, in the first place!  
  
Never name names and play the blame game! Keep it as impersonal as possible!   
Always look at what procedure, security, failsafe failed or that led to the compromise!  
  
Have a meeting as soon as practical (within two weeks of resuming production).  
Review the report!  
Finalize Executive Summary!  
Keep it short and professional (max length: half day).  
  
Based on what you learned, get appropriate approval and funding to fix: your process, your technology, improved incident-handling capabilities!  
  
  
  
1.9 Enterprise-Wide Identification and Analysis:  
- check connection logs, DNS cache, Web proxy  
- dump your current DNS cache and let it rebuild for 1 month, then run the dns-blacklists.py and you can find malware on your network.  
  
  
"if you try to see everything, you will see nothing!"  
Be smart about finding the bad guys in your network, when you look for them!  
  
Look up RITA (real intelligence threat analysis)  
  
Pull Information:  
wmic product get name, version  
wmic /node:@systems.txt product get description,name,vendor /format:csv > SoftwareInventory.txt  
  
the /node:@systems.txt allows you to run the same command on multiple systems!  
  
Learn SCCM! It has a feature to do an inventory of all the software installed on your company wide computers!  
  
Don't do incident response on 5000 endpoints in your organization! Do incident response on network segments! Do one segment at a time!  
  
Let's focus on Kansa, which is an excellent detection tool from Dave Hull!  
  
  
Kansa focuses on stacking like systems against each other to provide a ranked listing of processes, network connections, and configurations of systems! This is all part of statistical long-tail analysis!  
For functionality, install Handle.exe and autorunssc.exe from Sysinternals from Microsoft.  
For the machine launching the scripts, install LogParser from Microsoft.  
On all target systems, run the following command to enable Windows Remote Management:  
c:\winrm quickconfig  
Add all hosts you want checked into a text file and loaded in the Kansa-Master directory!  
Kansa supports the ability to pull the total count for specific things, such as Auto Start Entry Points (ASEP).  
In the following example, notice the count column on the left side, which contains MD5 hashes. These can be checked on websites, to make sure they have not been modified!  
  
.\kansa.ps1 -Targetlist .\hosts.txt -ModulePath .\Modules -verbose -Analysis  
  
Look for things that are different and things that show up only on a few systems! Use Kansa to look for these things!  
  
Ct Account:  
IEUSer  
Test\Domain Admins  
Administrator  
Support\_31337  
  
#########################  
Lab questions:  
Have we been compromised?  
Which system has been compromised?  
How was it most likely compromised?  
Who is the user on that system?  
Are any other systems at risk?  
What are our containment next steps?  
  
Hints:  
Excel or another spreadsheet helps, but is not necessary.  
You do not have to know every field of every log file  
Look for patterns  
Work as a team... Sometimes talking through what you see helps!  
  
Full walkthrough of all evidence is on the following slides!  
  
Look up a tool called Mandiant Redline!  
  
If a process was started by explorer.exe, it means someone/the user clicked it!  
  
Lookup in exploitdb U3D and flatedecode for Adobe PDF! You should be able to also find these in metasploit!  
  
In 504.5 will will revisit this case mentioned with Rekall memory analysis!  
SANS has great Windows Memory Forensics in depth courses!  
  
######################  
  
Check CyberCrimes in other countries:  
http://www.hg.org/computer-crime.html  
  
Check Logins:  
wmic computersystem get username  
  
wmic /node:@systems.txt computersystem get username /format:csv > 504\_Target\_LoggedIn.txt  
  
  
Checking Drives:  
USB drives  
Pull Historical USB usage with the following query:  
reg query HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR  
  
Or:  
wmic diskdrive get interfacetype, mediatype, model  
  
or:  
  
wmic /node:@systems.txt diskdrive get interfacetype,mediatype,model /format:csv > 504\_Target\_usb.txt  
  
