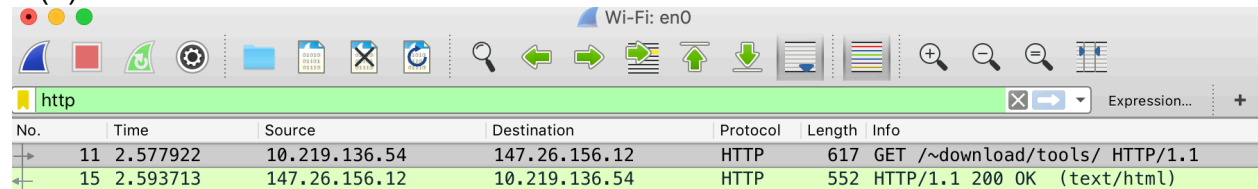


Hanna Rakhsha h\_r77  
CS 4371 – Gu  
Homework 1

- 1(a) Confidentiality, Mary should keep her homework in a personal folder or file, so only she has access to it. This would prevent copying.
- (b) Availability, Linda's system should block unauthorized attempts to her system with a simple login feature. This would prevent her system crashing.
- (c) Integrity, someone (other than Carol) should verify the amount on the checks to detect and limit dishonesty.
- (d) Integrity, the people with the deed should verify the signature from a personal document of Roger's (like passport, driver's license, government id, etc.) to prevent forgery.
- (e) Availability, the university should have a backup server in case of deletion.
- (f) Integrity, Julie should require a special security token to prevent spoofing attacks.

2 (a)



No.	Time	Source	Destination	Protocol	Length	Info
11	2.577922	10.219.136.54	147.26.156.12	HTTP	617	GET /~download/tools/ HTTP/1.1
15	2.593713	147.26.156.12	10.219.136.54	HTTP	552	HTTP/1.1 200 OK (text/html)

```

▶ Frame 11: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits) on interface 0
▶ Ethernet II, Src: Apple_a3:e8:c1 (f4:5c:89:a3:e8:c1), Dst: JuniperN_ea:dc:00 (f4:cc:55:ea:dc:00)
▶ Internet Protocol Version 4, Src: 10.219.136.54, Dst: 147.26.156.12
▶ Transmission Control Protocol, Src Port: 49420, Dst Port: 80, Seq: 1, Ack: 1, Len: 551
▶ Hypertext Transfer Protocol

```

```

0000 f4 cc 55 ea dc 00 f4 5c 89 a3 e8 c1 08 00 45 00  ..U....\ .....E.
0010 02 5b 00 00 40 00 40 06 76 65 0a db 88 36 93 1a  .[. @. @. ve...6..
0020 9c 0c c1 0c 00 50 71 7b 80 70 92 80 0a f9 80 18  ....Pq{ .p.....
0030 08 0a c2 a3 00 00 01 01 08 0a 0c a2 77 5d 7c ed  ....w]|.
0040 ab 75 47 45 54 20 2f 7e 64 6f 77 6e 6c 6f 61 64  .uGET /~ download
0050 2f 74 6f 6f 6c 73 2f 20 48 54 54 50 2f 31 2e 31  /tools/ HTTP/1.1
0060 0d 0a 48 6f 73 74 3a 20 66 75 78 69 2e 63 73 2e  .Host: fuxi.cs.
0070 74 78 73 74 61 74 65 2e 65 64 75 0d 0a 41 63 63  txstate. edu..Acc
0080 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61  ept: tex t/html,a
0090 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c  pplicati on/xhtmll

```

- Hypertext Transfer Protocol (http), 551 bytes      Packets: 32 · Displayed: 2 (6.2%) · Dropped: 0 (0.0%)      Profile: Default
- (b) Source: f4:5c:89:a3:e8:c1      Destination: f4:cc:55:ea:dc:00
  - (c) Source: 10.219.136.54      Destination: 147.26.156.12
  - (d) Source Port: 49420      Destination Port: 80
  - (e) Request: GET /~download/tools/ HTTP/1.1\r\n      Response: HTTP/1.1 200 OK\r\n

