The San Francisco Chapter of ISACA proudly presents...
SF ISACA 2007 Fall Conference
IT Audit
Information Security
IT Governance
Risk Management
Compliance

How to Protect from Malicious Code – Using Honeynet and Darknet Technology as Part of a Compliance Program

Michael Smith, PMP, CISSP
Senior Manager, Symantec

April 16, 2007

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Learning Objectives

- Define the importance of Configuration Management (CM) and sound engineering practices to security
- Understand the ways that honey net technologies could be valuable to your organization and how they can be a part of a greater compliance solution
- Know how to detect possible malicious code on your network
- Know what to do if you discover malicious code on your network

Why Focus On Untargeted Malicious Code

- Volume of Threats
  - Symantec documented 4,775 new vulnerabilities in 2006.
  - 8,258 new Win32 variants were reported to Symantec in the last half of 2006.
- Likelihood of Occurrence
  - Hard to say for a particular organization, but the nature of the problem is that it only takes once.
  - Symantec observed an average of 63,912 active bot-infected computers per day during the second half of 2006
- Possible Damage
  - Direct Costs
    - Lost revenue, Cost to remediate
  - Indirect Costs
    - Exposure of Personally Identifiable Information (PII), Negative Publicity

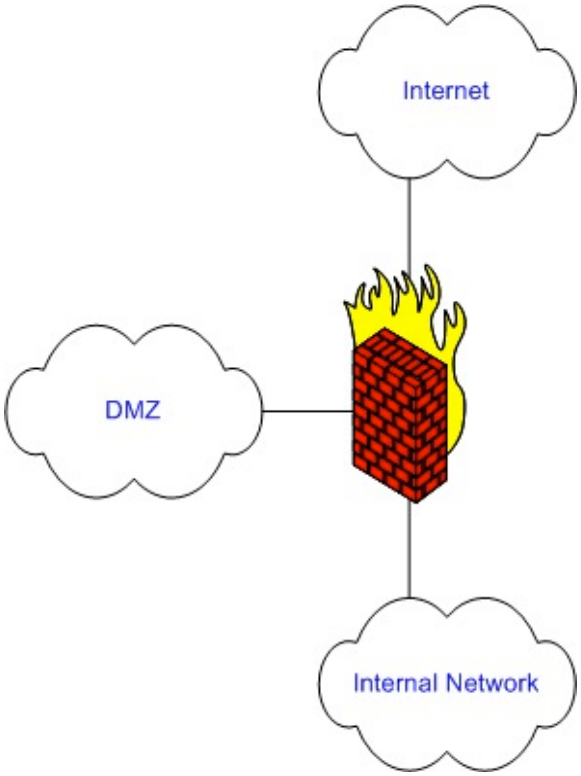
Why Focus On Untargeted Malicious Code

- Secure operations principals that assist in protecting against “crimes of opportunity” help protect against other threats
- Protecting against untargeted threats is a prerequisite to protecting against targeted/advanced threats
- Because the threats are known, there are more obvious data that can be gathered relating to performance of efforts to defend

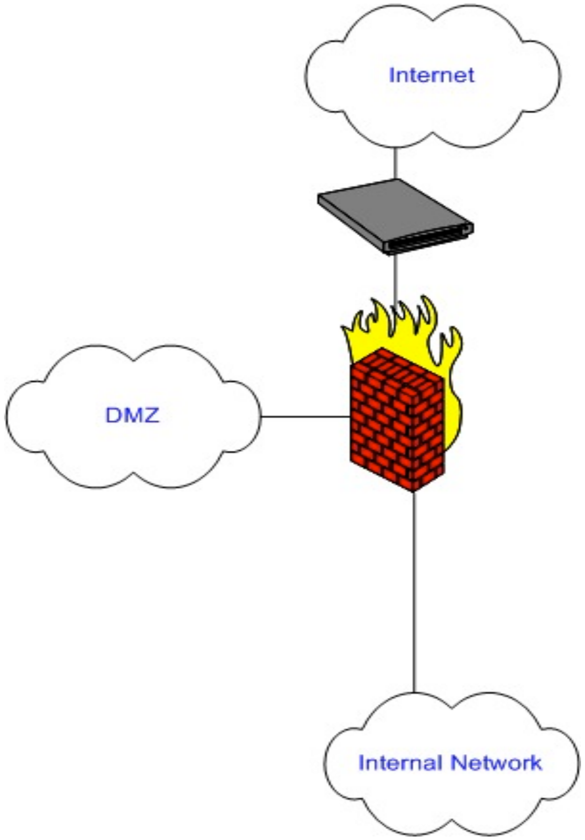
Prerequisites: Network

- Design Basics
  - Internal
  - DMZ
  - External
- Security Devices
  - Firewall
  - IDS/IPS
- How do we verify that a network is secure?
  - Verify Controls
  - Log Review
  - Is there such a thing as provable security?

