Server Security Testing

Once the Raspberry-Pi server and all security implementation is in place, an attempt was made to take control of the server from an outside source using DDOS, SQL injection and brute forcing.

Table 9 - Server Security Test Descriptors

Test #	Test Name	Description	Reason	Pass Condition	Outcome
S.1	Ping test	The router should not be pingable from an outside source.	When many people try to ping a server, it could create a DDOS attack. Therefore, pinging should be removed to prevent this from happening.	Trying to ping the router from outside the network should not work.	Since the server was located on RIT's campus, this test passes automatically since someone can not ping rit.edu.
S.2	Disable Root Login	While SSHing into the server, users should not be able to login as root	Root is all knowing in linux. If someone were to somehow gain access to root, they could wreak havoc on the server.	Trying to login as root results in an access denied.	Pass. Trying to login as root fails.
S.3	SSH non-standard port test	While trying to SSH into the server using the default ssh port, the result should be not being able to connect.	By moving the SSH port to a non-standard port, it makes it difficult for some hackers to find the ssh port, and try brute forcing.	Trying to login to port 22 via ssh will fail. Trying to login to the non-standard port will succeed.	Pass. Trying port 22 fails.
S.4	Disabled	Trying to login	SSHing with a user	SSHing into	Pass. A key

	Password Test	with SSH will have an access denied without an ssh key. SSHing will not be allowed without a password.	name and a password is not safe for a server. A hacker can brute force their way in.	a server without a key will result in an access denied. SSHing will not ask for a password.	is required to login to the server.
S.5	White hat hacker test	Borrow one of the many security majors the group knows, give them the ip address, and have them attempt to take the server down.	Having a friendly hacker attempt to break into the server will emulate a more sinister hacker trying to get in. If any information is compromised by the friendly hacker, they will not steal it.	The hackers should not be able to take the server down.	Pass. Two security majors tried to hack the server. They even complimented on how secure it was.