CSC347 Introduction to Information Security Assignment 3

Due: December 1, 2015 at 11:50 PM

Late penalty: 0% for 2 days, not accepted after that (so if you are swamped, hand in by the 3rd)

Hand in: Electronic submit here, your zip file (a3.zip) containing ...

```
a3/
    readme.txt (the members of your group)
    crypto/
        q1/
        q2/
                dhke_bob.py
                shared_secrets.txt
                cipher.py
                cipher_response.txt
        q3/
        openssl (the whole directory)
    network/
        1/
                report.txt
                # any other files you want to include

        2/
                report.txt
                # any other files you want to include
        3/
                firewall.bash
                # any other files you want to include
        4.txt
```

Marking: It is possible that some questions will not be marked.

Groups: Groups of size 2. Both students receive the same mark.

Cryptography

1. **[6 Marks]** Complete The Krypton wargame, submitting the passwords for each level.
2. **[4 Marks]** Download dhke.zip and unzip it.

   The Diffie Hellman Key exchange was used between Bob (you) and Alice (me) to exchange a shared symmetric key. Alice used the key in `cipher.py` to encrypt a message, resulting in `cipher.txt`. Your job is to

   - Complete `dhke_bob.py`
   - Run `dhke_bob.py` via `sample_run.bash`, producing a collection of shared secrets, save this as `shared_secrets.txt`.
   - Now complete `cipher.py` and use the last shared secret generated by `sample_run.bash` to decrypt `cipher.txt`
   - Encrypt your reply to my message and include it as cipher_response.txt. To make sure that I understand your message, try running decrypt on it. So decrypt(encrypt(message, key), key) should essentially be message again.

3. **[2 Marks]** Use openssl (see dgst) (installed on cslinux and on linux lab machines) to determine which of threeLaws1.txt or threeLaws2.txt or threeLaws3.txt the sha1 hash came from.
4. **[10 Marks]** Public Key Cryptography (openssl on cslinux and linux lab machines)

Please find the following:

- Arnolds Certificate: arnoldscert.pem
- Tapans Certificate: tapanscert.pem
- A Certificate Signing Request: req.pem
- openssl.zip (to be unzipped in your directory on cslinux).

Your job, understand and document the following scripts (in this order):

- openssl/caSetup
- openssl/caAnswerCSR
- makeCSR/doIt
- crypto/doIt (you need to complete this one)

The result of running these scripts leaves files in the openssl directory. Zip all of this and submit it back, again, with your documented scripts.

Network Security

Note

For this assignment you will be making extensive use of supplied virtual machines, DSL, FC4, Ubuntu804, RH7.2, and Kali. You can find it all in one zip at /virtual/arnold/csc347_a3.zip in our lab. Please let me know ASAP if you have any problem running these. You will have a problem with the virtual network in the lab, when you load a VM, please modify the network settings (Virtual Machine Settings -> Network Adapter) so that, an interface on VMNET3 is moved to VMNET8. Similarly, if an interface is on VMNET4, move it to VMNET1.

```
You will setup the following network:
-----------------------------------------------------------------------------------------------
Private Side: VMNET8 (from VMNET3), 192.168.0.0/255.255.255.0

    Ubuntu: 192.168.0.100
        Serving web and mail to the private network
        I will update this with a running smtp server for testing purposes later.
        sudo bash for root
        arnold/bpbthisisvulnerable2015

    Kali: IP (dhcp)
        root/toor

    DSL: 192.168.0.75  (To put this on the private network, you will need to switch to VMNET8)
        Administrators machine
        sudo su for root
        Setup networking by DSL->Setup->Net Setup->netcardconf

        Make the firewall the default gateway. Make sure you choose the
        correct side of the firewall depending on where you put this on the network.
        That is, either 10.10.10.10, or in this case 192.168.0.10

        NOTE: To boot DSL, change the settings so that it boots off the CD iso.
        You may have to change the path to directly point to the dslXXXX.iso.

FC4 Firewall/Gateway:
    eth1: 192.168.0.10
    eth0: 10.10.10.10
    root/password

    see /etc/sysconfig/myFirewall.bash

Public Side: VMNET1 (from VMNET4), 10.10.10.0/255.255.255.0
```

```
RH72: 10.10.10.11
    hacker/password
    root/password

NOTE: To boot DSL, change the settings so that it boots off the CD iso.
You may have to change the path to directly point to the dslXXXX.iso.

DSL_10: 10.10.10.128 (you can switch the IP of this machine manually)
DSL: 10.10.10.75
DSL: 10.10.10.33 (CEO)
```