Network: Design Basics

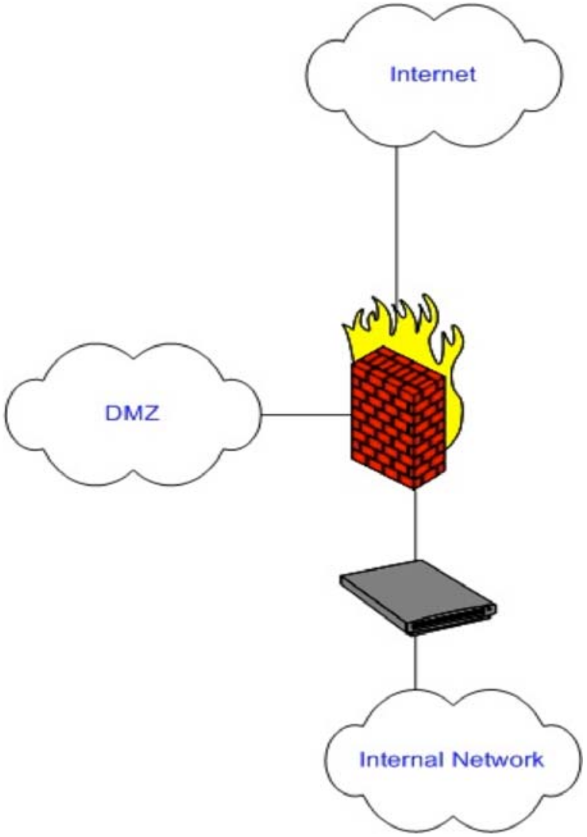


Network: Security Devices



- What are the advantages of placing an IDS/IPS outside of the firewall?
- What are the disadvantages?

Network: Security Devices



- What are the advantages of placing an IDS/IPS inside of the firewall?
- What are the disadvantages?
- What are the implications of switch configurations on internal visibility?

Network: Verification

- Verify Controls
  - Is the firewall configured properly? Has it always been configured properly?
  - Are network devices functioning as expected?
- Log Review
  - Can you review all logs?
  - Which ones do you review?
- Is there such a thing as provably secure?
  - PSOS
  - Covert Channels

Network: System

- Change Management/Patch Management
  - It all starts with Asset Management
  - What is your organizations' approach to change control? Is it considered a prerequisite for security?
- Security Software
  - Personal Firewall
  - Anti Virus
  - Application Proxies
- How do we verify that a system is secure?
  - Verify Controls
  - Log review
  - Can we prove that a system is secure?

System: Verification

- Verify Controls
  - Host Firewall
  - Host Antivirus
  - OS configuration and user level security
- Log Review
  - Can you review all logs?
  - Which ones do you review?
- Is there such a thing as provably secure?
  - PSOS
  - Covert Channels

Checkpoint

✓ Why Focus On Untargeted Malicious Code

✓ Prerequisites

- Tools For Alerting and Responding
- Summary
- Learning Objectives Review

Tools For Alerting: Traditional

- AV Software
- Firewall Logs
- IDS/IPS Logs
- Router Logs
- Email Gateway Logs
- User notices denial of service (DoS)

  (unfortunately, this is sometimes how we are alerted)

Tools For Alerting: Proposed

- Darknet
  - A Darknet is a portion of routed, allocated IP space in which no active services or servers reside. These are "dark" because there is, *seemingly*, nothing within these networks.
  - A Darknet does in fact include at least one server, designed as a packet vacuum. This server gathers the packets and flows that enter the Darknet, useful for real-time analysis or post-event network forensics.
- Honeynet
  - A Honeynet is a system or group of systems that are intentionally placed on a network advertising services to attract and capture code and actions of attackers (automated malware and/or human adversaries)
  - There is a distinction between low interaction and high interaction honeypots/honeynets that is important to be aware of.