  
Monitor things like logons, file access (sensitive files), drive usage with tools like Nagios, Tripwire, and SCCM in enterprises!  
Disable Windows firewall:  
netsh firewall set opmode disable  
  
netsh advfirewall set allprofiles state off  
  
  
or for Linux:  
#iptables -F  
  
###############################  
  
Logging in as Root Versus non-root (useradd):  
#useradd -d homedir login  
  
change password:  
#passwd  
or  
#passwd [login]  
  
Remember to do everything as a non-root user, except for things you truly need root for!  
If you need root:  
$sudo su -   
type your own password  
  
$whoami  
  
#service --status-all  
  
look for running processes:  
#ps aux  
  
investigate unusuall processes, getting more detail by using:  
lsof -p [pid]  
- shows all files and ports used by running processes  
  
Sometimes an attacker runs a backdoor or stashes some data on a machine and unlinks it so that it doesn't appear in the normal directory structure. We can find such files using:  
#lsof +L1  
(shows files with a link count less than 1 (that's 0 to you and me)  
  
On a Debian Linux, run the debsums tool to verify packages:  
#debsums  
  
Check size, MD5 sum, permissions, type, owner, and group of each file with information from package database. Pay attention to changes associated with items in /sbin, /bin, /usr/bin.  
  
Unusual Network Usage:  
#lsof -i  
#netstat -nap  
#arp -a  
  
Look for cron jobs scheduled by root and any other UID 0 accounts:  
#crontab -l -u root  
  
Look for unusual system-wide cron jobs:  
#cat /etc/crontab  
#ls /etc/cron.\*  
  
Unusual accounts  
- Look in /etc/passwd for new accounts, sorted from lowest to highest UID:  
#sort /etc/passwd -nk3 -t: | less  
  
Also look for UID and GID 0 accounts:  
#grep :0: /etc/passwd  
  
- normal accounts will be there, but look for new, unexpected accounts!  
  
As a final measure, look for files whose owner UID isn't assigned to a user!  
Sloppy attackers frequently create a temporary user, install a bunch of files (possibly owned by the user) and then delete that user to clean up.  
They leave the files with a non-existent user as the owner:  
#find / -nouser -print  
  
Check for resource utilization of the system!  
First, the system load (CPU particularly)  
$uptime  
  
Next the utilization of memory:  
$free  
Finally, it's useful to check available hard-drive space:  
$df  
  
  
  
- use Chkrootkit for anomalies on systems introduced by user-mode and kernel-mode RootKits  
- use TripWire to look for changes to critical system files  
- AIDE looks for changes to critical system files  
- CIS Hardening Guidelines provide a starting point for secure system configuration  
  
Unusual Files - SUID Root:  
#cd /tmp  
#cp /bin/sh /tmp/backdoor  
(any user who runs this program is given root access):  
#chmod 4111 /tmp/backdoor  
(look for SUID files):  
#find /tmp -uid 0 -perm -4000 -print  
(then remove the backdoor):  
#rm /tmp/backdoor  
  
Unusual Files - Unlinked:  
#cp /tmp  
#cp /home/tools/netcat/nc /tmp/nc  
#/tmp/nc -l -p 2222 &  
#ls /tmp/nc -l  
#unlink /tmp/nc  
#ls /tmp/nc -l  
#ps aux | grep /tmp/nc  
#lsof +L1  
#killall nc  
  
Network Usage - "lsof -i"  
#nc -l -p 2222 &  
#lsof -Pi  
  
Unusual UID 0 Accounts:  
- look for UID 0 accounts with grep  
- create a new UID 0 account called test with useradd  
- look for UID 0 accounts again with grep  
#grep :0: /etc/passwd  
#useradd -i -u 0 -s /sbin/nologin test  
#grep :0: /etc/passwd  
  
Sorting Accounts:  
- run the sort command and look for your test account  
- delete your test account when finished  
#sort /etc/passwd -nk3 -t: | less  
#userdel -r test  
  
  
Unusual Log Entries:  
- run tcpdump to force the interface into promiscuous mode  
- look in /var/log messages with grep to see promisc log entry  
#tcpdump host 10.10.75.1 &  
#grep promisc /var/log/messages  
#killall tcpdump  
  
########### Computer & Network Hacker Exploits, Part 1 ############