NTNU

Innovation and Creativity

Digital Forensic Reconstruction and the Virtual Security Testbed ViSe

DIMVA 2006

André Årnes, Norwegian University of Science and Technology
Paul Haas, University of California Santa Barbara
Giovanni Vigna, University of California Santa Barbara
Richard A. Kemmerer, University of California Santa Barbara

The Problem

- Test attack tools as part of a digital forensic reconstruction to support or refute a hypothesis
- Analogy to testing firearms ballistics in physical forensics
- We employ the ViSe virtualization environment to minimize resource usage
- The goal is to perform testing in a forensically sound manner in order to present the results in court

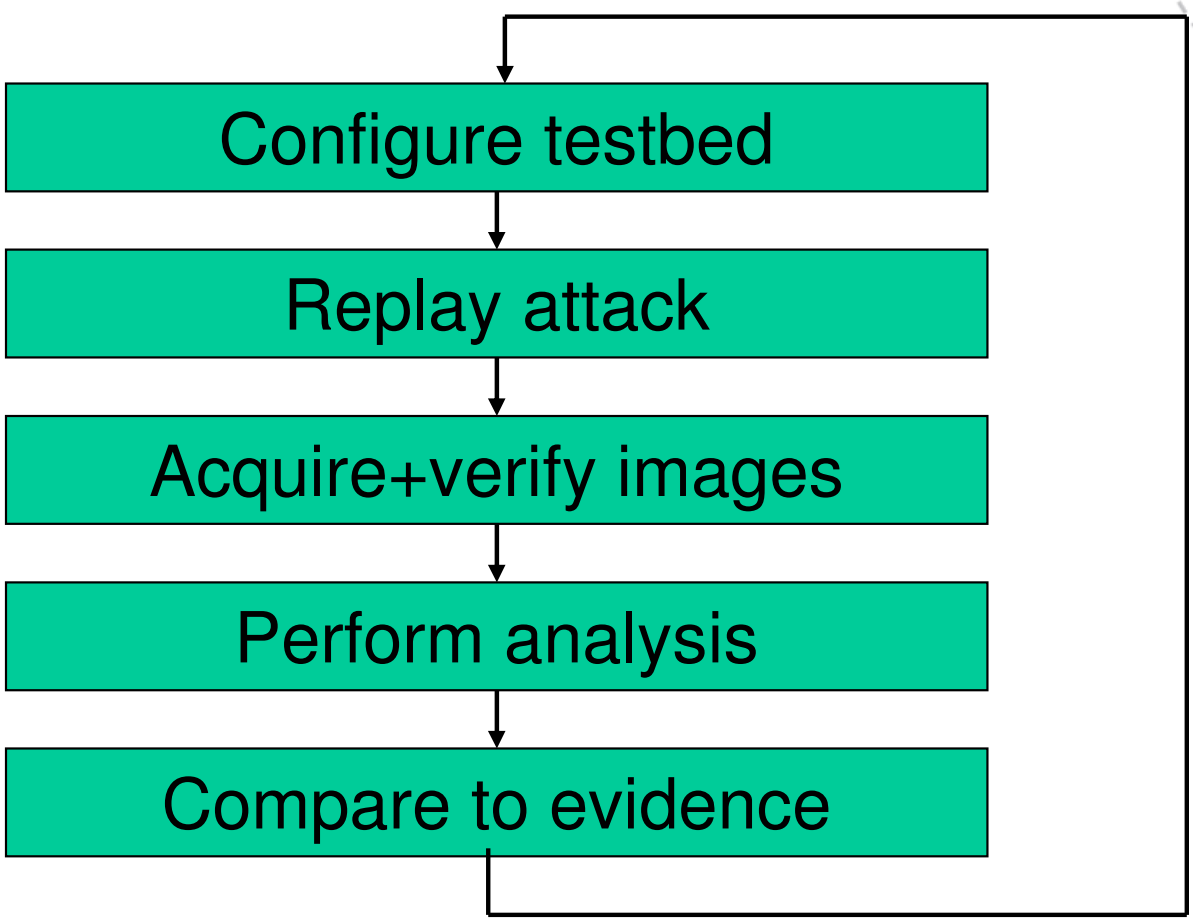
NTNU
Innovation and Creativity

Digital Forensics

- Digital crime scene
  - Attack hosts
  - Victim hosts
  - Third-party hosts
- Digital evidence
  - E.g., network dump, file, log entries, IDS alerts, RAM, etc.
  - Evidence dynamics: ”any influence that changes, relocates, obscures, or obliterates physical evidence, regardless of intent” [Chisum 2000]
- Event Reconstruction
  - We wish to determine the most probable sequence of events
  - Hypothesis
  - Event chain
  - Each event has causes and effects

NTNU
Innovation and Creativity

Methodology



NTNU
Innovation and Creativity

Clarifications

- This work does not subsitute the digital forensic investigation itself.
- The event reconstruction is not a ”crime reenactment”.
- The reconstruction can only be an approximation of the real case. Its purpose is only to support or refute a hypothesis.
- A reconstruction with corresponding testing is still possible even if all the evidence in a digital crime scene may not be available to an investigation.

