CMPSC 443, Homework 5 – Pramod kumar pjk5502

1. (12 pts) Recall that the anomaly-based IDS example presented in the slides is based on file-use statistics. The expected file use percentages (the Hi values in the Table are periodically updated, which can be viewed as a moving average)

   (a) Why is it necessary to update the expected file use percentages? (3pts)
   (b) When we update the expected file use percentages, it creates a potential avenue of attack for Trudy. How and why is this the case? (3 pts)
   (c) Suppose that at the time interval following the results in the second update of the table in the slides, Alice's file use statistics are given by A0=0.05, A1=0.25, A2=0.25, and A3=0.45. Is this normal for Alice? (3pts) Compute the updated values of H0 through H3. (3 pts)

Answer: a) it is updated to consider change in user behaviour over time (or particular time) for example, consider canvas website and file access percentage of user during start of the semester and during the exam. if percentage is not updated then admin will get huge false alarm.

b) Trudy if trudy want to access any specific file, he just has to go slow so that it will be considered for next updationg and shift the file percentage to little higher side. which wont set the alarm.
c)
After second update

H0	H1	H2	H3
.10	.38	.364	.156

(.10-0.05)^2 + (.38-.25)^2 + (.364-0.25)^2 +(0.156-0.45)^2 = 0.0025 + 0.0169 + 0.012996 + 0.086436 = 0.118832 > 0.1
No, it will be abnormal

A0	A1	A2	A3

0.05	0.25	0.25	0.45

New H

H0	H1	H2	H3
0.081	0.323	0.3094	0.13884

2. (8pts) Explain the two types of IDS systems by approaches and list two advantages of one against the other.
   page 296 textbook

Answer:

Two types of IDS systems are -

- Signature based IDS
  - compare with intrusion with known intrusion attacks. uses pattern of known attacks.
  - N failed attempts in M seconds is an indication of an attack. This is also called signature
  - Whenever such signature pattern is recognized, IDS issues a warning. This is signature-based IDS
  - Advantages -
    - Simplicity in design and efficiency
    - Detect know attacks without much compute power(unlike AI inference based)
    - Efficient and detect the attack timely.
    - Another major benefit is that the warning that is issued is specific, since the signature matches a specific attack pattern. With a specific warning, an administrator can quickly determine whether the suspected attack is real or a false alarm and, if it is real, the admin can usually respond appropriately.

- Anomaly based IDS
  - looks for abnormal or unusual behaviour
  - uses statistical methods to define normal behaviour

    Advantages

- High chance of detecting previously unknown attacks,

advantage again one another:
signature can detect only known attacks while anomaly method can do of unknown attacks.
signature based is simple math with mean and variance. while anomaly based is very complex to setup.

signature based attacks can tell exact attack while anomaly based give probability.

anomaly detection evolves adaptively better than signature based but it is more computationally expensive.

3. **(9 pts)** Explain the same origin policy (3pts) and how it is exploited by cross-site scripting (XSS) attacks (6pts).

Answer:

same origin policy detectate that only the creator of the data(cookies or other web resource) can request or access it. example we login to facebook then facebool will create session id and other cookies information in our browser and if we visit other websites then our browser will restrict access by stating SOP rules.
formal definition says that : The same-origin policy is a critical security mechanism that restricts how a document or script loaded from one origin can interact with a resource from another origin. It helps isolate potentially malicious documents, reducing possible attack vectors.

XSS attack work by injecting malicious code into legitimate and trusted website so when user visit trusted website, that code gets executed in the context of user and send the information(or do something) with privilege of current user.
from our previous example: if attacker add comment on a post on Facebook, which has script to send cookies to remote server, then whoever visit that website will end up sending the cookies information to the attacker. it defies SOP security, because to SOP it is correct resource request..

4. **(8 pts)** Explain what is SQL Injection attack and why it can happen? Give an example.

Answer:

SQL Injection is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can also use SQL Injection to add, modify, and delete records in the database.

Example :

Consider an application that lets users log in with a username and password. If a user submits the username ‘use’ and the password ‘passwd’, the application checks the credentials by performing the following SQL query:

SELECT * FROM users WHERE username = 'user' AND password = 'passwd'

If the query returns the details of a user, then the login is successful. Otherwise, it is rejected.

Here, an attacker can log in as any user without a password simply by using the SQL comment sequence -- to remove the password check from the WHERE clause of the query. For example, submitting the username administrator'-- and a blank password results in the following query:

SELECT * FROM users WHERE username = 'administrator'--' AND password = ''

This query returns the user whose username is administrator and successfully logs the attacker in as that user.

5. **(10pts)** Firewall concepts.
   (1) List the tree types of firewalls and describe their differences (e.g., locations in network stack, content they look at)
   (2) Explain why stateful packet filter can prevent TCP ACK scan attack whereas packet filter cannot.

