

SCRIPT FOR CYBERSOFT CIT TRAINING VIDEO

By Peter V. Radatti Feb. 3, 2006

A three-man play in three parts

PART ONE

A: Person (A) is sitting at a desk doing paperwork.

A knock is heard at the door and a second person (B) enters.

B: Do you have a moment?

A: Sure, what do you need?

B: I think we might have a serious security breach but I want your opinion.

A: Wow, what do you have?

B: Here are the CIT reports from last night.

A: I don't remember, what is CIT?

B: CIT is the abbreviation for the CyberSoft Cryptographic Integrity Tool. It is one of the tools in the VFind Security Tool Kit we bought last year for our Unix and Linux servers.

A: I thought VFind was just antivirus.

B: It includes antivirus but there is a whole suite of security tools. CIT is one of the tools that is included in the tool kit.

A: OK, what does it say?

B. Well, CIT shows us what files have been added, deleted, modified, duplicated or flagged over a specific period of time. Since we run it every night the time period is daily. We could run it more often if we wanted. It can also be used for other things but we don't care about that in this instance. The problem is what it is telling us about the filesystem.

A: OK.

B: Having this kind of information provides us with deep insight into what is happening in the server. In this case it is one of our development servers used by the engineering staff.

PAUSE FOR EFFECT. Papers that were brought in by B are displayed to A.

B: Look at the report here in the section that tells us what files were deleted.
SLIGHT PAUSE. A FROWNS AS HE READS THE REPORT.

B: As you can see Harry deleted most of the files in his home directory yesterday.

A: Gee, that is suspicious but why not just ask Harry why he deleted the files? He might have a good reason.

B: Well, if that was all there was I would have but this is must more disturbing. Look at the section of the report dealing with added files. Harry added files called 567.c, xyz.jpg and report.txt.

A: I don't see anything suspicious about that.

B: There is nothing suspicious about that. In fact it would be suspicious if Harry wasn't doing any work. What makes this suspicious is in this next section. Look at the report of duplicate files.

A: Oh! I see what you mean. All of the files that Harry added were copies of files from George's home directory. In addition, Harry changed the names to hide not just the fact that he copied them but as an attempt to disguise what they really are. This is really serious.

B: It gets worse. Look at the flagged files section of the report. It flagged a file in the /tmp directory that is a know hacker tool. In fact it is a cloaking devise. Since /tmp is a common directory I can't tie this to Harry but Harry is already doing things that are suspicious and maybe unethical.

A: I agree. This makes me really nervous. What else do you have?

B: Look at the added files section.

A: I see that Harry and George added files. I see that some of the files that were added are also duplicate files so that ties us down to the files having been copied within the last day.

B: Yes but that is not what I am concerned about. Look at this file, /var/log/uucp/Log.

A: I don't know what the file is.

B: It is the log file for the UUCP system. UUCP is mostly an archaic file transport system that was used to move email and files over modems prior to the availability of the Internet. Almost no one uses it anymore but it is still part of the operating system. We

don't use it but as you can see it was used. This is basically an unauthorized back channel. We don't know what was moved with it. We are investigating more.

A: This just gets worse and worse.

B: If you look again at the Modified files section you can also see that the file /var/adm/sulog was modified. That indicates that someone was able to penetrate super user access and gain administrative privileges on the system. When you combine that with the hacker program, the back channel we discovered and Harry's suspicious actions I don't know what to do!

A: I think we need to call security and legal.

B: Sigh. I was afraid of that.

FADE OUT

PART TWO – SAME DAY

A and B are sitting at a desk with a third person C.

C: OK, let me recap what I just learned from you and see if I understand this correctly.

SLIGHT PAUSE

C: One. Harry deleted all of his work. This was not authorized and destruction of company property is normally a firing offence.

C: Two. Harry made unauthorized copies of George's work. This is suspicious.

C: Three. Harry tried to hide the fact he made copies of George's work. This is very suspicious and dishonest.

C: Four. Someone placed a known hacker tool on the system.

C: Five. Someone was using an unauthorized back channel communications tool on the system. This is very suspicious.

C: Sixth and final item. Someone has fully or partially penetrated security on the system as evident since they could execute uucp and either did or was planning on hiding their actions using the hacker tool.

A: Yes, that's about right.

C: Anything else?

B: Is anything else needed? We can do additional investigations now but considering we have a full set of backup tapes that go back for months we can review them at our leisure to get a really in-depth investigation.

C: No, I heard enough.

C MAKES A PHONE CALL.

C: (On phone) I need you to remove Harry from the building immediately. Tell him someone will be contacting him at home within the hour.

FADE OUT

PART THREE

A and B are at lunch.

A: Wow, who would have believed that Harry was a spy?

B: I would never have believed it. He confessed to everything!

A: Well we did have him nailed thanks to that security tool you used.

B: Yea and the funny thing is that when we bought that tool kit we only cared about the antivirus program. The rest of the stuff was icing as far as we were concerned. I guess we got lucky that we looked at the other tools in the kit.

A: Really! I guess we really got lucky then. Uh, what is that tool kit called again?

B: VFind Security Tool Kit from CyberSoft. It doesn't even cost much.

A: Are we running it on our other servers?

B: No! I think I better look into it. Who knows how many Harry's we might have!

FADE OUT.