ID:20543555
Jiayu Xie

1.Mail of various colours

a:S >=dom B
By the Bell-La Padula confidentiality model,Contact can read the data iff C(s) >=dom C(o), and can only write the file
iff C(s) <=dom C(o).Then we can know level B has a lower security level than the contact level,then contact can read it.
And level S is higher than contact,hence contact can only write to it but not read it.Hence S >=dom B.

b:(1)read
(2)write
(3)read
(4)neither
(5)read
(6)write
c:
The company might use Stateful inspction firewall to block the files.Because Stateful inspction firewall can check each
file and figure out if it should be let it through.
d:
Start state: I(s)=Management{5,8,13,21} I(o) = Director{5,8,23,37}
step:write D401,read D118,write D401.read D340,writeD401,read D276,write D401

2.Adding salt to an open wound
a:
This hash code might be generate by SHA-1 hash function.Firstly,all character in this hash code are in range (1~9,a~f),we can
guess that they are representing hex number.And this code have length 40,which is also match the characteristic of SHA-1 hash
function.
MD-5 hash function should not produce this hash because MD-5 hash function produce a code of length 32.

b:
Guessing attack can be use to crash this hash.Since SHA-1 is standard cryptographic hash,if contents are the same,then the hash
code that created will also be the same.Read all the passwords in the data,try to find if there is are some hash code exist as
different password,then it might be a easy guess password.Combining some social enginering technique is also helpful.
c:
Adding salt has two main purpose.First,adding salt can make user's password become longer,can harder to be decrypt by rainbow table.
Second,by adding different salt,two same password will genrate different hash,which a guess attack become mostly impossible.
This bug make the salt become a fix string,then it lose its second function,two same password will still be the same after adding
salt and hash.

d:Since a non-iterated cryptographic hash function mighe be crash be finding a collision(find two different contend create a same hash),and adding salt cannot help to against this attack.

3.Going viral
a:
Packet filtering gateway.It block the IP outside from the company.
b:
The Ip address become legal when I physically go into the company.
c:
I might be block by a signature-based intrusion detection systems.
d:
Try to modify the virus to be a new attack that with a new signature,which cannot be detect by the IDS.