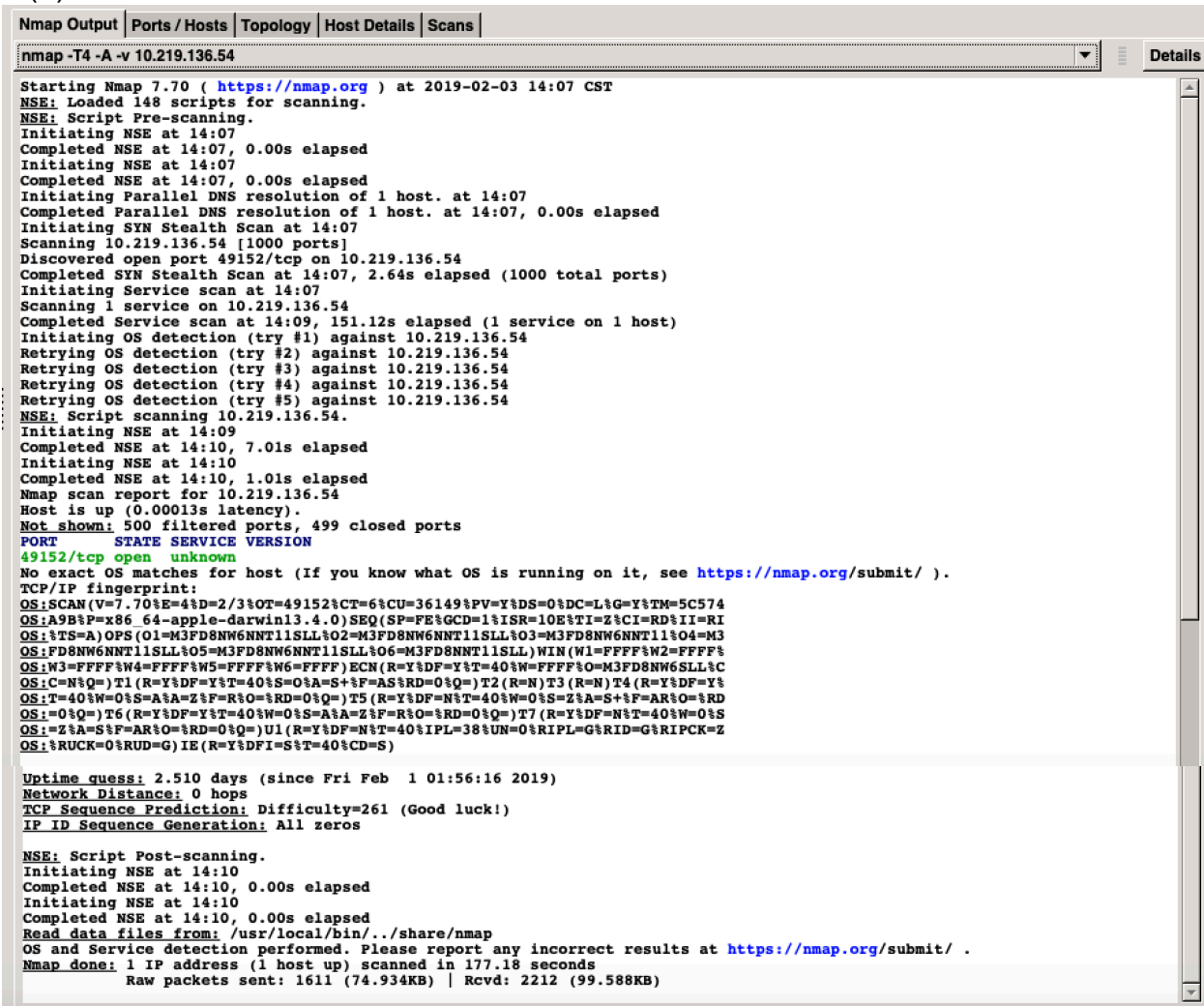
3 (a) IP address of the website: 147.26.156.12