NTNU
Innovation and Creativity

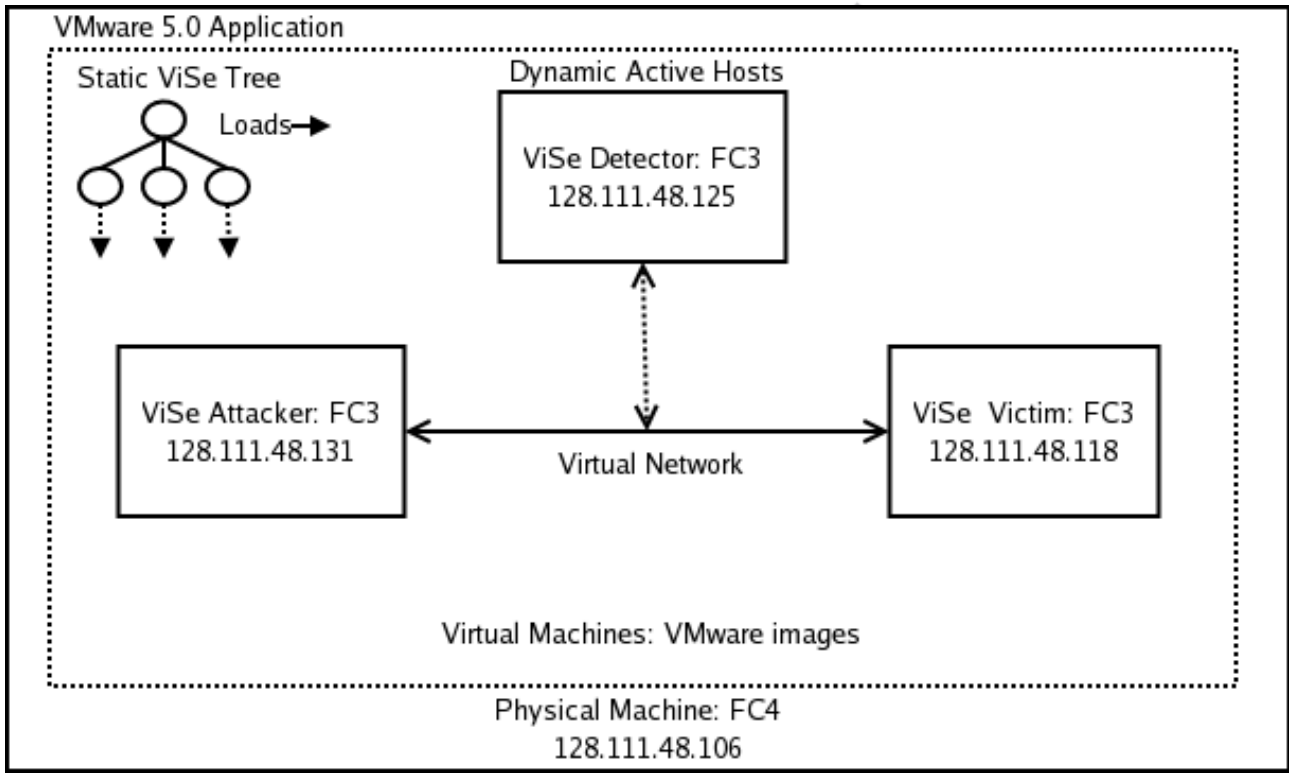
Testbeds

- Physical testbeds
  - Netbed, Deter
- Virtualization platforms
  - Xen, MS Virtual PC, UML, VMware
- Simulations and modeling
  - LLSIM, [Stephenson 2003], [Gladyshev et al 2004]

NTNU
Innovation and Creativity

ViSe