Tools For Alerting: Suggested Advantages

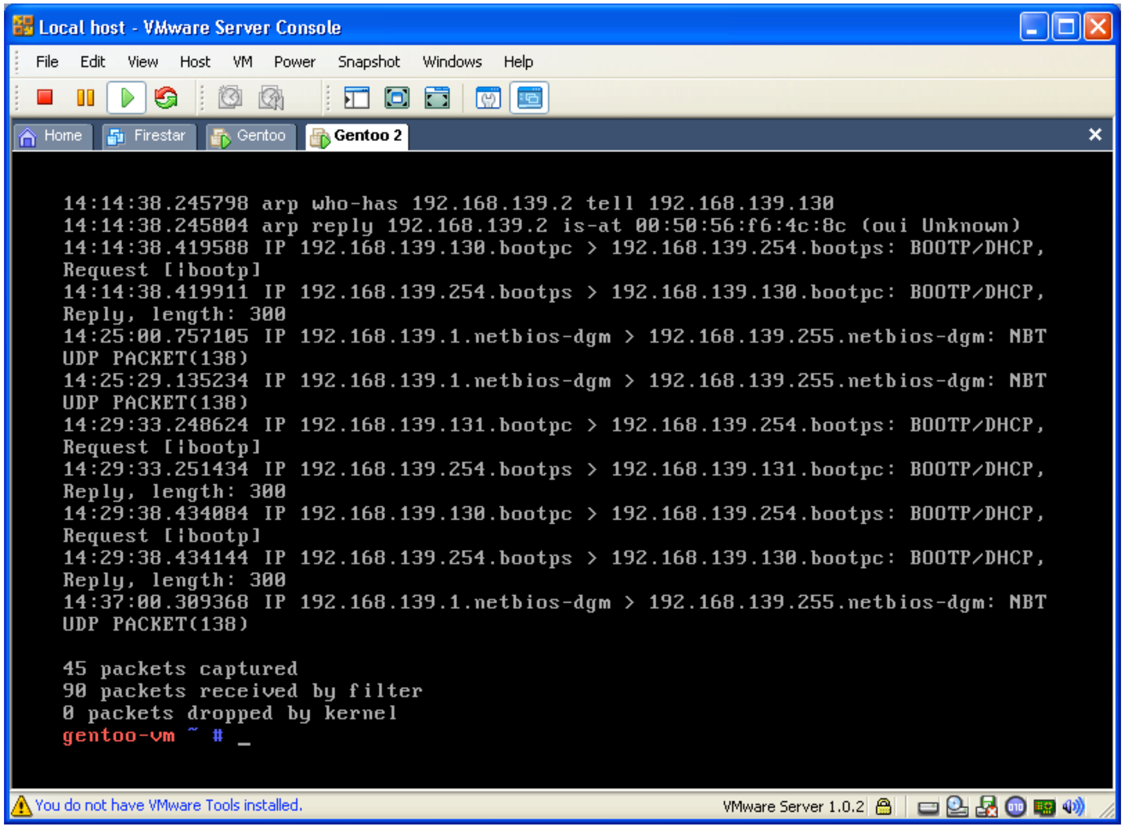
- After tuning there “should” be no false positives
  - No legitimate traffic should be destined for either a darknet or honeynet
  - Can catch misconfigurations as well as secondary indicators of infection
- Serve as a confirmation that other controls are functioning correctly
  - Not 100%, targeted and/or stealth attacks are not covered
  - However, the possibility exists for early warning
  - Also, if placed externally, can help to prove the threat and justify the expense of traditional security measures

Demonstration: Dark Net

- This example is done inside of a virtual environment and therefore there are some artificialities, please suspend disbelief. ;-)
- There are some great resources available on how to setup and use a darknet at the end of this presentation, and I will not try to recreate those here
- I will try to show some examples of some possible quick wins that hopefully you could use in a proof on concept capacity to see if it is worth the investment in time and resources to implement within your environment
- The following slides that are titled “Demonstration: *” attempt to capture the idea of the demonstrations for anyone reading this presentation

Demonstration: Dark Net

- If we just sniff on a given network segment then there will be noise:

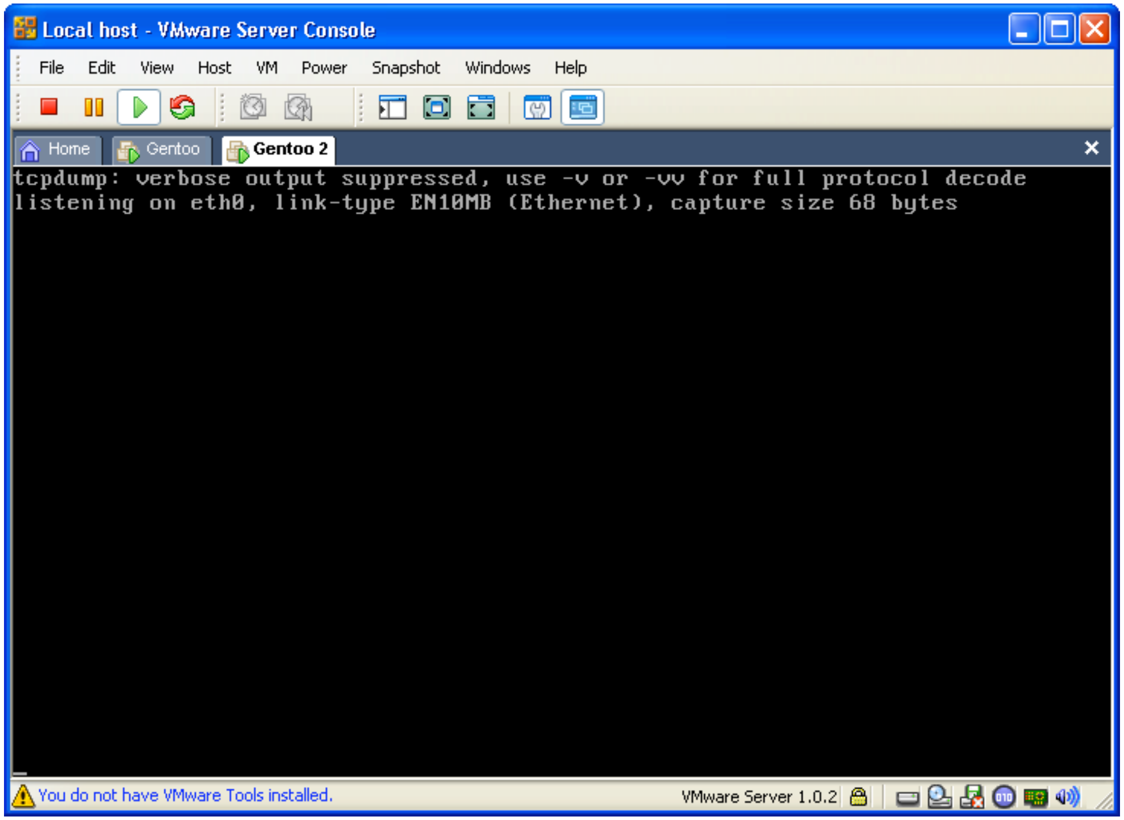


```
14:14:38.245798 arp who-has 192.168.139.2 tell 192.168.139.130
14:14:38.245804 arp reply 192.168.139.2 is-at 00:50:56:f6:4c:8c (oui Unknown)
14:14:38.419588 IP 192.168.139.130.bootpc > 192.168.139.254.bootps: BOOTP/DHCP,
Request [|bootp]
14:14:38.419911 IP 192.168.139.254.bootps > 192.168.139.130.bootpc: BOOTP/DHCP,
Reply, length: 300
14:25:00.757105 IP 192.168.139.1.netbios-dgm > 192.168.139.255.netbios-dgm: NBT
UDP PACKET(138)
14:25:29.135234 IP 192.168.139.1.netbios-dgm > 192.168.139.255.netbios-dgm: NBT
UDP PACKET(138)
14:29:33.248624 IP 192.168.139.131.bootpc > 192.168.139.254.bootps: BOOTP/DHCP,
Request [|bootp]
14:29:33.251434 IP 192.168.139.254.bootps > 192.168.139.131.bootpc: BOOTP/DHCP,
Reply, length: 300
14:29:38.434084 IP 192.168.139.130.bootpc > 192.168.139.254.bootps: BOOTP/DHCP,
Request [|bootp]
14:29:38.434144 IP 192.168.139.254.bootps > 192.168.139.130.bootpc: BOOTP/DHCP,
Reply, length: 300
14:37:00.309368 IP 192.168.139.1.netbios-dgm > 192.168.139.255.netbios-dgm: NBT
UDP PACKET(138)

45 packets captured
90 packets received by filter
0 packets dropped by kernel
gentoo-vm ~ # _
```

Demonstration: Dark Net

- If we allocate darknet space, there should be no noise:



Local host - VMware Server Console
File Edit View Host VM Power Snapshot Windows Help
Home
Gentoo
Gentoo 2

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
```

You do not have VMware Tools installed.
VMware Server 1.0.2

Demonstration: Dark Net

- If there is no noise, then any traffic that is seen on a darknet is worth investigating
- Some things that you might be able to easily find with this technology are:
  - Misusage of tools (unauthorized vulnerability scan).
  - Misconfigured applications (“noisy” apps might be wasting bandwidth).
  - Unapproved applications (P2P, maybe others?).
  - Malware (worms, bots, etc) (technically these are a subset of unapproved applications).

Demonstration: HoneyNet

- How to quickly setup a nepenthes instance
  - There are other honeynet/honeypot products
  - I chose nepenthes to use as an example, but please examine your choices and use what is best for you
- I will try to show some examples of some possible quick wins that hopefully you could use in a proof on concept capacity to see if it is worth the investment in time and resources to implement within your environment
  - How to capture malware for analysis/contribution to mwcollect
  - How to detect secondary indicators of malware on your network
  - How to detect misconfigured programs

Demonstration: Honey Net
Quick Nepenthes Installation Steps

- Download vmware image from http://www.vmware.com/vmtn/appliances/directory/569 , turn it on and log in as root
  - This is a gentoo image, you are welcome to use whatever you are most familiar with, but I have found this to be the easiest/fastest way to get up and running
- Type: passwd
  - Change the root password ;-)
- Type: ACCEPT_KEYWORDS=“~x86” emerge nepenthes
  - Install nepenthes
- Type: nepenthes &
  - Run it

Demonstration: Honey Net

- If the services that the honey are offering are not legitimate, then nothing should be trying to talk to them
- Some things that you might be able to easily find with this technology are:
  - misusage of tools (unauthorized vulnerability scan)
  - misconfigured applications (“noisy” apps might be wasting bandwidth)
  - unapproved applications (P2P, maybe others?)
  - malware (worms, bots, etc) (technically these are a subset of unapproved applications)
- Similar list, isn’t it?
  - Both Honeynet and Darknet technologies can be used to capture similar information. There are pros and cons to each that make one more appropriate depending on your business needs.

Tools For Responding: Network

- Thumbs (pull the plug)
  - Is this possible technically?
  - Is there policy that defines when this is appropriate?
  - Are there legal implications for doing (or not doing) this?
- Firewall, Router, IPS, Switches
  - (Do you have protocols to deal with the people that control all of these devices?)
  - Have you tested them?
  - If your network is down due to malicious code DoS, how will you get patches distributed?
- Telephone
  - (Can you call your upstream ISP for help?)
  - Can you call your Anti Virus (or any other applicable) vendor?

Tools For Responding: Host

- Toolkit (what needs to be in it to do quick, in the field host analysis and malicious code sample capture? What are _your_ documented processes? They are a part of the toolkit)
- Telephone (Can you call your AV vendor for help to figure out what this is and how to detect/remove it?)

Summary

- Why this is important?
- Alerting – we have to know about it before we can deal with it
- Responding – now that we know, what do we do?
- There is no substitute for Proper Prior Planning (PPP)!
- The most important part of PPP is establishing communication lines and trust with all stakeholders that you will need to engage to detect and respond to malicious code. A part of this is testing/exercising the ability to detect and respond.

Checkpoint

- ✓ Why Focus On Untargeted Malicious Code
- ✓ Prerequisites
- ✓ Tools For Alerting and Responding
- ✓ Summary
- Learning Objectives Review

Learning Objectives Review

- Define the importance of Configuration Management (CM) and sound engineering practices to security
- Understand the ways that honey net technologies could be valuable to your organization and how they can be a part of a greater compliance solution
- Know how to detect possible malicious code on your network
- Know what to do if you discover malicious code on your network

QUESTIONS & ANSWERS

References

- Infrastructure:
  - http://www.vmware.com/
  - http://www.gentoo.org/doc/en/handbook/
- Darknet:
  - http://www.cymru.com/Darknet/
  - http://www.infosectoday.com/Articles/Darknets.htm
- Honeynet:
  - http://nepenthes.mwcollect.org/
  - http://www.honeyd.org/
- Malware/General:
  - http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport
  - http://mwcollect.org/
  - http://offensivecomputing.net/
  - http://www.virustotal.com/en/indexf.html
  - http://www.whitehouse.gov/pcipb/priority_1.pdf