

CS 491S: Computer and Network Security

Fall 2008

Lab Exercise 3: Incident Handling

Abstract:

This lab is intended to give you experience with real world incident analysis remediation and countermeasures. The lab builds on many of the topics covered in class so far. The lab is oriented towards research and analysis of recent incidents and calls for a reasonable degree of extending what you learned in class.

1 Tools required for this lab:

- Access to a web browser
- Ability to reason and clearly explain your thoughts and designs

2 Pre-lab Background:

You may need to use things like google to help you find some of the background materials to complete this lab.

Please complete the following exercises. As always, you must hand in a lab write up containing answers to questions asked for each task.

3 Lab exercise: Sasser worm

The sasser worm was discovered on 30 April 2004. The University's network security tools detected the first sasser infection at 10:30 on 3 May 2004. Within 1 hour we reached 95% saturation of vulnerable hosts.

The intent of this lab is to understand the process of security. You will research the worm, suggest theoretical countermeasures for prevention and detection and determine an appropriate incident handling process for a theoretical organization.

Required reading

LURHQ Sasser Analysis
<http://www.secureworks.com/research/threats/sasser/>

Microsoft Sasser Information
<http://www.microsoft.com/technet/security/alerts/sasser.msp>

Note: You may have to do some additional reading beyond the above on your own in order to complete the lab.

What to hand in

Question 1. After doing the above reading, what steps could the organization have implemented before the worm hit. Describe three explicit steps that the organization could have taken between 13 April, when the patches were released, and 30 April, when the worm was released.

Question 2. Sasser took advantage of the LSASS vulnerability patched by Microsoft's MS04-011 update. Why was the spread of Sasser so much greater than the spread of bagel or netsky. Specifically speak to the vectors each exploit uses and the mechanism necessary for propagation of the malware.

Question 3. Why does Sasser.D open an ftp server on 5554/tcp? What are the advantages from the perspective of the malware author?

Question 4. Sasser.D also scans 10.0.0.0/8 and 192.168.0.0/16 looking for vulnerable hosts to infect. Why would the malware author want to scan these ranges?

Question 5. What perimeter defenses would an organization use to prevent the spread of Sasser across their network border? Don't simply state "They would use a firewall", but instead explain how they would configure a perimeter security you choose. Describe three (separate or additive) countermeasures.

Question 6. Suppose a new variant of Sasser is released tomorrow. It varies from previous variants in that it randomly modifies one byte of data on the hard drive every second. What effect would this have on the propagation of this new variant?

Question 7. Evaluate the snort signatures at the link below. Comment on the effectiveness of these signatures.

```
alert tcp $HOME_NET any -> any 9996 ( msg:"Sasser ftp script to transfer up.exe";  
content:"|5F75702E657865|"; depth:250; flags:A+; classtype: misc-activity; sid:1000000;  
rev:3;)
```

```
alert tcp any any -> $HOME_NET 5554 ( msg:"Sasser binary transfer get up.exe";  
content:"|5F75702E657865|"; depth:250; flags:A+; classtype: misc-activity; sid:1000001;  
rev:1;)
```

4 Analysis exercise: Web-Attacker toolkit

Required reading

Web-Attacker description and background

<http://securitylabs.websense.com/content/Alerts/1074.aspx>

Web-Attacker source code analysis

<http://securitylabs.websense.com/content/Blogs/2608.aspx>

S'kiddies get into spyware for just \$15

http://www.theregister.co.uk/2006/03/27/spyware_diy/

What to hand in

Question 9. The assigned readings describe the background and source code of the Web-Attacker toolkit. The toolkit permits attackers to use a compromised web server to spread malicious software easily and for little cost. Analyze the description of the *ie0609.cgi* script. Describe why the attacker would want to use a database to store the UserID and related data. Also explain the advantage to the attacker of being able to view the statistics generated by the toolkit.

Question 10. Toolkits such as Web-Attacker provide a platform for attackers that are not technically sophisticated. These attackers can cause substantial harm to a large number of unsuspecting users with relatively limited effort. As such, these toolkits can pose substantial challenges for internet hosting companies that serve a large number of website where they do not control the content of each site. Suppose you are brought in as a consultant to recommend steps an internet hosting company could take to prevent the use of toolkits like Web-Attacker. What defenses (both tools and processes) would you suggest to prevent the use of toolkits like Web-Attacker? There are two scenarios for the use of Web-Attacker: attackers who compromise a hosted site; and attackers who are legitimate customers of the hosting company but using it for nefarious purposes. Describe how you would defend against each of these cases. Write up a 1-2 page set of recommendations.

5 StormWorm

Required reading

StormWorm is a still active piece of malware that has been causing problems not only for users, but also targeting well known anti-spam and anti-malware sites.

<http://www.secureworks.com/research/threats/storm-worm/>
http://www.infoworld.com/article/07/02/23/090Psecadvise_1.html

What to hand in

Question 12: Why would the creator of stormworm decide to use DNS instead of HTTP as the messaging mechanism for dDoS targets? Defend your answer.

Question 13: Why does stormworm use p2p protocols for distribution of multi-stage executables? What properties do p2p networks have that would make this more desirable than a single source for the malware.

6 Anti-virus effectiveness

Required reading

<http://blog.fireeye.com/research/2008/11/does-antivirus-stop-bots.html#more>

What to hand in

Question 14: Explain how the arguments laid out in the above article reinforce the concepts of 'defense-in-depth' that we have stressed through the semester. Cite specific example for how to deploy a security architecture the will defend against the current threat environment and effectively mitigate risk.

7 Evaluation

Question 15: How hard was this lab? Was it fair? How would you change it to improve it?