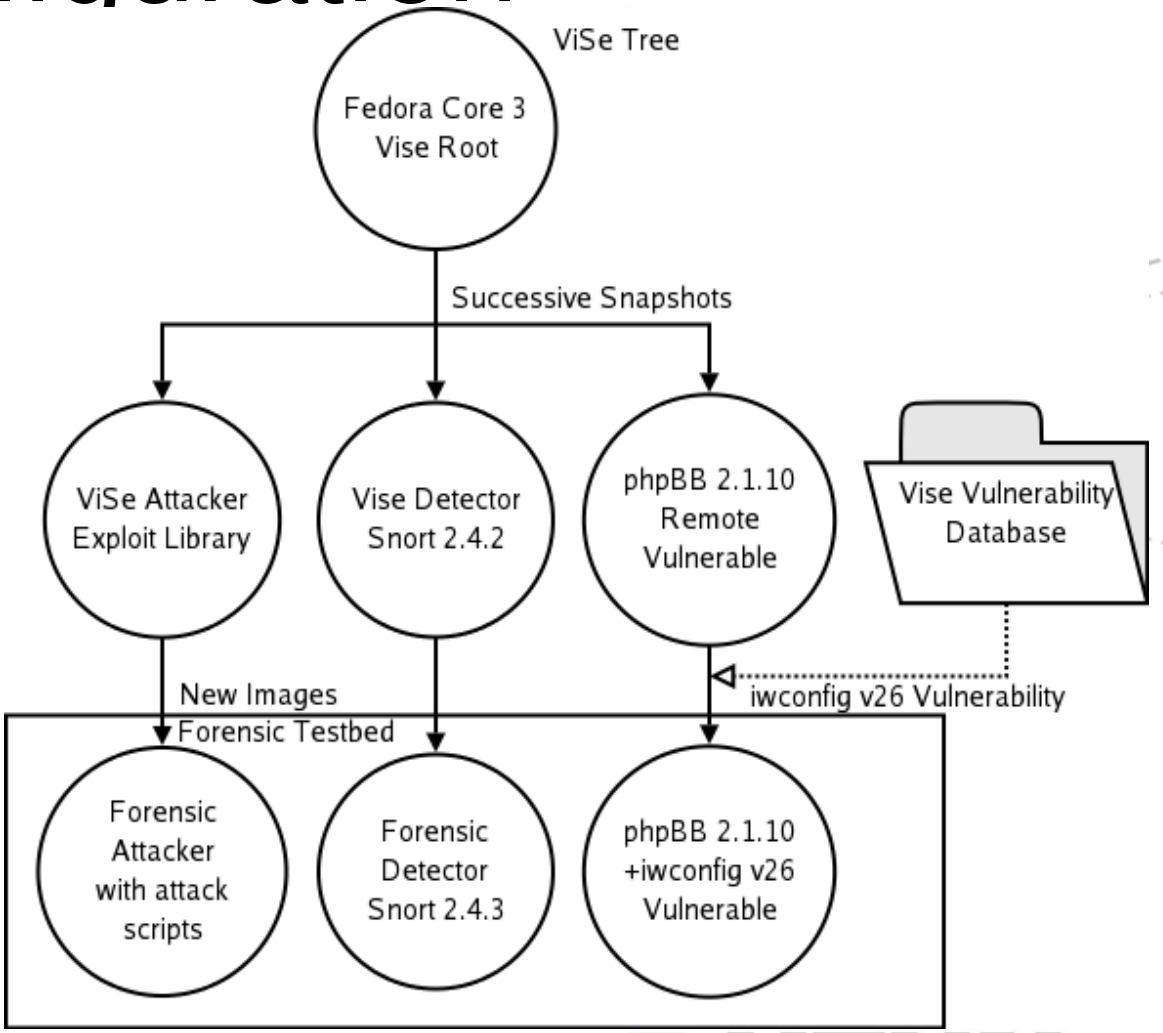
- The Virtual Security Testbed, developed by Mike Richmond at UCSB.
- Virtualization with VMware
- Resource and time savings through the use of VMware snapshots.
- 80GB for 70 system configurations based on 10 OSs.
- Setup: Digital crime scene, analysis host