Answer:
3 type of firewall:

1) packet filter :
   a) it is placed at network layer, looks at packet headers, for example it can filter based on :
      i) source and destination ip address
      ii) source and destination port number
      iii) flag bit (for acknowledgement and SYN)

iv) direction of packet,(Egress and ingress)

2) stateful packet filter
    a) works at the Transport layer,
    b) it add state to the packet filter, example it remember ongoing TCP and udp connections

3) application proxy
    a) works at the application layer
    b) it is the midater between server and the client. All TLS/SSL connections terminate on the proxy and proxy will forward the request with new TTL's
    c) this help in avoiding port scanning for internet network.
    d) it inspect application payload completely and generally we have different proxy for each type of service like SMTP, DNS, FTP server.

6. **(15pts)** Understand firewall rules. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a) Describe the effect of each rule.

Anwser:

a) Rule A, allow packet from external to internal address with destination port as 25 and protocol is TCP.

Rule B, allow outgoing packet with destination port > 1023, with source ip is internal and any external ip address. protocol should be TCP

Rule C, allow outgoing packet with destination port 25, with source ip is internal and any external ip address.protocol should be TCP

Rule D, allow incoming packet from external ip to internal ip with destination port more > 1023

Rule E , deny , packet from either side of the firewall to any port and any protocol.

b) Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and

mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are shown:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

192.168.3.4(user) ----------Firewall----------SMTP server(172.16.1.1)
Packet 1: Permit
packet 2: permit
packet 3: permit
packet 4: permit

c) Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

Answer: Rule D will allow indirection connection request and rule B will allow response for the connection. Hence attack will succeed.

7. **(6pts) 10.36 Question** : Suppose That We Modify WEP So That It Encrypts Each Packet Using RC4 With The Key K, Where K Is The Same Key That Is Used For Authentication. A. Is This A Good Idea? Why Or Why Not?

Answer:

No, it's a bad idea. RC4 is a stream cypher, using the same key will lead to vulnerability associated with it. Also, since IV in key is 24 bit and K is same, then K_{iv} will repeat itself. Modified version is much worse as we are not changing K_{iv} at a lot so no need to wait for long as cypher will repeat very quickly and it will exposed to vulnerability like frequency attacks.

8. **(6pts) 10.37 (a, b, c)**

Answer:

a) Probability of one number is $½^{24}$.
Porb of not getting this number is (1- $1/2^{24}$)
Prob of **not getting** after N trial is $(1-1/2^{24})^N$
Prob of **getting** after N trial is when is $1- (1-1/2^{24})^N > ½$

$1 –(16777215/16777216)^N = ½$
$½ = (16777215/16777216)^N$

Solve the N =>
Number of packet per second is 916
So final answer would be = N/916

b) If it's a sequence then we need to observer 2^24 packet which will be 2^24/916 = 18316 seconds => 18316/3600=> 5.0877 hours
c) If key repeats then it will be same as one-time pad used more then once and so vulnerability will inherit.

9. **(8pts)** Suppose an attacker wants to secretly send out the bits "11000111" through a file lock covert channel. Explain how it works.

Answer:

Consider lock as 1 and unlock as 0
Lock lock unlock unlock unlock lock lock lock

How it works?

1) Both sender and receiver share the same shared resources
2) Receiver monitors some global file attributes and sender modifies those attributes to send the message
3) So lock means 1 and unlock means 0

10. **(6pts)** What is a rootkit? Please list at least four types of rootkits .

Answer:

A rootkit is a malicious software that allows an unauthorized user to have privileged access to a computer and to restricted areas of its software. It composed of **dropper**, **loader** and the **rootkit**. A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks
Type is defined based on the how deep it goes in the system

1) Kernel rootkit – root kit boots along with the os
2) Virtual root kit - root kit boot before OS itself
3) Memory rootkit – hide in RAM
4) Application rootkit - Hide in application's.

11. (**6pts) 11.22.**

Question :

Virus writers use encryption, polymorphism, and metamorphism to evade signature detection.

- What are the significant differences between encrypted worms and polymorphic worms?
- What are the significant differences between polymorphic worms and metamorphic worms?

Answer:

Answer :

Encrypted Worms: These *worms* are designed to bypass the detection mechanism of antiviruses.

Polymorphic Worms : These worms constantly change their identifiable features in order to evade detection. Only some part of the malicious software changes in this case

Metamorphic worms : These are rewritten with each iteration so that each succeeding version of the code is different from the preceding one.

a) Encrupted encrypt it to evade and polymorphic evade by changing the signature.
b) Polymorphic write only some part of the code while Metamorphic rewrite whole code.

12. (6pts) The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produced by the metamorphic code.

Original code	Metamorphic Code
Mov eax, 5 Add eax, ebx	Mov eax, 5 Push ecx

Call [eax]	Pop ecx
	Add eax, ebx
	Swap eax, ebx
	Swap ebx, eax
	Call [eax]
	nop

Answer:
as such there is not effect of code change but it modifies the signature of the virus by adding useless instruction.