**Military College of Signals**

**2nd OHT**

**BESE 16 (B)**

**Introduction to Computer Security**

**Faculty Member:** Mian Muhammad Waseem Iqbal **Time: 60** Mins

**Max Marks:** 30

**NOTE:**

1. **Answer the questions on question paper**
2. **Write appropriate answer only in space provided**
3. **Ambiguous answer may leed to cutting of marks**

**Q-1** Explain how public key cryptography can be used for digital signature. (2)

Sol - By using the private key in encryption and the public key as the signature.

**Q-2** a. Many spam filters rely on users to report spam. Once a user has reported an email as spam, the filter tries to learn how to recognize future instances of similar spam. One simple scheme is to remember the “from” addresses of the spam and not allow any future emails from those addresses. How can the spammer dodge this filter? (2)

Spoof the “from” address. (1)

Use a botnet to send the spam so it is coming from millions of different addresses. (1)

b. What is the difference between Vulnerability Assessment and Penetration Testing in terms of goal, cost and role? (3)

goal: determine possible vulnerabilities, exploit vulnerabilities existing in an environment. Cost: Less, More. Role: Act as the Security Admin, Act as the Hacker

c. What is Footprinting? In which situation would it be used? (1)

info gathering, used by a determined hacker targeting a specific company or person.

d. A signature-based IDS at a new site first requires access to logs of the site’s historical activity in order to train the detector. True or False? (1)

false

e. Behavior-based IDS works well for detecting known attacks but do not work well for detecting novel attacks. True or False? (1)

False

f. What component of Kerberos helps mitigate replay attacks?

Authenticator

**Q-3** Consider the following authentication protocol, which uses a classical cryptosystem. Alice generates a random message r, enciphers it with the key k and shares with Bob, and sends the enciphered message {r}k to Bob. Bob deciphers it, adds 1 to r, and sends {r+1}k back to Alice. Alice deciphers the message and compares it with r. If the difference is 1, she knows that her correspondent shares the same key k and is therefore Bob. If not, she assumes that her correspondent does not share the key k and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not? (3)

Yes. Because

a. the key is shared between Alice and Bob only.

b. the number that is sent is random, so the intruder cannot reply or guess the number.

**Q-4** A buffer overflow occurs when more data is copied to a local buffer than it can handle. Review the C code below and determine if the program is vulnerable to buffer overflow or not? Explain (5)

#include <stdio.h>

#include <strings.h>

#define SIZE\_OF\_ARRAY 25

#define SEN "This is a short sentence"

int main(int argc, char \*argv[])

{

char buf[SIZE\_OF\_ARRAY];

if(argc < 2)

{

printf("Usage of the program is: program\_name <parameter>");

}

else

{

strncpy(buf,SEN,size(SEN)-1);

}

return 0;

}

Here, this program is not vulnerable to buffer overflow since you are copying 22 characters (size(SEN)-1) to a buffer of 25 which is completely safe since even if you add \0 with it, you only get 23 characters that can easily fit into the 25 character buffer.

**Q-5** State weather this piece of code is vulnerable to buffer overflow attack or not. If yes then what type of buffer overflow attack is depicted in this code? (5)

#include<stdio.h>

#include<string.h>

int main()

{

char mystring[] = "MCS NUST";

char buffer[8];

strcp(buffer,mystring)

printf("The copied string is %s",buffer)

return 0;

}

This is called the off by one as we discussed. You are copying a string of 8 characters to a buffer of 8 characters. However, you need one additional space for the null terminator \0 that is why it is going to allow buffer overflow.

Q-6 You are the network administrator for a large company. Your company will be held liable for any spooﬁng attacks that originate from within your network. What can you do to prevent spooﬁng attacks by your own employees?

Inspect the source IP address of all outgoing packets. If a packet has an address from outside the range

assigned to your network, block the packet

Q-7 a. What is a certificate authority? Explain a scenario in which they are useful.

A certificate authority is an entity that issues public key certificates -- that is, digitally signed statements asserting that a certain key is the public key of a certain entity.

* A certificate authority is useful if one entity A wishes to reliably ascertain the public key of another, B, say in order to send B a message encrypted with its public key. The entity A can obtain B's public key certificate from a certificate authority that it trusts.
* A certificate authority is useful if, for example, a user A wishes to obtain a secure web session with her bank B.  A's browser software can obtain B's public key certificate from a certificate authority, and thereby be sure that the session really is with B and not with an imposter.

b. Alice receives an email, apparently signed using a PGP private key by Bob. She  
           does not know Bob's public key, but she knows and has signed the public keys of  
           Carol and Dave. Dave has signed the keys of Alice, Bob and Eve. Eve has  
           signed Carol's and Dave's keys. Alice has "complete trust" in Dave, and "part  
           trust" in Carol and Eve. Should Alice accept the signature on Bob's email?  
           Explain your answer, specifying any assumptions you make about PGP.

Alice trusts Dave completely and knows his key. Dave has signed Bob's key, so according to the rules of PGP, Alice should accept the value for Bob's key and use it to verify the signature on his email. If the signature is valid using Bob's public key, then she should accept it.

Q-8 Alice, who often uses her company’s secure mail server, has just lost her private key but still has the

corresponding public key. Answer the following questions both with yes/no and by giving a reason for

each.

1. Is she still able to send encrypted mails? What about receiving?

Yes, she can send encrypted mails, she needs only the public key of the receiver. The receiver

cannot be sure that it was Alice who sent the message, though.

No, she cannot meaningfully receive mails since she cannot decrypt them without her private key.

1. Is she still able to sign the mails she sends? What about verifying the signatures of mails she

receives?

No, she cannot sign her mails, as she needs her private key to do that.

Yes, she can verify others’ signatures by using their public key, unless the signature is encrypted.

1. What must she do to again be able to carry out all the operations mentioned above?

She needs to generate a new key pair, revoke her old key, get the new public key signed (preferably

by a CA) and publish it.