

Has Your Computer Been Compromised?

Nick Savvides

School of Physics

The University of Melbourne

nicks@ph.unimelb.edu.au



Material To Be Covered.

- How Access is Gained.
 - Common exploits
 - Investigating a Compromise
 - Root Kits
 - Hidden Files
 - Hidden Processes
 - Password Harvesting
 - Log File Checking
 - Evidence Collection
-
-

How Access Is Gained.

- Motivation.
 - Entertainment (Benign)
 - Proof of Skill
 - Merit
 - Commercial (Malicious)
 - Random (DDOS)
 - Targeted (Espionage, Blackmail)
 - Vengeance (Malicious)
 - Opportunistic
 - Kids
 - Automated
-
-

How Is Access Gained.

- Local Exploits
 - Require authenticated access on host.
 - Make use of local system service exploits.
 - Escalation of privileges.
 - Shell, kernel and other privileged applications.
 - Fool local user run exploit.
 - Remote Exploits
 - Do not require authenticated access.
 - Make use of network services.
 - Commonly buffer overruns.
 - Mail, SMB, UPNP, RPC,
-
-