NTNU
Innovation and Creativity

Example Configuration

- ViSe contains a tree of successive changes derived from base systems.
- Each configuration is saved using the VMware snapshot feature.



NTNU
Innovation and Creativity

ViSe Integrity Issues

- Data contamination between the host and guest operating system.
- Virtual networks should be disconnected from physical networks during testing.
- Shared folders should be disabled during testing.
- Virtualized environment may differ from physical – this may be fingerprinted by intelligent tools and exploited.

NTNU
Innovation and Creativity

Forensic Analysis Image

- The purpose is to acquire and verify images of the different snapshots.
- Both hard drives and RAM can be imaged.
- The tools used are **dcfldd** and **md5sum**.
- The VMware files are proprietary, but we only care about the virtual file system that is contained within the VMware files.

NTNU
Innovation and Creativity

Example – Multistep Attack

"An attack host running Fedora Core 3 has launched and completed a multi-step attack against the victim host running Fedora Core 3. The multi-step attack consists of an Nmap scan (e1), an exploit of the phpBB 2.0.10 viewtopic.php vulnerability (e2), an installation of bindshell on port 12497 named httpd (e3), an exploit of a vulnerable iwconfig buffer overflow vulnerability (e4), the creation of a non-root user and root backdoor (e5), and finally the removal of traces (e6)."

