**Description for: CS 492 Homework 7**

Authorization 2

**You must work individually**

1. Firewalls
   1. [12pts] Suppose that incoming packets are encrypted with a symmetric key that only the sender and receiver know. Which type(s) of firewall will work with such packets and which will not? Why?

Packet Filter and Stateful Packet Filter can accept because neither has the capability to analyze the contents. Application Proxy has the ability to determine if the contents of the packet are safe. The other types of firewalls do not. If it can’t make that determination then it wouldn’t be able to penetrate the firewall.

* 1. [13pts] Why are DMZs used by businesses? Explain briefly why they are designed the way they are using example from slides (placement, types of firewalls).

Businesses utilize DMZ’s so that they can experience the best of both worlds. Typically, what business’ do is place the web server, FTP Server, and DNS Server behind a packet-filter firewall so that they can access the internet quickly (not pay much of a price). If there is an attack on the web server, FTP Server, or DNS Server, the downside would be relatively minor compare to if attacks occurred in other portions of the business. To protect the other portions of the business (ie. Financial data), a business would typically arrange the financial data behind another – more restrictive firewall (ie. Application Proxy) for the added protection.

1. Intrusion Detection Systems
   1. [10pts] List the advantages of a signature-based IDS vs. a anomaly-based IDS

- Signature based is much more simple that anomaly based.

- Detect Known attacks (It’s obviously good that it does this but it’s not really effective against unknown attacks)

- Know which attack at time of detection – administrator can quickly determine the legitimacy of the attack & respond appropriately.

- Efficient (assuming there is a reasonable # of signatures but not excessive) –

* 1. [10pts] List the advantages of an anomaly-based IDS vs. a signature-based IDS

- Chance of detecting unknown attacks and signature based only detects know attacks

* 1. Using the last table of file frequencies from the sides:

|  |  |  |  |
| --- | --- | --- | --- |
| H0 | H1 | H2 | H3 |
| .1 | .38 | .364 | .156 |

The new file frequencies are A0=.05, A1=.25,A2=.25,A3=.45

* + 1. [20pts] Is this normal for Alice? (once again assume .1 is the threshold)

S = (H0 – A0)2 + (H1 – A1)2 + (H2 – A2)2 + (H3 – A3)2

S = (0.1 – 0.05)2 + (0.38 – 0.25)2 + (0.364 – 0.25)2 + (0.156 – 0.45)2

S = (0.05)2 + (0.13)2 + (0.114)2 + (-0.294)2

S = (0.0025) + (0.0169) + (0.012996) + (0.086436)

S = 0.118832

0.118832 > 0.1

I conclude that Alice’s recent use is **abnormal**.

* + 1. [20pts] What would the new frequencies be (assume same percentages as slides and update should be made)?

Hn = 0.2An + 0.8Hn

H0 = 0.2(0.05) + 0.8(0.1)

H0 = 0.01 + 0.08

H0 = 0.09

H1 = 0.2(0.25) + 0.8(0.38)

H1 = 0.05 + 0.304

H1 = 0.354

H2 = 0.2(0.25) + 0.8(0.364)

H2 = 0.05 + 0.2912

H2 = 0.3412

H3 = 0.2(0.45) + 0.8(0.156)

H3 = 0.09 + 0.1248

H3 = 0.2148

Updated File Frequencies:

|  |  |  |  |
| --- | --- | --- | --- |
| H0 | H1 | H2 | H3 |
| .09 | .354 | .3412 | .2148 |

* 1. [15pts] Poisoning IDS – If Trudy wanted to poison the IDS so that the system being under an attack was the new “normal” as fast as possible what would they need to do?

**I’m guessing your talking about Trudy.**

Trudy could intentionally modify what “normal” is, as long as she executes it slow enough to make her attack appear to be normal. She can launch her attack full on, and if she stops her attack that should trigger anomaly detection. Her attack would now be considered the “new normal”. By going slowly, Trudy will eventually convince the anomaly detection algorithm its normal for Alice to only access 1 file (ie F3)

The company should incorporate variance. To incorporate variance, the company would need to measure more than 1 statistic and then combine them in a formula. This would allow the company to have a more comprehensive understanding of “normal” behavior. Simlar approaches are NIDES,