Viruses, Infections, Attacks

A presentation by

Barry Schuetz

Linux Supporters Group Adelaide

Wed 2 Sep 2009

Virusess Infections Attacks

Types of Malicious Code

- How They Attack, Infect and are Fixed
- Beware of Attacks
- Quotes from Rick's paper
- Summary

Some Early Stuff

- Early Viruses
- On Portable Media
- The Early Internet
- Gammima Virus
- Morris Worm 1988

TYPES OF MALICIOUS CODE

- A VIRUS
- A WORM
- TROJANS
- MALWARE
- VECTORS

TYPES OF MALICIOUS CODE

- NON-RESIDENT VIRUS
- RESIDENT VIRUS
- A FAST INFECTOR
- SLOW INFECTOR
- VIRUS SIGNATURES

TYPES OF MALICIOUS CODE

- ENCRYPTION WITH A VARIABLE KEY
- POLYMORPHIC VIRUS
- THE SIMILE D VIRUS
- METAMORPHIC VIRUS

UNIX-LINUX INFECTIONS

- BLISS 1996
- ADM 1998
- LION 2001
- IPDWORM 2001
- SLAPPER 2002

UNIX-LINUX INFECTIONS

- SSHD 2001
- SORSO 2003
- LUPPER 2005
- J BELLS (J BELLZ) 2003
- OTHERS

BEWARE OF ATTACKS

- ATTACKERS
- VULNERABILITY SCANNER
- PACKET SNIFFER
- SCRIPT KIDDIE
- SOCIAL ENGIN EERING

BEWARE OF ATTACKS

- ARP SPOOFING
- BRIEFLY HOW ARP WORKS
- INTERNAL ATTACKERS
- ARP PACKET
- MAC SPOOFING

BEWARE OF ATTACKS

- ARP WATCH
- ARP GUARD
- HACKERS CATEGORIES
- SPOOFING ATTACK
- KEY LOGGERS/ CLICKJACKERS

INFECTIONS & FURTHER READING

- QUOTES FROM RICK'S PAPER
- NICK PETRELEY
- ERIC RAYMOND
- KARSTEN M. SELF

SUMMARY

- There is more information
- See my handout notes
- Draw your attention to nasties
- Keep your system up-to-date

summary

- Use Firewalls, Anti Virus, and Filters
- Use strong passwords:
- alpha + numeral + other characters
- Keep reading latest info.
- Attend Linux meetings, ask other users
- Be Alert

THE END

“THATS ALL FOLKS”