

Name: _____ Date: _____

Northampton Community College
CISC271 – CCNA 3 & 4 – WANs and Security
Chapter 4 - Study Guide

1. What is a brute-force attack?

2. What is a DMZ?

3. What is a DoS attack?

4. What is a computer virus?

5. What is a security password policy?

6. What is an IDS? How is it used in a network?

7. What are the primary objectives of a security policy?

8. What are the characteristics of a good security policy?

9. What risk does a DNS service introduce on a network?

10. What are some risks associated with SNMP?

11. How does Cisco auto-secure minimize risks?

12. Why would you set privilege levels for users that can log into routers?

13. Identify the parts of the IOS image: **c2801-ipk9-mz.124-19.bin**

14. When upgrading to a new IOS, what should be verified prior to beginning the tftp transfer?

15. Describe the password recovery procedure for a Cisco router.

16. What is Cisco SDM?

17. What is “phishing” and how would you defend against it?

18. What is a security audit?

19. Why is it recommended to configure authentication for routing protocols?

20. What is the command sequence for configuring authentication for OSPF?
(include the prompts!)