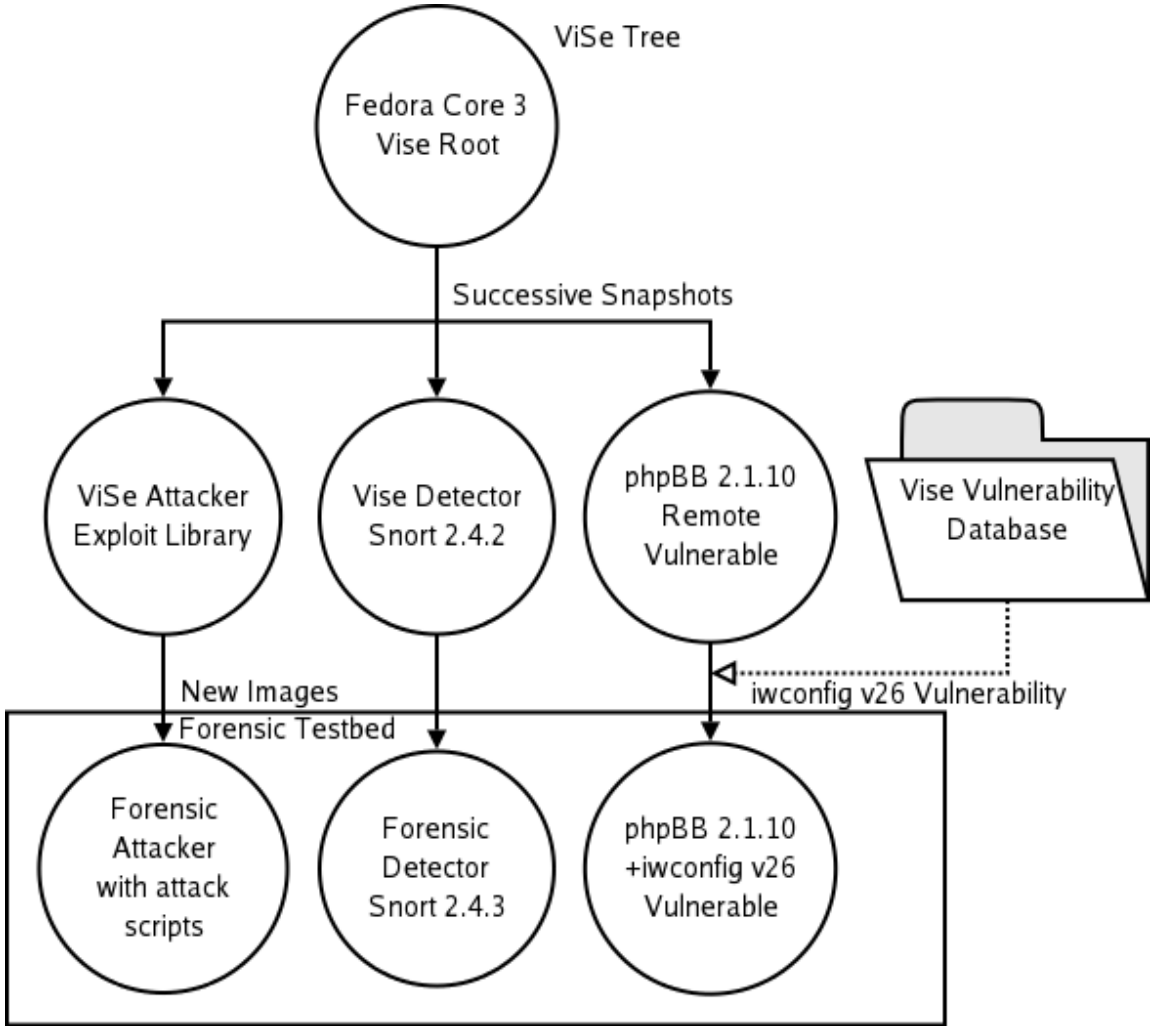
NTNU
Innovation and Creativity

Example – Multistep Attack

1. Network scan
2. Attacker exploits phpBB 2.0.10 viewtopic.php
3. Attacker retrieves a bindshell using wget
4. Attacker discovers vulnerable version of iwconfig
5. Attacker creates a user and retrieves a backdoor
6. Attacker becomes root