1. **[5 Marks]** (Kali) Use nmap or zenmap to perform a network footprinting exercise on the private (192.168.0.*) network. Report all services and versions running all systems inside the network.
2. **[5 Marks]** Ubuntu804/Kali. Using tools on kali linux, scan the Ubuntu8.04 machine as well as the FC4 and the RH7.2 VMs. Check for vulnerabilities at, for example, The National Vulnerability Database. Are there vulnerable services? Provide a report, listing vulnerable services, and their issues. Also advise on a course of action.
3. **[10 Marks]** (FC4/DSL/Ubuntu/...) Configure your FC4 firewall using IP tables (see the lecture notes for my example firewall scripts).
    a. The 10.10.10.* network is the public network. The 192.168.0.* is the private network.
    b. Configure your firewall so that external http, https and smtp traffic can get to your web/mail server (the Ubuntu box).
    c. The web/mail server will also need to connect out on port 25 to relay email (the RH72 machine should be running a mail server for testing). You may have to sign in as root and start the service on the RH7.2 machine (/etc/init.d/sendmail start).
    d. Allow 192.168.0.75 to ssh into the firewall. No other access into the firewall is permitted.
    e. Allow 10.10.10.75 (outside the local network) to ssh into the web/mail server by using port 2222 on the external side side of the firewall. This is the only external ssh access allowed into the web/mail server.
    f. You might want to check that no other IPs outside can ssh into the web/mail server and the firewall.
    g. The CEO has a windows box inside the private network (192.168.0.33). The CEO (with fixed IP 10.10.10.33) would like to have remote desktop access to his desktop. Configure your firewall so that this is the case. The CEO's windows machine should have RDP restricted so that only their external machine
    h. The CEO has a windows box inside the private network (192.168.0.33). The CEO (with fixed IP 10.10.10.33) would like to have remote desktop access to his desktop. Configure your firewall so that this is the case. The CEO's windows machine should have RDP restricted so that only their external machine can connect (discuss what should be done to make sure this is the case).
    i. Sid, would also like RDP access to his windows box (with fixed IP 192.168.0.37) from his home at fixed IP 10.10.10.211. Can IP tables be used to do this as well? What if we want both to use the same RDP port on the firewall? No access to any services from 10.10.10.128 should be allowed.
    j. All machines inside the private network have their default route set to 192.168.0.10. All external machines know nothing about the internal network. Their default route can be set to 10.10.10.99 (a non-real machine).
    k. Finally, imagine that the only routable IP is 10.10.10.10. All internal machines should share this IP for internet traffic.

    Submit your firewall script annotated so that it is clear to Tapan which parts of your script accomplish which parts of this question.

4. **[8 Marks]** I used wireshark to sniff a bit of traffic on my network. Take a look at the wiresharkCapture
    a. Report everything you know about my network and its systems.
    b. Riddle: Whats the question? Whats the answer?
    c. Describe how you solved the above questions and two different ways one could prevent such an attack.

d. List anything else you discovered. Be creative.

Questions and Answers

Question:

Can't decrypt the ciper.txt in the dhke question.

Answer:

Yes, there was a problem with the cipher text. Please download cipher.txt. Also updated in the zip.

Question:

dhke_bob.py does not work.

Answer:

Yes, you are correct, it works in python2, it now works in python3.

Question:

```
> $ bash sample_run.bash
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
> sample_run.bash: ./dhke_bob.py: /usr/bin/python3: bad interpreter: No such
> file or directory
```

Answer:

```
Your platform does not have python3, or its located elsewhere. In our lab it is located in

    /usr/local/bin/python3

try

    which python3

to find yours.
```

Question:

```
        I can't get the RH72 machine on the network.
```

Answer:

I have uploaded a configured version at dh2020pc00.utm.utoronto.ca:/virtual/rosenbl6/RH72LabImage_A1_2015.zip