(b) <http://fuxi.cs.txstate.edu/~download/tools/>  
<http://fuxi.cs.txstate.edu/icons/blank.gif>  
<http://fuxi.cs.txstate.edu/icons/back.gif>  
<http://fuxi.cs.txstate.edu/icons/folder.gif>  
<http://fuxi.cs.txstate.edu/icons/compressed.gif>  
<http://fuxi.cs.txstate.edu/~download/tools/Kali.vbox/>  
<http://fuxi.cs.txstate.edu/icons/back.gif>  
<http://fuxi.cs.txstate.edu/icons/text.gif>  
<http://fuxi.cs.txstate.edu/icons/unknown.gif>  
<http://fuxi.cs.txstate.edu/icons/blank.gif>  
<http://fuxi.cs.txstate.edu/icons/script.gif>  
<http://fuxi.cs.txstate.edu/~download/tools/Kali.vbox/readme.txt>  
<http://fedoraproject.org/static/hotspot.txt>

(c) Content-Type: text/plain; charset=utf-8\r\n

Line based text data: OK

4 (a)



```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans |
nmap -T4 -A -v 10.219.136.54

Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-03 14:07 CST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:07
Completed Parallel DNS resolution of 1 host. at 14:07, 0.00s elapsed
Initiating SYN Stealth Scan at 14:07
Scanning 10.219.136.54 [1000 ports]
Discovered open port 49152/tcp on 10.219.136.54
Completed SYN Stealth Scan at 14:07, 2.64s elapsed (1000 total ports)
Initiating Service scan at 14:07
Scanning 1 service on 10.219.136.54
Completed Service scan at 14:09, 151.12s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.219.136.54
Retrying OS detection (try #2) against 10.219.136.54
Retrying OS detection (try #3) against 10.219.136.54
Retrying OS detection (try #4) against 10.219.136.54
Retrying OS detection (try #5) against 10.219.136.54
NSE: Script scanning 10.219.136.54.
Initiating NSE at 14:09
Completed NSE at 14:10, 7.01s elapsed
Initiating NSE at 14:10
Completed NSE at 14:10, 1.01s elapsed
Nmap scan report for 10.219.136.54
Host is up (0.00013s latency).
Not shown: 500 filtered ports, 499 closed ports
PORT      STATE SERVICE VERSION
49152/tcp  open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=2/3%OT=49152%CT=6%CU=36149%PV=Y%DS=0%DC=L%G=Y%TM=5C574
OS:A9B%P=x86_64-apple-darwin13.4.0)SEQ(SF=FE%GCD=1%ISR=10E%TI=Z%CI=RD%II=RI
OS:TS=A)OPS(O1=M3FD8NW6NNT11SLL%O2=M3FD8NW6NNT11SLL%O3=M3FD8NW6NNT11%O4=M3
OS:FD8NW6NNT11SLL%O5=M3FD8NW6NNT11SLL%O6=M3FD8NW6NNT11SLL)WIN(W1=FFFF%W2=FFFF%
OS:W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M3FD8NW6SLL%C
OS:C=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%
OS:T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD
OS:O=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S
OS:Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=Z
OS:%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Uptime guess: 2.510 days (since Fri Feb  1 01:56:16 2019)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

NSE: Script Post-scanning.
Initiating NSE at 14:10
Completed NSE at 14:10, 0.00s elapsed
Initiating NSE at 14:10
Completed NSE at 14:10, 0.00s elapsed
Read data files from: /usr/local/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 177.18 seconds
Raw packets sent: 1611 (74.934KB) | Rcvd: 2212 (99.588KB)
```

(b)

