Phases of a computer attack assignment

Reconnaissance uses a variety of sources to learn as much as possible about the target business and how it operates, including ; Internet searches ; Dumpster diving Domain name management/search services Non-intrusive network scanning Social engineering Phase 2 – Scanning Once you have enough Information to understand how the target works and what information of value might be available, you begin the process of scanning perimeter and internal network devices looking for weaknesses, including ; Open ports

Open services Make and model of each piece of LILLIAN equipment Vulnerable applications, Including operating systems Weak protection of data In transit Phase 3 – Gaining Access Gaining access to resources is the whole point off modern-day attack. The usual goal is to either extract information of value to you or use the network as a launch site for attacks against other targets. In either situation, you must gain some level of access to one or more network devices. Phase 4 – Maintaining Access Having gained access, you must maintain access long enough to accomplish your objectives.

Although you have reached this phase has successfully circumvented their security controls, this phase can increase your vulnerability to detection. Phase 5 – Covering Tracks After achieving your objectives, you typically takes steps to hide the Intrusion and possible controls left behind for future visits. Again, In Dalton to anta-mallard, personal firewalls, and host-based PIPS solutions, deny business users local administrator access to desktops. Alert on any unusual activity, any activity not expected based on your knowledge of how the business works.

To make this work, he security and network teams must have at least as much knowledge of the network as the attacker has obtained during the attack process. Unit 9 Assignment 1 Once you have enough information to understand how the target works and what Vulnerable applications, including operating systems Weak protection of data in transit Gaining access to resources is the whole point of a modern-day attack. The usual After achieving your objectives, you typically takes steps to hide the intrusion and possible controls left behind for future visits. Again, in addition to anti-mallard,