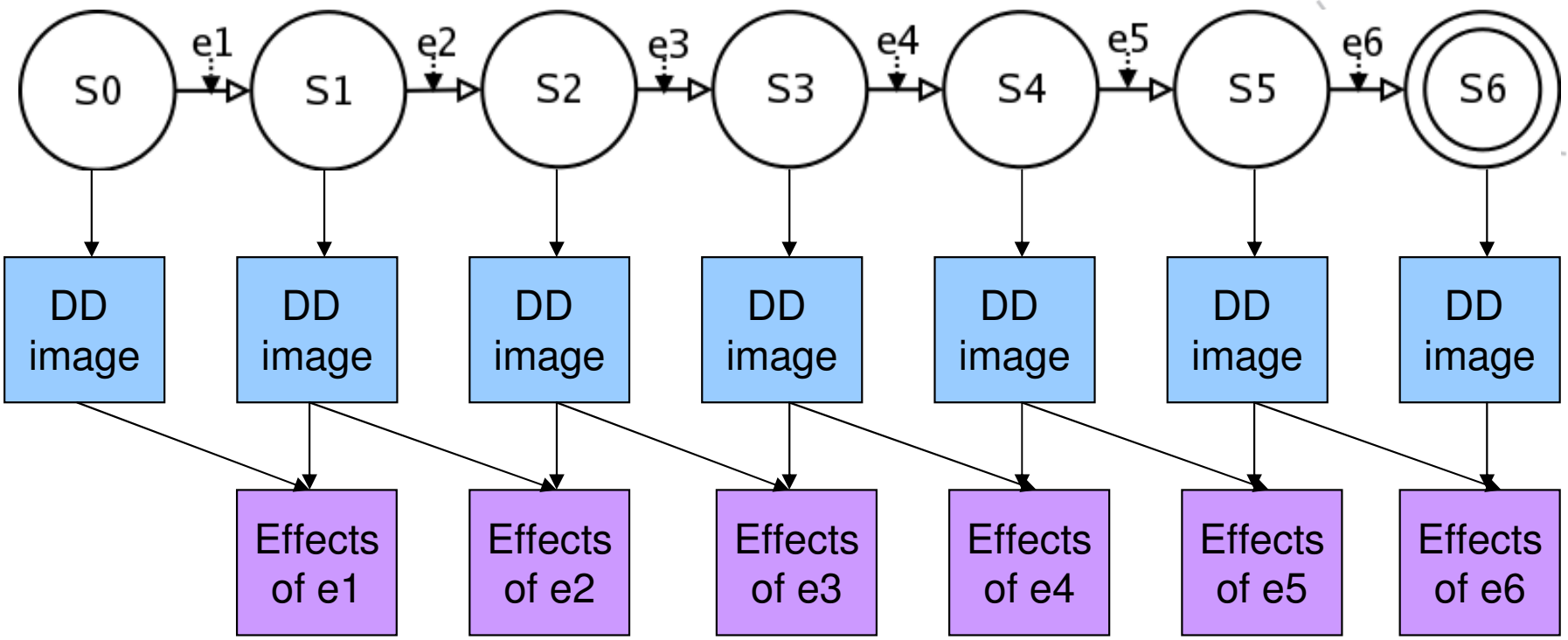
NTNU
Innovation and Creativity

Example -- Configuration



NTNU
Innovation and Creativity

Example – Event Chain



NTNU
Innovation and Creativity

Example -- Effects of Event 1

Host	Evidence Type	Name	Action
Vulnerable	File	/var/log/messages	M
Vulnerable	File	/var/log/httpd/access_log	M
Vulnerable	File	/var/log/secure	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_sessions.MYI	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_sessions.MYD	M
Vulnerable	File	/etc/cups/certs/0	M
Third-party	File	/var/log/snort/snort.log.*	C
Vulnerable	IDS	(portscan) TCP Portsweep: Attacker	C
Third-party	IDS	(portscan) TCP Portscan: Attacker to Victim	C
Third-party	Network	GET /phpBB2/ HTTP/1.1: Attacker to Victim:80	C