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-03 14:25 CST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:25
Completed NSE at 14:25, 0.00s elapsed
Initiating NSE at 14:25
Completed NSE at 14:25, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:25
Completed Parallel DNS resolution of 1 host. at 14:25, 0.01s elapsed
Initiating SYN Stealth Scan at 14:25
Scanning 10.219.136.54 [1000 ports]
Discovered open port 8080/tcp on 10.219.136.54
Discovered open port 49152/tcp on 10.219.136.54
Discovered open port 8000/tcp on 10.219.136.54
Discovered open port 11111/tcp on 10.219.136.54
Completed SYN Stealth Scan at 14:25, 3.10s elapsed (1000 total ports)
Initiating Service scan at 14:25
Scanning 4 services on 10.219.136.54
Service scan Timing: About 75.00% done; ETC: 14:28 (0:00:51 remaining)
Completed Service scan at 14:28, 151.13s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.219.136.54
Retrying OS detection (try #2) against 10.219.136.54
Retrying OS detection (try #3) against 10.219.136.54
Retrying OS detection (try #4) against 10.219.136.54
Retrying OS detection (try #5) against 10.219.136.54
NSE: Script scanning 10.219.136.54.
Initiating NSE at 14:28
Completed NSE at 14:28, 7.17s elapsed
Initiating NSE at 14:28
Completed NSE at 14:28, 1.07s elapsed
Nmap scan report for 10.219.136.54
Host is up (0.00011s latency).
Not shown: 499 filtered ports, 497 closed ports
PORT      STATE SERVICE VERSION
8000/tcp  open  http      Werkzeug httpd 0.12.2 (Python 3.4.3)
|_ http-title: 404 Not Found
8080/tcp  open  http      nginx 1.4.6 (Ubuntu)
|_ http-favicon: Unknown favicon MD5: 6631AFC41997015FAF23425A09EA74DC
|_ http-methods:
|_   Supported Methods: GET HEAD
|_ http-server-header: nginx/1.4.6 (Ubuntu)
|_ http-title: TxState Ctf - Homepage
11111/tcp open  vnc?

fingerprint-strings:
  DNSStatusRequestTCP:
    ODY===
  DNSVersionBindReqTCP:
    NDC0===
  FourOhFourRequest:
    OTg4===
    NDU1===
    NjA5===
  GenericLines:
    NDAz===
    ODU1===
    Odk2===
  GetRequest:
    MjYz===
    MjQ2===
    Mjc0===
  HTTPOptions:
    MzY4===
    MzEw===
    NjM5===
  Help:
    ODkz===
    NDC1===
  JavaRMI:
    Nzg===
  Kerberos:
    OTc5===
    OTgx===
  LANDesk-RC:
    MTc0===
  LDAPBindReq:
    NzIO===
  LDAPSearchReq:
    MjA0===
    MjY===
    NzUw===
  LPDString:
    MzA1===
    NDK0===
  NCP:
    NDQz===
  NULL:
    NDAz===
  NotesRPC:
```

