

SCRIPT FOR CYBERSOFT VFINN DATA SPILL TRAINING VIDEO

By Peter V. Radatti May 4, 2007

A three-man play in one part

Joe: Folks, we have a situation. There has been a data spill from project Top Secret Blue Hats to project Top Secret Deep Seven. As you know this is a matter of national security. The last time something like this happened it took us two weeks of 24/7 to recover and we were never completely sure if we got it all. I have been in a meeting with Director Stross and he has authorized \$10 Million for this cleanup. \$9 Million for loss of productivity and \$1 Million for the actual work.

Joe: George, how long do you think it will take to do a full cleanup?

George: Do we know what was spilled?

Joe: Not entirely. We know the data should be tagged as Blue Hats but it may not all be. We do have a liaison with Blue Hats who will provide us with samples of the data that may have been compromised. The source code that was lost will have Blue Hats in the headers but the remainder of the code will not. Documents will of course all be labeled but as you may remember from the last time there are issues in that people all type the label in different ways. Some use all caps, some all lower case, and some mixed case. People put spaces or tabs between the words, some put spaces between every letter. In addition, we don't know when the leak happened or how. We discovered Blue Hats data on a Deep Seven server this morning. Finally, there is several hundred terabytes of data to search. In other words, it's not going to be easy. We have incomplete information; a complex pattern of what we need to search for and Director Stross is waiting.

George: I assume we have authorization for overtime?

Joe: Effective immediately you not only are authorized for overtime but it is mandatory. Double shifts for everyone. Lay out a work schedule so we keep operating 24/7. We need to keep down time to a minimum. As you know there are a lot of people who are going to be idle while you are doing the cleanup. Not only is this a large waste but it will impact our development schedules and of course our ability to actually operate. Given the information so far does anyone have any idea how long we will be down? Keep in mind that last time it was two weeks and we really cannot afford two weeks again.

Sue: Well, it's 4:00 now. Most folks are going home in one hour. We can "schedule" a system crash that will keep a lid on what is going on. No reason to instill panic in the troops. If I leave now we can have all of the servers rebooted in single user mode by 6:00. As you know there are a lot of servers.

George: OK. How long do you think your team will take for the cleanup?

Sue: Well, if I meet with Blue Hats at 5:00 while the team is bringing down the systems we should have an initial idea of what we are looking for about the same time the servers are rebooted. You already gave me a good description of what to look for in the way of labels. We can manually start a virus scan of the system about 7:00. That would be early for the scan....

Joe: There is no need for a virus scan. This is critical and all other processes, including backups are to be suspended.

Sue: Oh, in this case we will do the cleanup using the virus scanner.

Joe & George: What?

Sue: Sure, we are using the VFind Security Tool Kit from CyberSoft. The virus scanner is a tool called VFind. It is fully programmable. Not only can we program it but also it has the most complete pattern analysis language available. Solving the problem with letter case and white space is actually very simple using VFind's CVDL language. With the decomposition tool UAD that it normally runs with we can even scan stored email messages, zip files and other archives. We will have 80% of the cleanup done by the time first shift reports for work tomorrow.

Joe & George: Impossible!

Sue: No, it really will be easy to do. Not only will we be able to scan all the data for the labels but since we can add pattern analysis directives to VFind we can scan for Blue Hats data that is not labeled as long as the Blue Hats people can give us a good idea of what to look for. Since VFind is fast there is no reason that it can't look for Blue Hats data at the same time that it does its normal virus scan. This also helps us understand if there was a cyber attack component involved in the data spill. Finally, since all of the VFind Security Tool Kit tools are fully scriptable we can use a script that will quarantine the Blue Hats data to a directory. That will give us a chance to review the data once it is removed and give us an exact measurement of what was spilled and thereby how. Maybe even who did the spill.

Joe: OK, Sue it is in your hands. Lets meet again tomorrow morning.

NEXT DAY

Sue: OK, we are done and just waiting for authorization to put the servers back into production! The quarantined Blue Hats data is in the hands of the Security Analyst and off of all Deep Seven. The Analyst is happy and gave his blessing.

Joe: Then you are authorized to go back to production. What I want to know is how you were able to do this in less than 24 hours when the last time it took two weeks?

Sue: Our servers have large disk I/O bandwidth and fast processors. We broke the file system tree into multiple paths on each server and processed all of them at the same time. With a little experimentation we figured out the optimal number of files we can scan at the same time without a bottleneck. We did not even use the CIT tool to reduce the files scanned to just those that were added or modified so that we can state that 100% of all data on all servers were scanned for Blue Hats data. I am confident that we found 100% of the Blue Hats data as it was defined to us.

Joe: Wow, great job!

George: So do we get to keep the \$10 Million authorized for the cleanup? We really could use some more equipment.

Sue: Yes and how about a raise?

Joe: As far as keeping the \$10 Million the answer is No. Its use it or lose it.

Sue: OK, but I am the hero so I should get a nice bonus at least! That comes in under use or lose.

Joe: Tell you what Sue; lets increase your responsibilities to include Manager of Data Spill Cleanup. Then it's a normal part of your job.

Sue: Gee thanks.