

Forensic Survey, help needed for a research/training program

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-01/msg00515.html>

- *From:* Mike Haberman <mikeh@xxxxxxxxxxxxxx>
 - *Date:* Thu, 31 Jan 2008 11:09:07 -0600
-

Hello Security Expert,

I am a network/security researcher at NCSA/UIUC. I am requesting your help to answer a list of 24 security/forensic related questions. The survey is part of a research and training program that we are hosting.

If you are interested in knowing the results, I will set up a web page with the tabulated answers (anonymously).

Please email the completed form back to me: mikeh@xxxxxxxx
Thanks again; I appreciate the time you are taking to help me out,

mike haberman
mikeh@xxxxxxxx

Instructions

For most questions, try to provide at least 3 different answers (list/rank the answers in order of importance).

If an answer involves using a tool to obtain the necessary information, be as specific as possible. If the tool used is a private/internal tool, please mention that as well. If the answer requires a complete tool chain, just list the tools required.

For questions that don't specify a specific platform, be sure to list what platform (Windows XP, Linux, etc) the answer applies to.

You can respond to this email with your answers in line, or send me back just the answers (with a reference to the question number). If you want to remain completely anonymous, you can spoof the from address or use old fashioned mail:

NCSA
mike haberman

Forensic Survey, help needed for a research/training program

1205 W. Clark St.
Room 1008
Urbana, IL 61801

O./_____

O\
Forensic Survey

Background:

A. What OS are you most knowledgeable about?

B. Do you consider yourself to be more knowledgeable in host based forensics or network based forensics?

C. How many years of experience to you have with respect to computer security?

Host based forensic questions
=====

Question #1

When on a system that you are trying to seize evidence from, what are the most important things you should AVOID doing? List in order of importance.

Question #2

What are the most important items to capture before isolating or shutting down a suspected host? For each item list the command you would use along with the information for both a Unix based machine and a Windows based machine.

Question #3

A hacker installs a piece software on a Linux based machine. What does he do to prevent its detection? For each technique listed, what could you do to reveal the hacker's ploy.

Question #4

A machine has just been Owned, what generally is the hackers' first order of business?

Question #5

During an investigation, a file named destr0yAll is found. What tools would you use to reverse engineer the functionality of the program/binary? (Assume a Unix based analysis environment).

Question #6

Where can you find hidden data?

Question #7

Name the most important sources of logs for identification of an event at the host perimeter (when data leaves/enters a host)?

Question #8

Give a reason why you would want to literally pull the plug of a infected system rather than shutting it down or disconnecting it from the network?

Question #9

Perpetrator is caught; laptop apprehended. But he's not talking. Where do we gather information to determine what he was using his laptop for.

Network Based Questions

=====
Question #10

Name the most important sources of logs for identification of an event at the network perimeter?

Question #11

You're given a log of network traffic. What are the issues surrounding the contents of the file?

Question #12

What evidence might there be of a compromised DHCP server?

Question #13

During an investigation, you find out that a firewall was unable to stop a hacker. What are the most likely causes of this?

Multi Layer Questions

=====

Question #14

A hacker connects to the Internet from his home, what techniques can he use to obscure the computer he uses?

Question #15

Given a log file for an incident, what can you look for to determine if the log file itself has been tampered with?

Question #16

You need to figure out who has logged into a host. Name all the possible sources that could be used to determine when and who has logged into a particular system.

Question #17

What evidence will there be of an IRC bot running on a Windows 2000 box?

Question #18

An employee notices that when his browser is pointed at google.com, whitehouse.com is served up. What are the possible causes of this problem? For each cause, what information source would you need to verify?

Question #19

You are need to access data that might provide evidence for suspicious Internet activity. Name a few sources that might get you this information.

Question #20

You received an "anonymous tip" through an email. What sources do you use to figure out who the actual author of the email is.

Miscellaneous Questions

=====
Question #21

Name several sources for finding recently vulnerable (zero day) software exploits?

Question #22

What are the biggest problem(s) you have encountered when working with outside law enforcement (local police, fbi,) on an incident?

Question #23

87.242.82.70 is involved with attempting to brute force it's way into the victim's network. What tools/processes can you use to determine who to talk to.

Question #24

During an investigation, you use whois to determine the owner of an address (or block of addresses), what are the potential problems with the information returned from whois?

For the following questions, just provide a single answer.

Forensic Survey, help needed for a research/training program

1. How can one mark digital data such that a single bit flip would flag the data as tampered with.
2. Name me your favorite Unix text processing tool.
3. What is the single most important rule of digital forensics?
4. During an investigation of a computer running Windows 2000, what are the most important types of information you can acquire from examining the Registry?
5. Name me an important log file on a client running Windows XP
6. Which movie makes the biggest mockery of digital forensic investigation?
7. Who is your favorite TV based police/fbi/crime fighter (not a superhero) ?
8. Name a technique to gain illicit access to a system.
9. Name a technique to illicitly escalate privileges on a system.