Shellcode Detection in IPv6 Networks with HoneydV6

Sven Schindler

Potsdam University
Institute for Computer Science
Operating Systems and Distributed Systems

Vienna, August 30, 2014

Outline

1 Introduction

2 Shellcode detection and analysis

3 Honeypot shellcode detection extension

4 Evaluation

5 Summary

Outline

1 Introduction

2 Shellcode detection and analysis

3 Honeypot shellcode detection extension

4 Evaluation

5 Summary

What is shellcode

- Shellcode: **exploit payload** that spawns a shell

What is shellcode

- Shellcode: **exploit payload** that spawns a shell
- ... or any other malicious code carried by an exploit

What is shellcode

```
0000000: 31c9 89cb 6a46 58cd 806a 0558 31c9 5168  1...jFX..j.X1.Qh
0000010: 7373 7764 682f 2f70 6168 2f65 7463 89e3  sswdh//pah/etc..
0000020: 41b5 04cd 8093 e828 0000 006d 6574 6173  A......(...metas
0000030: 706c 6f69 743a 417a 2f64 4973 6a34 7034  ploit:Az/dIsj4p4
0000040: 4952 633a 303a 303a 3a2f 3a2f 6269 6e2f  IRc:0:0::/:/bin/
0000050: 7368 0a59 8b51 fc6a 0458 cd80 6a01 58cd  sh.Y.Q.j.X..j.X.
0000060: 80
```

Listing 1 : Example Metasploit exploit [6]

Honeypots

- **honeypots** to encounter modern attacks
- systems without production value
- high- and low-interaction honeypots available
- direct interaction to **observe encrypted connections**
- major IPv6 general-purpose honeypots: Dionaea [3] and HoneydV6 [9]
- no shellcode detection support in HoneydV6 → **extend HoneydV6**

Why HoneydV6

- customised network stack in userspace
- **simulate entire IPv6 networks** with thousands of hosts
- dynamically creates virtual low-interaction honeypots
- **monitor layer 3 attacks**

Outline

1 Introduction

2 Shellcode detection and analysis

3 Honeypot shellcode detection extension

4 Evaluation

5 Summary

Shellcode detection and analysis

- identify traffic containing shellcode automatically
- analyse shellcode behaviour
- goal: **find and evaluate existing libraries** for HoneydV6 integration

Shellcode detection mechanisms

- pattern matching

Shellcode detection mechanisms

- pattern matching
- execution on a real OS

Shellcode detection mechanisms

- pattern matching
- execution on a real OS
- emulation
  - **execute shellcode** in a safe environment [8]
  - many papers but **few implementations**
  - **libemu** only open source library[2]
  - alternative Shellzer is limited to JS, Flash and PDF malware [4]

libemu

- C library developed in 2007
- used by Dionaea
- x86 emulator - registers, program counter, virtual memory, disassembler
- utilises address determination problem to locate code sequences
- *emu_shellcode_test()* returns position of detected shellcode sequence
- ability to trace accessed system calls

Online malware analysis

- Malwr [5]
  - web interface for Cuckoobox
- Anubis [1]
  - provides interface to upload shellcode samples
  - provides HTML/XML/PDF/ASCII result protocol

Outline

1 Introduction

2 Shellcode detection and analysis

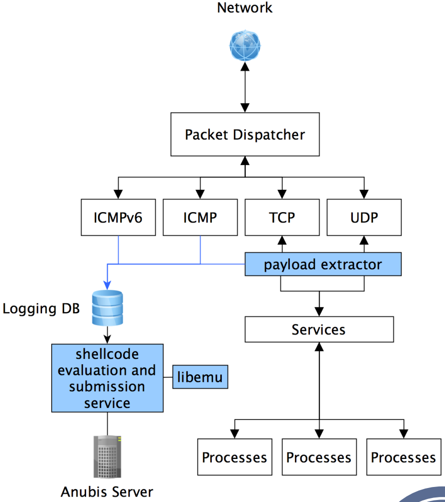
3 Honeypot shellcode detection extension

4 Evaluation

5 Summary

Integration of libemu and Anubis into HoneydV6

- added **shellcode buffer** to connection structures(*tcp_con*, *udp_con*)
- **extended callbacks** for traffic handling (*cmd_tcp_write*, *cmd_tcp_write*)
- **SQLite database** setup and connector
- background job uses libemu to **mark and submit "interesting" received traffic**



Modifications for Anubis

- **support for Windows and Android binaries only**
- msfencode to **create unencrypted x86 binaries**
- MD5 checksum generation for samples to avoid duplicates
- libcurl-based uploader for submission and report url logging

