

# Remote Intrusion Detection

Mario Sutton  
Fayetteville State University  
Research Alliance in Math and Science  
[info.ornl.gov/sites/rams2012/m\\_sutton](http://info.ornl.gov/sites/rams2012/m_sutton)

Stacy Prowell, Ph.D.  
Oak Ridge National Laboratory  
Cyber Warfare and Research Team  
Computational Sciences and Engineering

## Motivation

Securing United States cyber infrastructure is critical

Everyone has access to infrastructure

- Individual / personal
- Institutions
  - Public
  - Private
- Hackers attack infrastructure
  - Steal
  - Damage
  - Destroy
- Remote Intrusion Detection (RID) can be advantageous

## Objectives

- Observe rootkits effect on computer performance
- Identify RID techniques
- Implement techniques in virtual environment

## Resources

- D400 Fedora Core 11 Virtual Machine
- Oracle Virtualbox
- Intel Pentium 4 HT processor
- Rootkit

## Installation and Implementation



Figure 1. Screenshot of Virtualbox virtual machine setup on host machine



Figure 2. Zoom in of login screen of Fedora Core used as virtual test environment

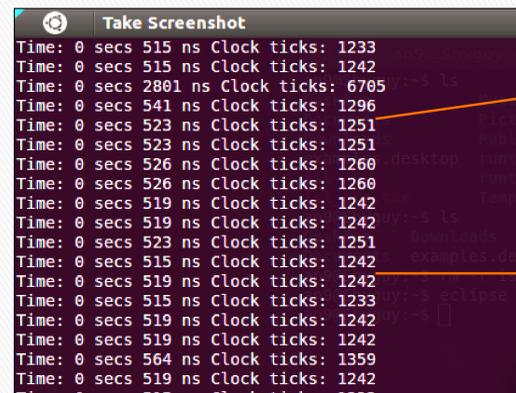


Figure 3. Screenshot of execution time gathering

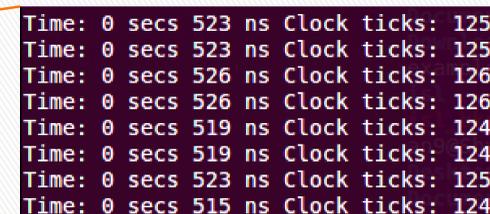


Figure 4. Zoom in of timing information in seconds, nanoseconds, and clock ticks

- Created execution time collection code
- Performed initial timing tests
- Identified Linux rootkits relevant to D400 device
- Identified system calls targeted most by Linux rootkits

Blunden, Bill (2009). *The Rootkit Arsenal, Escape and Evasion in the Dark Corners of the System*. Plano: Wordware Publishing

Medley, D. P. (2007). *Virtualization Technology Applied to Rootkit Defense*. Wright-Patterson Air Force Base, Ohio.

Retrieved August 3, 2012 from [www.dtic.mil/dtic/tr/fulltext/u2/a469494.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/a469494.pdf)

Levine, J. G. (2004). *A Methodology of Detecting and Classifying Rootkit Exploits*. Georgia Institute of Technology.

Retrieved August 3, 2012 from [smartech.gatech.edu/jspui/.../1853/.../john\\_g\\_levine\\_200405\\_phd.pdf](http://smartech.gatech.edu/jspui/.../1853/.../john_g_levine_200405_phd.pdf)

## Conclusion

- Continuing research needed
- Successfully conducted initial timing tests on clean machine
- Baseline execution time can be established
- Gathered data can be used for later comparisons against compromised machines