NTNU
Innovation and Creativity

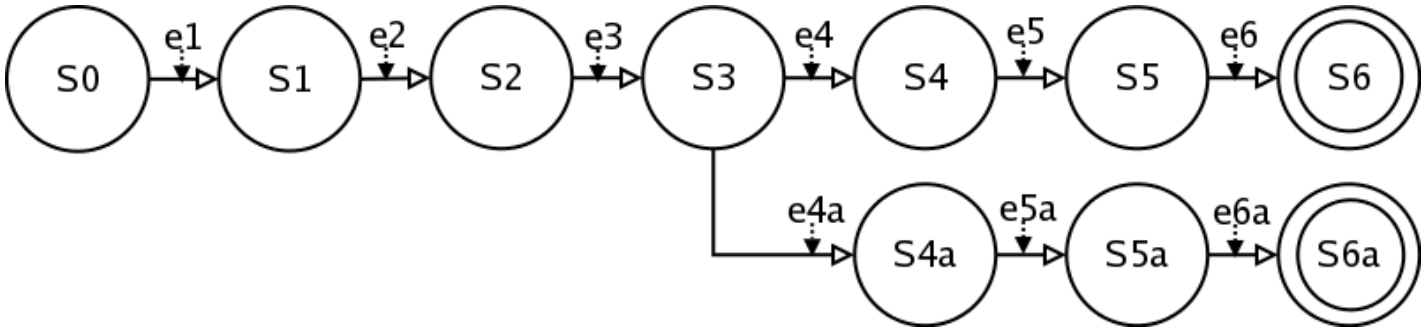
Example -- Effects of Event 2

Host	Evidence Type	Name	Action
Vulnerable	File	/var/log/httpd/error_log	M
Vulnerable	File	/var/log/httpd/access_log	M
Vulnerable	File	/var/log/secure	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_sessions.MYI	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_sessions.MYD	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_topics.MYI	M
Vulnerable	File	/var/lib/mysql/mysql/phpbb_topics.MYD	M
Vulnerable	File	/etc/cups/certs/0	M
Third-party	IDS	WEB-PHP viewtopic.php access: Attacker to Victim:80	C
Third-party	IDS	(http inspect) DOUBLE DECODING ATTACK: Attacker to victim:80	C
Third-party	Network	TCP Connection established: Attacker to Victim: 4321	C
Third-party	IDS	ATTACK-RESPONSES id check returned userid: Victim: 4321 to Attacker	C

NTNU
Innovation and Creativity

Example – alternative hypothesis

- *"An attack host running Fedora Core 3 has launched and completed a multi-step attack against the victim host running Fedora Core 3. The multi-step attack consists of an Nmap scan (e1), an exploit of the phpBB 2.0.10 viewtopic.php vulnerability (e2), an installation of bindshell on port 12497 named httpd (e3), an exploit of the cdrecord environment variable privilege escalation vulnerability (e4a), the creation of a non-root user and root backdoor (e5a), and finally the removal of traces (e6a)."*



NTNU
Innovation and Creativity

Discussion

- Presentation in court
  - Support interpretation of digital evidence
  - Explain discrepancies
- Timing and complexity issues
  - Some attacs are nondeterministic
  - Large number of hosts involved
- Performance issues
  - Snapshots are efficiently saved and restored
  - Forensic analysis can be perfmormed outside ViSe for performance reasons

	Pentium 4	VMware
Boot time	1m9s	2m
Reboot time	1m22s	2m20s
Take snapshot	NA	8s
Restore state	NA	9s
Clone full image (7,6GB)	NA	8m6s
Copy partition image (dcfldd)	11m21s	48m46s
Hash all files in image (sha256deep)	3m56s	26m38s
Extract all strings from image (strings)	6m57s	118m47s

NTNU
Innovation and Creativity

Conclusions

- Efficient event reconstruction
- Reusable snapshots
- Focus on forensic analysis
- Supports or refutes hypotheses in court

NTNU
Innovation and Creativity

Open Research Issues

- Time aspects of attacks, manipulated timestamps, etc.
- Anti-forensics issues with VMware.
- Embedded systems – testing attack tools in mobile environments.
- Worm attacks and testing whether worms could have caused a particular attack.

NTNU
Innovation and Creativity

Questions ?

NTNU
Innovation and Creativity

Digital Event Reconstruction

Digital event reconstruction in five steps [Carrier 2004]:

1. Evidence examination
2. Role classification
3. Event contruction and testing
4. Event sequencing
5. Hypothesis testing

NTNU
Innovation and Creativity