Five steps of a hacking attack essay sample

Business, Company

1. Reconnaissance , Scanning, Gaining Access, Maintaining Access , Covering Tracks

2. During the reconnaissance step of the attack, describe what task Zenmap GUI performs to do passive OS fingerprinting. Nmap uses the –O option to perform OS fingerprinting. The process monitors and captures network traffic. The traffic is then analyzed for patterns that would suggest which operating systems are in use. 3. What step in the hacking attack process uses Zenmap GUI? Scanning

4. What step in the hacking attack process identifies known vulnerabilities and exploits? Vulnerabilities and exploits are identified by enumeration, which is the most aggressive of the scanning stage.

5. During the scanning step of the hacking attack process, you identified known software vulnerabilities in a Windows XP Professional Workstation. List the name and number of the critical Microsoft® vulnerabilities identified. What is vulnerability “ MS08-067”? MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) MS03-043: Buffer Overrun in Messenger Service (828035)

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) MS03-039: Microsoft RPC Interface Buffer Overrun (824146) MS04-011: Security Update for Microsoft Windows (835732) MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION Packet Remote Overflow DoS (326830) MS05-007:

Vulnerability in Windows Could Allow Information Disclosure (888302) Vulnerability MS08-067 is an exposure in Server Service that could allow remote code execution in an affected system. The operating systems affected are Microsoft Windows 2000, Windows XP, and Windows Server 2003.

6. Which tool and application were used to exploit the identified vulnerability on the targeted Microsoft® Windows 2003 XP server? Backtrack4, Metaspolit Exploitation Framework

7. What do If you were a member of a security penetration testing team, and you identified vulnerabilities and exploits, should you obtain written permission from the owners prior to compromising and exploiting the known vulnerability? Once you've identified the vulnerabilities and exploits you should always get written permission before actually hacking into the system.

8. What does the tool Ettercap do?

Ettercap features sniffing of live connections, content filtering on the fly. It is able to perform attacks against the ARP protocol by positioning itself as " man in the middle" and, once positioned as this, it is able to alter data in a connection, discover passwords, and provide fake SSL certificates.

9. The most important step in the five-step hacking process is step 5, where the security practitioner must remediate the vulnerability and eliminate the exploit. What is the name and number of the Microsoft® Security Bulletin? Microsoft Security Bulletin MS08-067 – Critical

10. What is the name of the Microsoft® Windows 2003 XP server Security Patch needed to remediate this software vulnerability and exploit? Security Update for Windows XP (KB958644)