**CS591 F2010 Final**

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**You have 2 hours and 30 minutes until 7pm to turn in your exam.
This is open book, open note, with internet access to online material.
But you cannot chat with others or send requests to a person for help.
Email me a copy of your answers before you leave and make sure I have received it**.

To save your time, you can copy and paste answers from power point presentations, search engine results, and online material.

1. Firewall
	1. MASQUERADE. Use the secure site of hw5 as an example.
		1. How MASQUERADE is used?
		Ans:
		2. Give an example of iptables command for setting up MASQUERADE.
		Ans:
		3. MASQUERADE operation.
			1. When the http request of the xpup intranet machine (with source IP address 10.0.212.2, port number 3000) was received by fwout, what action will be performed on the packet based MASQUERADE function?
			Ans:
			2. What is the source IP address and port number of the http request will be sent by fwout for the above http request to the web server on the internet?
			Ans:
			3. http requests from DMZ web server or intranet are processed through the FORWARD chain and http requests from fwout itself are processed through the OUTPUT chain. Do we need to specify two separate iptables commands with MASQUERADE operation for these two different streams of packets? Explain.
			Ans:
	2. DNAT.
		1. How DNAT is used?
		Ans:
		2. Is it applied in PREROUTING or POSTROUTING?
		Ans:
	3. A web site uses cgi-scripts on a DMZ web server to save the purchasing/credit card information filled by the customer. The purchasing/credit card information is then transferred back to the intranet database server for processing. Unfortunately *(or we should say inconveniently for the designer)* the security policy of the inner firewall prohibits the DMZ web server from initiating a connection to the intranet. We need to let intranet database server periodically pull the credit card files in. Here we assume the hacker can only read the directory for the purchasing/credit card info but not changing the cgi-scripts.
		1. One security engineer proposes to use AES to encrypt the credit card info as a file before the data is transferred back by the intranet database server for processing. What is wrong with the design?
		Ans:
		2. Someone suggest other type of encryption scheme will work. Please name the scheme and describe how and why it will work even when the hacker is scanning the directory continuously.
		Ans:
		3. Assume now the hacker can read the main memory content from a different account. Will the above scheme still work? Can you prevent the plain credit card info in the memory from being snatched?
		Ans:
		4. Assume now the hacker can overwrite files including the scripts. Will the above scheme work? How do you detect that? Hint: One type of IDS system can help you detect that.
		Ans:
		5. Once detects that your web server is compromised, we need to bring back another fresh copy of the server image. How do you ensure the fresh copy of the server image is not modified by the hacker?
		Ans:
2. IDS
	1. How can zero-day worm be detected? Briefly discuss one technique.
	Ans:
	2. If a hacker changes the content of the TFN DDoS attack msg from "1234" to "blast", what will be the new snort rule to be added?
	Ans:
	3. The above scenario indicates the problem with IDS detection based on specific patterns.
		1. If the attacker changes the content again, the existing rules will produce false \_\_\_\_\_\_\_. (Fill in the blank).
		2. One security engineering suggests change the attribute “Content:blast” to “Content: \*” a wildcard pattern that match. This new snort rule will produce way to many false \_\_\_\_\_. (Fill in the blank).
		3. What is your solution to this? Hint. We discuss a paper using this approach for detecting zero day worm.
		Ans:
	4. What are the rule optons in SNORT that can improve the efficiency of the intrusion detection process? List two. Briefly discuss why.
	Ans:
	5. Explain how the honeypot can be used to reduce the false positives.
	Ans:
	6. New iptables feature allows the match of a string and thus can be used to implement snort IDS rule.
	For example,
	alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS (msg: “WEB-ATTACKS nmap command attempt”; flow:to\_server, established; content:”nmap%20”; nocase; classtype:web-application-attack; sid:1361; rev:5;)
	can be implemented as
	$IPTABLES –A FWSNORT –p tcp - - dport 80 –m string –string “nmap%20” –algo bm –m comment – comment “WEB-ATTACKS nmap command attempt; classtype:web-application-attack; sid:1361; rev:5; FWS:1.0;” –j LOG –log-ip-options –log-tcp-options –log-prefix “[20] SID1361 ESTAB “
		1. What is the advantage on implementing IDS rule as an iptables command?
		2. What will be the iptables command for the following SNORT Rule:

		Alert tcp any any -> 192.168.1.0/24 143 (content: “|90CB C0FF FFFF|/bin/sh”; msg: “IMAP buffer overflow!”)