

1783: GENI Experiments for Traffic Capture Capabilities and Security Requirement Analysis:

ProtoGENI Security Experimentation

Jingcheng Gao, Fnu Shalini, Sneha Rao,
Yang Xiao, and Xiaoyan Hong

The University of Alabama

Introduction

- **Goal:**
 - help define GENI security requirements based on investigations through ProtoGENI experiments
- **Approach:**
 - – Select functions of ProtoGENI control framework
 - – Experiments on aggregates (EMULAB first)
 - Experiment design, run, identify/ exploit/ validate potential vulnerabilities
 - Delivered experiment design documents

Introduction



- This presentation only provides a partial status report conducted by the first three authors (students);
- Other experiments:
 - ExptsSec-milestone3-findings-b.pdf (it will be posted on the project website)

Threats to Availability of Resources

- Distribution of resources
 - As many as slices created by users requesting few resources in each slice
 - Few slices but requesting a large number of resources at a time
 - Analysis of Vulnerability of wildcard allocation of resources through Rspecs.

Experiments

- **Experiment A: creation of as many as possible slices to see resources outage**
- **Creation of slices and allocation of resources to slivers**
 - Initial Emulab status : 33 free PCs
 - 16 slices were created as a series of similar names like shailslice1, shailslice2.... shailslice16, each with a request of 2 PCs , then to observe for 17th slice
 - Could not create all 16 slices. 3 slices were aborted and only one free PC was left after creation of 14th Slice.
- **Deletion of slices and freed resources back**
 - Slices were deleted backwards and Emulab site was changing its status of free PCs with each slice's deletion.
 - After deletion of all slices, all acquired resources were freed

Applications Places System   ? Wed

shailrspec.xml (~) - gedit - □ ×

File Edit View Search Tools Documents Help

New Open Save Print... Undo Redo

shailrspec.xml ×

```
<rspec xmlns="http://protogeni.net/resources"
<node virtual_id="geni1"
virtualization_type="emulab-vnode"
exclusive="1">
<interface virtual_id="virt0"/>
</node>
<node virtual_id="geni2"
virtualization_type="emulab-vnode"
exclusive="1">
<interface virtual_id="virt0"/>
</node>
<link virtual_id="link0">
<interface_ref virtual_interface_id="virt0"
virtual_node_id="geni1"/>
<interface_ref virtual_interface_id="virt0"
virtual_node_id="geni2"/>
</link>
</rspec>
```

XML Tab

sshali@ubuntu: ~/protogeni/test - □ ×

File Edit View Terminal Help

M2Crypto-0.20.2 protogeni Python-3.1.1

```
sshali@ubuntu:~$ sudo cp shailrspec.xml protogeni/test/shailrspec.xml
sshali@ubuntu:~$ cd protogeni
sshali@ubuntu:~/protogeni$ cd tets
bash: cd: tets: No such file or directory
sshali@ubuntu:~/protogeni$ ls
M2Crypto.egg-info test
sshali@ubuntu:~/protogeni$ cd test
sshali@ubuntu:~/protogeni/test$ ls
binduser.py          jailtun.rspec          resolve.py
bound-type.rspec    linktest.rspec        shailrspec.xml
createsliver.py     list-ch.py            showcredential.py
delegate.py         listcomponents.py     shutdownslice.py
deleteslice.py     listusage.py          slice.py
deletesliver.py    loctuntest.rspec     sliveraction.py
discover.py         lookupuser.py         sliverstatus.py
fwtest.rspec       map.py                spp-lan.rspec
getcredential.py    protogeni-tests.tar.gz spp-link.rspec
getslicecredential.py redeemticket.py       test-common.py
getticket.py       registerslice.py      tuntest.py
getversion.py      releaseticket.py     unregisterslice.py
jaillink.rspec     renewsliver.py        updatesliver.py
jailtest.rspec     resolve-ch.py         waitforsliver.py
sshali@ubuntu:~/protogeni/test$
```

1 Free PCs
9 PCs reloading
22 active users
63 active expts.

'shail01' Logged in.
Mon May 03 3:36pm MDT

```
sshalini@ubuntu:~/protogeni/test$ python createsliver.py -n shailslice16 shailrs
pec2.xml
Got my SA credential
No such slice registered here:Creating new slice called shailslice16
New slice created
Creating the Sliver ...
Could not map to resources: Could not create sliver
sshalini@ubuntu:~/protogeni/test$
```

```
id="eth0"/>
type="raw" excl
component_uuid=
:publicid:IDN+e
d-ad1f-001143e4
="pcwf1.emulab.
```

sshalini@ubuntu: ~/protogeni/test

File Edit View Terminal Help

```
-773e-102b-8eb4-001143e453fe" hostname="pc2.emulab.net" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8942">
<interface virtual_id="virt0" component_id="eth0"/>
</node>
<link virtual_id="link0" sliver_uuid="a7ea0362-56fb-11df-ad83-001143e453fe" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8943">
<interface_ref virtual_interface_id="virt0" virtual_node_id="geni1" sliver_uuid="a8a15152-56fb-11df-ad83-001143e453fe" component_urn="urn:publicid:IDN+emulab.net+interface+pc306:eth4" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8944" MAC="000423b7126a" IP="10.10.1.1"/>
<interface_ref virtual_interface_id="virt0" virtual_node_id="geni2" sliver_uuid="a9152728-56fb-11df-ad83-001143e453fe" component_urn="urn:publicid:IDN+emulab.net+interface+pc2:eth0" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8945" MAC="00d0b713f28e" IP="10.10.1.2"/>
</link>
</rspec>
```

```
sshalini@ubuntu:~/protogeni/test$ python createsliver.py -n shailslice15 shailrs
pec2.xml
Got my SA credential
No such slice registered here:Creating new slice called shailslice15
New slice created
Creating the Sliver ...
Could not map to resources: Could not create sliver
sshalini@ubuntu:~/protogeni/test$
```



```
ssh@kali: ~$ sshalini@ubuntu: ~/protogeni/test
File Edit View Terminal Help
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
ssh@kali: ~$ sshalini@ubuntu:~/protogeni/test$ python deleteslice.py -n shailslice11
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
No such slice here: Could not delete slice
ssh@kali: ~$ sshalini@ubuntu:~/protogeni/test$ python deleteslice.py -n shailslice10
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
ssh@kali: ~$ sshalini@ubuntu:~/protogeni/test$ python deleteslice.py -n shailslice9
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
ssh@kali: ~$ sshalini@ubuntu:~/protogeni/test$
```

