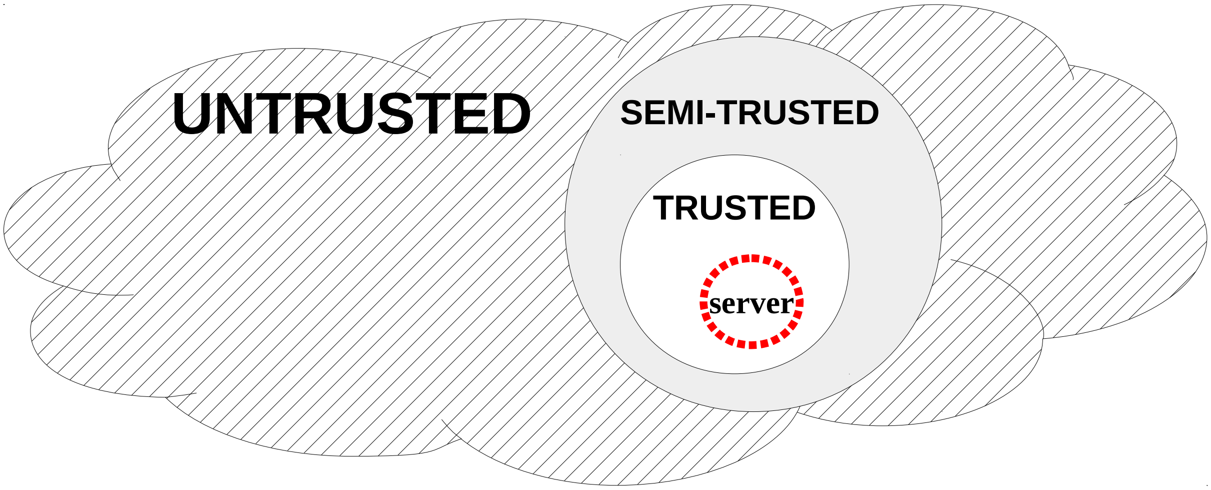
Network Firewall

In this project, your firewall defense program will attempt to implement the rules of the firewall protecting a server so that it only responds to allowed incoming traffic. Your attack program will try to get unallowed traffic through the firewall and get a response from the server.

There will be a set of TRUSTED source IP addresses and a separate set of SEMI-TRUSTED source IP addresses. Any source IP that is not TRUSTED or SEMI-TRUSTED is UNTRUSTED. But just because a source is TRUSTED or SEMI-TRUSTED does not mean all traffic from it is allowed. Traffic will only be allowed from certain ports and for certain application protocols.



Defense

Various sources will try to communicate with your network server. Your firewall defense program should inspect the source IP, port and application protocol to ensure that only some traffic is responded to. Log the IP address from the communication socket, as well as the message received. The application protocol and port will be contained in the message.

- Send back an “Accept” message to communication attempts from a TRUSTED source IP and TRUSTED source port if the application protocol type is TRUSTED.
- Send back a “Reject” message to communication attempts from a TRUSTED source IP and TRUSTED source port if the application protocol type is SEMI-TRUSTED.
- Send back a “Reject” message to communication attempts from a TRUSTED source IP and TRUSTED source port if the application protocol type is UNTRUSTED.

- Send back a “Reject” message to communication attempts from a SEMI-TRUSTED IP and TRUSTED source port if the application protocol is TRUSTED.
- Send back a “Reject” message to communication attempts from a TRUSTED source IP and SEMI-TRUSTED source port if the application protocol type is TRUSTED.
- Otherwise, do not send back a response, “drop” the communication.
- In all cases, write the IP address and message sent along with the action taken for a communication attempt to a file, to simulate passing the information to an IDS, whether “Accept”, “Reject”, or “Drop”.

Attack

A network server is protected by a firewall that attempts to only respond to certain traffic. You will test this firewall defense with your attack program. The goal of the attack is to get a response from the server that is not in accordance with the rules described above in the Defense section.

- Each attack program will make one communication attempt to the server.

Assignment Instructions

Using Repy v2 (Restricted Python)

Defense and Attack Programs will be written in repy v2 (Restricted Python). Usage instructions for RepyV2 are here:

https://github.com/SeattleTestbed/docs/blob/master/Programming/RepyV2Tutorial.md

If you’re familiar with Python, RepyV2 is similar, but has a few differences that are explained here:

https://github.com/SeattleTestbed/docs/blob/master/Programming/PythonVsRepyV2.md

Virtual Machine

A VirtualBox machine with Repy v2 installed will be provided. There will be a repy_v2 folder under home.

Message format for communication attempt

The attack programs will include an application protocol in the first 2 characters of the message and a source port number in the following 5 characters. Any further characters in the message are optional. An example message with an application protocol of HT and port of 87654 is below.

protocol		port					additional message (optional)									
H	T	8	7	6	5	4	H	E	L	L	O	0	0	0	0

The defense programs will get the source IP from the connection request, and parse the protocol and port in the message to determine the appropriate (if any) response.

A sample, though insufficient, program for your defense is provided. You will need to modify the code to implement all the firewall rules. Also modify the given code to use the 3-digit student code you have been assigned.

A sample attack program is also provided to test against your defense code prior to submission.

Trust Definitions

In this project, the following values represent trusted sources.

TRUSTED

IP	127.0.0.1 through 127.0.0.12
Port	20001, 28724, 39845
AP	HT, GL

In this project, the following values represent semi-trusted sources.

SEMI-TRUSTED

IP	127.0.0.13 through 127.1.1.255
Port	49034
AP	SR

UNTRUSTED

Anything not specifically enumerated above. Note that this program will be running locally, so all IP addresses used must be in the 127 network.

Submission

Defense – Part 1

- Submit one defense program, named firewalldefend_###.r2py, where ### is your assigned 3-digit student code.
- Be sure that you have modified the defense program to include your 3-digit student code as part of the firewall logfile that is created.

Attack – Part 2

- You may select up to 5 defense programs to attack. Submit one attack program for a defense.
- Name your submitted attack programs "Firewall_DDD_Attack_###.r2py", where DDD is the number code in the defense program being attacked, and ### is your unique student code.