CS458 - Assignment 2

Name: Lawson Fulton
UserId: ljfulton
Student#: 20381453

Written Answers

1. a) Alice can read documents D102, D104, and D105. She can write to documents D101, and D104.

b) Begin: Alice (Secret, {CIA, FBI})

	Action	Level after action
i.	Alice writes to D105:	Alice (Secret, {CIA, FBI}), D105 (Unclassified, {CIA})
ii.	Alice writes to D104:	Alice (Secret, {CIA, FBI}), D104 (Secret, {CIA, FBI})
iii.	Alice reads from D103:	Alice (Classified, {CIA, FBI}), D103 (Classified, {CIA, NSA, FBI})
iv.	Alice writes to D102:	Alice (Classified, {CIA, FBI}), D102 (Classified, {FBI})
v.	Alice writes to D101:	Alice (Classified, {CIA, FBI}), D101 (Classified, {CIA, FBI})

2. a) In normal usage the signature looking for the pattern "/..%c0%af../" should have a low false positive rate because legitimate urls have no reason to contain such a pattern. Therefore, the pattern would likely be encountered only in malicious URLs.

b) To get a naive sysadmin to disable the snort signature, an attacker could trigger a bunch of false alarms by sending innocuous requests containing the offending the signature from many unique sources. The sysadmin then might see that the alerts are responding to something innocuous and turn them off. The attacker could hide their IP address by potentially using a bot net that they already have control of.

c) In light of the previous proposal, it indicates that the false positive rates advertised for security software may be inaccurate. It is in general not possible to always distinguish between what alert is related to a real attack, or is flagging non-malicious activity.

d) Modify the attack such that its signature changes. Instead of using a url containing "/..%c0%af../", the attacker could use a url containing "/..%c0%**2**f../" which will also decode to "/../../". Since the signature has changed, snort will not detect the attack.

3. a) If there is only room in the budget for a single firewall, then it should be placed between the internet and all of the company computers, including the webserver and the database. This is to provide protection to the entire company network from the outside, where an attack is most likely to originate.

b) If room in the budget is found for a second firewall, it should be placed between the company desktop computers and the webserver + database subnetwork. This way, the webserver and database are protected from any potential attacks originating from one of the employee computers.

Bypassing the IDS (Bonus)

1. The IDS rules for detecting scans could be abused to frame an innocent system on the LAN if there is a local DNS server (which is common in many company networks). An attacker could send 10 DNS requests in quick succession with unique spoofed source addresses. When the DNS server responds with 10 replies to 10 distinct destinations, it will be flagged by the IDS.
2. The code red worm could avoid detection by my IDS by simply changing a single character in its signature. For example, one could replace the first 'N' in the original signature: "GET./default.ida?NN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a..HTTP/1.0"

With an 'X':

"GET./default.ida?XNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a..HTTP/1.0"

Due to the nature of the buffer overflow, this should still work correctly.