Outline

1 Introduction

2 Shellcode detection and analysis

3 Honeypot shellcode detection extension

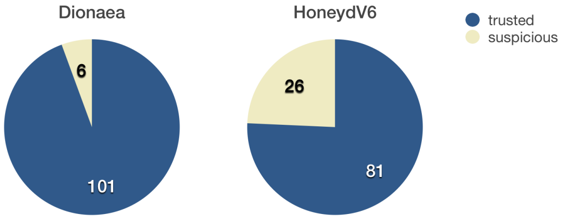
4 Evaluation

5 Summary

Detection rate measurement setup

- Metasploit framework [6] to generate **107 shellcode samples**
- Dionaea with modified default configuration to accept **http requests**
- HoneydV6 configured with a single host running a web server
- Netcat [7] for shellcode transmission (different source ports for correlation)
- inspected both databases for traffic marked as malicious

Detection rate measurements results



- all shellcodes detected by Dionaea were also detected by HoneydV6
- **both honeypots use libemu** to detect shellcodes
- further malware profiling in Dionaea

HoneydV6 shellcode buffer size variations

Buffer Size	16	32	64	128	256 - 8192
#Detected samples	0	12	23	25	26

Table : HoneydV6 detection rate for different shellcode buffer sizes

- measurements with **default buffer size of 1024 bytes**
- at least 31 bytes buffer needed to detect first sample
- depending on exploit larger buffer sizes needed

Outline

1 Introduction

2 Shellcode detection and analysis

3 Honeypot shellcode detection extension

4 Evaluation

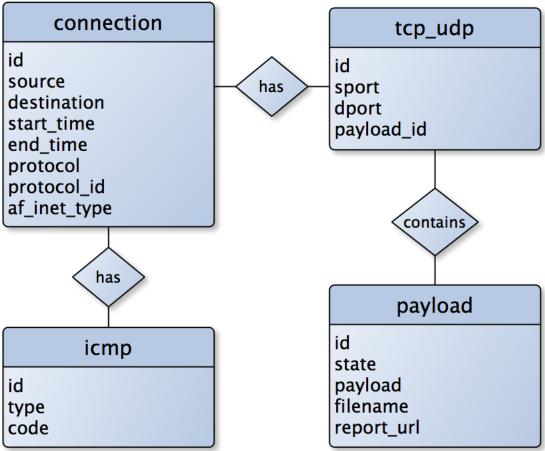
5 Summary

Summary

- IPv6 attack detection still in early stage
- integration of libemu into HoneydV6 is a first step
- only two general-purpose low-interaction honeypots available
- no further developed open source shellcode detection libraries available

Time for questions...

New HoneydV6 logging database



connection
id
source
destination
start_time
end_time
protocol
protocol_id
af_inet_type

tcp_udp
id
sport
dport
payload_id

icmp
id
type
code

payload
id
state
payload
filename
report_url

References

[1] Anubis.
Anubis: Analyzing Unknown Binaries, nd.
Available from: http://anubis.iseclab.org.

[2] Paul Baecher and Markus Koetter.
libemu – x86 Shellcode Emulation, nd.

[3] Dionaea.
dionaea catches bugs.
http://dionaea.carnivore.it/, nd.

[4] Yanick Fratantonio, Christopher Kruegel, and Giovanni Vigna.
Shellzer: A tool for the dynamic analysis of malicious shellcode.
In *Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection*, RAID'11, pages 61–80, Berlin, Heidelberg, 2011. Springer-Verlag.

[5] Malwr.
Malwr - Malware Analysis by Cuckoo Sandbox, nd.
Available from: https://malwr.com.

[6] Metasploit.
Metasploit: Penetration Testing Software, nd.
Available from: http://www.metasploit.com.

[7] Netcat.
The GNU Netcat project, nd.
Available from: http://netcat.sourceforge.net.

[8] Michalis Polychronakis, Kostas G. Anagnostakis, and Evangelos P. Markatos.
Network level polymorphic shellcode detection using emulation.
In *Proceedings of the Third International Conference on Detection of Intrusions and Malware & Vulnerability Assessment*, DIMVA'06, pages 54–73, Berlin, Heidelberg, 2006. Springer-Verlag.

[9] Sven Schindler, Bettina Schnor, Simon Kiertscher, Thomas Scheffler, and Zack Eldad.
Ipv6 network attack detection with honeydv6.
In *Communications in Computer and Information Science (CCIS)*. Springer, 2014.
to appear.