```
OTM4==
RPCCheck:
Mg==
RTSPRequest:
NjA==
MzQ1==
MjM0==
SIPOptions:
OTE3==
NTY2==
Njkz==
NzM2==
MzcX==
OTA1==
NjIw==
Mjc0==
NTg1==
ODAY==
MTCZ==
MzU2==
SMBProgNeg:
OTg2==
SSLSessionReq:
Mzg4==
NjU1==
TLSSessionReq:
MTAY==
OTc5==
TerminalServer:
ODk2==
WMSRequest:
MjI4==
X11Probe:
NTI0==
afp:
ODY2==
giop:
NDY4==
ms-sql-s:
MTQ0==
oracle-tns:
NzM0==
```

49152/tcp open unknown

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
SF-Port11111-TCP:V=7.70%I=7%D=2/3%Time=5C574E43%P=x86_64-apple-darwin13.4.
SF:0%r(NULL,7,"NDAZ==\n")%r(GenericLines,15,"NDAZ==\nODU1==\nODk2==\n")%r(
SF:GetRequest,15,"MjYz==\nMjQ2==\nMjc0==\n")%r(HTTPOptions,15,"MzY4==\nMzE
SF:w==\nNjM5==\n")%r(RTSPRequest,15,"NjA==\nMzQ1==\nMjM0==\n")%r(RPCCheck
SF:7,"Mg==\n")%r(DNSVersionBindReqTCP,7,"NDc0==\n")%r(DNSStatusRequestT
SF:CP,7,"ODY==\n")%r(Help,E,"ODkz==\nNDc1==\n")%r(SSLSessionReq,E,"Mzg4==
SF:nNjU1==\n")%r(TLSSessionReq,E,"MTAY==\nOTc5==\n")%r(Kerberos,E,"OTc5==
SF:nOTGz==\n")%r(SMBProgNeg,7,"OTg2==\n")%r(X11Probe,7,"NTI0==\n")%r(Four
SF:OhFourRequest,15,"OTg4==\nNDU1==\nNjA5==\n")%r(LPDString,E,"MzA1==\nNDk
SF:0==\n")%r(LDAPSearchReq,15,"MjA0==\nMjY==\nNzUw==\n")%r(LDAPBindReq,7,
SF:"NzI0==\n")%r(SIPOptions,54,"OTE3==\nNTY2==\nNjkz==\nNzM2==\nMzcX==\nOT
SF:Al==\nNjIw==\nMjc0==\nNTg1==\nODAY==\nMTCZ==\nMzU2==\n")%r(LANDesk-RC,7
SF:"MTC0==\n")%r(TerminalServer,7,"ODk2==\n")%r(NCP,7,"NDQz==\n")%r(Notes
SF:RPC,7,"OTM4==\n")%r(JavaRMI,7,"Nzg==\n")%r(WMSRequest,7,"MjI4==\n")%r(
SF:oracle-tns,7,"NzM0==\n")%r(ms-sql-s,7,"MTQ0==\n")%r(afp,7,"ODY2==\n")%r
SF:(giop,7,"NDY4==\n");
```

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

```
OS:SCAN(V=7.70%E=4%D=2/3%OT=8000%CT=3%CU=37177%PV=Y%DS=0%DC=L%G=Y%TM=5C574E
OS:EB%P=x86_64-apple-darwin13.4.0)SEQ(SP=FD%GCD=1%ISR=109%TI=Z%CI=RD%II=RI%
OS:TS=A)SEQ(CI=RD%II=RI)OPS(O1=M3FD8NW3NNT11SLL%O2=M3FD8NW3NNT11SLL%O3=M3FD
OS:8NW3NNT11%O4=M3FD8NW3NNT11SLL%O5=M3FD8NW3NNT11SLL%O6=M3FD8NNT11SLL)WIN(W
OS:1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%
OS:O=M3FD8NW3SLL%CC=N%Q)ECN(R=N)T1(R=Y%DF=Y%T=40%W=0%S=A%F=AS%RD=0%Q)T2(
OS:R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%F=R%O=RD=0%Q)T5(R=Y%DF=N%T=40%
OS:W=0%S=Z%A=S+F=AR%O=RD=0%Q)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=RD=0%Q)
OS:T7(R=Y%DF=N%T=40%W=0%S=Z%A=S+F=AR%O=RD=0%Q)U1(R=Y%DF=N%T=40%IPL=38%UN
OS:0%RIPL=G%RID=G%RIPCK=Z%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)
```

Uptime guess: 2.522 days (since Fri Feb 1 01:56:17 2019)

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=261 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

NSE: Script Post-scanning.

Initiating NSE at 14:28

Completed NSE at 14:28, 0.00s elapsed

Initiating NSE at 14:28

Completed NSE at 14:28, 0.00s elapsed

Read data files from: /usr/local/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 178.97 seconds

Raw packets sent: 1645 (76.906KB) | Rcvd: 2235 (100.996KB)

## 5 and 6.

Witches - 20	Coding - Solved
The Race - 30	Coding - Solved
Hacker Level - 40	Coding - Solved
Gatta Catch Em All - 50	Coding - Solved
<a href="#">Solve</a>	<a href="#">Hint</a>