A28438 No calculator permitted in this examination

**THE UNIVERSITY OF BIRMINGHAM**

**THIS PAGE TO BE REPLACED BY OFFICE**

06 23900

**Network Security**

June 2016 1 hour 30 minutes

[Answer ALL questions]

1. In the context of network security, a "zero day exploit" is a previously unknown flaw in a piece of software which allows an attacker to penetrate or otherwise interfere with the correct operation of a system.

   (a) Describe two techniques which will reduce the risk that a zero-day attack is successful against a network you control. **[8%]**

   (b) Describe the process you would follow to audit a network in order to check that the risk of a zero-day exploit had been minimised. **[8%]**

   (c) What records would you keep as part of this audit in order to provide evidence that the audit had been performed adequately? **[4%]**

2. Most firewalls today are *stateful*, otherwise known as *connection tracking*. These share some technology with *Network Address Translation* systems.

   (a) Describe how a stateful firewall would deal with outgoing UDP packets for which responses might be expected. **[6%]**

   (b) DNS can be subject to a "Kaminsky attack". Describe briefly what this attack involves. **[8%]**

   (c) What mitigation is commonly used to extend the size of the attackers' search space when they attempt a Kaminsky attack? Why is this mitigation effective? **[4%]**

   (d) Why does this potentially not work correctly when placed behind a network address translation boundary? **[8%]**

3. An *intrusion detection systems* (IDS) examines network activity and attempts to identify attacks. An *intrusion prevention system* (IPS) takes active counter-measures when such an attack is detected.

   (a) Describe two techniques that an IDS can use to identify traffic that is suspicious. Compare their strengths and weaknesses with reference to attacks that one technique might detect that the other will not. **[12%]**

   (b) Why does the increasing use of encryption make IDS and IPS installations less useful? What types of behaviour might still be checked by an IDS on a heavily encrypted network? **[8%]**

4. It is often implied that it is easy to intercept data in motion on wired networks.

   (a) Explain why the move from "hubs" to "switches" as the most common form of network hardware has made some interception harder. **[4%]**

   (b) There are a variety of active attacks on switches which permit the interception of traffic destined for other network nodes. Explain two of them. **[8%]**

   (c) What two mechanisms could an administrator use to reduce the effectiveness of these attacks? **[8%]**

(d) What technology would you use to make interception near-useless to the attacker? **[2%]**

5. A *virtual private network* (VPN) can be used to connect a remote user to a corporate network.

   (a) VPNs are often secured with *one time passwords* linked to some sort of hardware token. How can a simple GSM mobile phone be used to provide one-time passwords? **[2%]**

   (b) What part of the GSM mobile phone would have to be compromised in order to defeat this scheme? **[2%]**

   (c) How might a more sophisticated "Smart Phone" be used, which would work even in the absence of a mobile phone signal or WiFi connectivity? Explain the algorithms you propose. **[8%]**