Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años
UNIVERSIDAD
POLITÉCNICA
DE SAN LUIS POTOSÍ

BugCon
security conferences

Retos forenses de red

Hugo González

@hugo_glez

UPSLP

¿Qué es un reto forense?

Donde encontrarlos

- Sans ?!?!
  - http://forensicscontest.com/
- The Honeynet Project
  - http://honeynet.org/challenges
- Google
  - http://www.google.com/search?q=network+forensics+challenge

¿Por qué resolverlos?

Tips

- Las preguntas sirven como guía
- Las preguntas son tips de que buscar
- Tener herramientas disponibles
- Python !!!

Forensics Contest

Puzzle # 6 Ann's Aurora

Descripción

- The contest is a client-side attack based on Operation Aurora. This packet capture contains a full recording of a real Windows system getting exploited via the same mechanism that was used to exploit Google. Ann spear-phishes a developer, who clicks on a link and connects to her malicious web server. Then she configures the victim to make outbound persistent connection attempts to her server so that she can retain access and reconnect in the future.

1 What was the full URI of Vick Timmes’ original web request? (Please include the port in your URI.)

http://10.10.10.10:8080/index.php

2 In response, the malicious web server sent back obfuscated JavaScript. Near the beginning of this code, the attacker created an array with 1300 elements labeled “COMMENT”, then filled their data element with a string. What was the value of this string?

- vEI

3 Vick’s computer made a second HTTP request for an object.

- 1. What was the filename of the object that was requested?

index.phpmfKSxSANkeTeNrah.gif

- 2. What is the MD5sum of the object that was returned?
- df3e567d6f16d040326c7a0ea29a4f41

4 When was the TCP session on port 4444 opened? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)

- 1.2
-

5 When was the TCP session on port 4444 closed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)

- 87.5

6 In packet 17, the malicious server sent a file to the client.

a What type of file was it? Choose one:

* Windows executable ******

* GIF image

* PHP script

* Zip file

* Encrypted data

b What was the MD5sum of the file?

- b062cb8344cd3e296d8868fbef289c7c

7Vick’s computer repeatedly tried to connect back to the malicious server on port 4445, even after the original connection on port 4444 was closed. With respect to these repeated failed connection attempts:

a How often does the TCP initial sequence number (ISN) change? (Choose one.)

* Every packet
* Every third packet ****
* Every 10-15 seconds
* Every 30-35 seconds
* Every 60 seconds

B How often does the IP ID change? (Choose one.)

* Every packet ***

* Every third packet

* Every 10-15 seconds

* Every 30-35 seconds

* Every 60 seconds

C How often does the source port change? (Choose one.)

* Every packet
* Every third packet
* Every 10-15 seconds ****
* Every 30-35 seconds
* Every 60 seconds

8 Eventually, the malicious server responded and opened a new connection. When was the TCP connection on port 4445 first successfully completed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds) 123.6

9 Subsequently, the malicious server sent an executable file to the client on port 4445. What was the MD5 sum of this executable file?

10 When was the TCP connection on port 4445 closed? (Provide the number of seconds since the beginning of the packet capture, rounded to tenths of a second. ie, 49.5 seconds)

- 198.4

Herramientas a utilizar:

- Cerebro !!
- Wireshark
- Tcpdump
- Editor hexadecimal
- python

Manos a la obra !!!

Challenge #1 2010

Pcap attack trace
By Tillmann Werner

- A network trace with attack data is provided. (Note that the IP address of the victim has been changed to hide the true location.) Analyze and answer the following questions:

1 Which systems (i.e. IP addresses) are involved? (2pts)

2 What can you find out about the attacking host (e.g., where is it located)? (2pts)

3 How many TCP sessions are contained in the dump file? (2pts)

4 How long did it take to perform the attack? (2pts)

5 Which operating system was targeted by the attack? And which service? Which vulnerability? (6pts)

6 Can you sketch an overview of the general actions performed by the attacker? (6pts)

7 What specific vulnerability was attacked? (2pts)

8 What actions does the shellcode perform? Pls list the shellcode. (8pts)

9 Do you think a Honeypot was used to pose as a vulnerable victim? Why? (6pts)

10 Was there malware involved? Whats the name of the malware? (We are not looking for a detailed malware analysis for this challenge) (2pts)

11 Do you think this is a manual or an automated attack? Why? (2pts)

Manos a la obra !!!

Preguntas, comentarios.

hugo.glez@gmail.com

@hugo_glez

Tools

- Xplico
- Networkminer
- Honeysnap
- Ngrep
- Argus
- Sancp
- Cxtracker

Fuzzing

- Taof
- Gpf
- Peach
- Minifuzz
- Comraider
- Danzier
- Scapy