6 Free PCs	14 Free PCs	32 Free PCs
5 PCs reloading	14 PCs reloading	5 PCs reloading
22 active users	23 active users	21 active users
61 active expts	55 active expts.	52 active expts.

'shail01' Logged in.
Mon May 03 3:36pm MDT

• **Experiment B: Creation of few slices with larger set of required resources in single Rspecs to see resources outage**

• **Creation of 5 stress slices and allocation of resources to slivers**

- Stressrspec.xml was created to request 6 PCs and 3 links
- Stressrspec2.xml was created to request 14 PCs and 7 links
- Could not create all 5 slices. Stressslice3 was aborted. After 4th slice, free PCs were 7 and slice 5 was requesting 14 PCs, so could not allocate the resources.

• **Deletion of slices and freed resources back**

- Slices were deleted backwards and Emulab site was changing its status of free PCs with each slice's deletion.
- After deletion of all slices, all acquired resources were freed

7 Free PCs
3 PCs reloading
21 active users
56 active expts.

'shail01' Logged in.
Mon May 03 3:36pm MDT

sshalini@ubuntu: ~/protogeni/test

```
File Edit View Terminal Help
sshalini@ubuntu:~$ cd protogeni
sshalini@ubuntu:~/protogeni$ cd test
sshalini@ubuntu:~/protogeni/test$ sudo vim stressrspec2.xml
sshalini@ubuntu:~/protogeni/test$ python createsliver.py -n stresssliver4 stressrspec2.xml
Got my SA credential
No such slice registered here:Creating new slice called stresssliver4
New slice created
Creating the Sliver ...
Created the sliver
<rspec xmlns="http://protogeni.net/resources/rspec/0.1">
<node virtual_id="geni1" virtualization_type="raw" exclusive="1" component_urn="urn:publicid:IDN+emulab.net+node+pc350" component_uuid="de9f66a1-773e-102b-8eb4-001143e453fe" component_manager_urn="urn:publicid:IDN+emulab.net+authority+cm" component_manager_uuid="28a10955-aa00-11dd-ad1f-001143e453fe" sliver_uuid="de9f66a1-773e-102b-8eb4-001143e453fe" hostname="pc350.emulab.net" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8995">
<interface virtual_id="virt0" component_id="eth4"/>
</node>
<node virtual_id="geni2" virtualization_type="raw" exclusive="1" component_urn="urn:publicid:IDN+emulab.net+node+pc306" component_uuid="de9dbf1c-773e-102b-8eb4-001143e453fe" component_manager_urn="urn:publicid:IDN+emulab.net+authority+cm" component_manager_uuid="28a10955-aa00-11dd-ad1f-001143e453fe" sliver_uuid="de9dbf1c-773e-102b-8eb4-001143e453fe" hostname="pc306.emulab.net" sliver_urn="urn:publ
```


18 Free PCs
13 PCs reloading
21 active users
54 active expts.

'shail01' Logged in.
Mon May 03 3:36pm MDT

```
sshshalini@ubuntu: ~/protogeni/test
File Edit View Terminal Help
er_urn="urn:publicid:IDN+emulab.net+sliver+8975">
<interface_ref virtual_interface_id="virt2" virtual_node_id="geni5" sliver_uuid=
"3160aee1-5705-11df-ad83-001143e453fe" component_urn="urn:publicid:IDN+emulab.ne
t+interface+pc57:eth3" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8976" MAC=
"0002b365c1d7" IP="10.10.3.1"/>
<interface_ref virtual_interface_id="virt2" virtual_node_id="geni6" sliver_uuid=
"31cf8c8c-5705-11df-ad83-001143e453fe" component_urn="urn:publicid:IDN+emulab.ne
t+interface+pc65:eth3" sliver_urn="urn:publicid:IDN+emulab.net+sliver+8977" MAC=
"0002b33f74fd" IP="10.10.3.2"/>
</link>
</rspec>
sshshalini@ubuntu:~/protogeni/test$ python deleteslice.py -n stressslice2
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
sshshalini@ubuntu:~/protogeni/test$ python deleteslice.py -n stressslice1
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
sshshalini@ubuntu:~/protogeni/test$
```



```
sshali@ubuntu: ~/protogeni/test
File Edit View Terminal Help
sshali@ubuntu:~/protogeni/test$ ls
binduser.py                jaillun.rspec            shailrspec2.xml
bound-type.rspec          linktest.rspec           shailrspec.xml
boundtype.xml             list-ch.py               showcredential.py
client.c                  listcomponents.py        shutdownslice.py
createsliver.py          listusage.py             slice.py
delegate.py              loctuntest.rspec        sliveraction.py
deleteslice.py           lookupuser.py            sliverstatus.py
deletesliver.py          map.py                   spp-lan.rspec
diewitherror.c           pctype.xml              spp-link.rspec
discover.py              protogeni-tests.tar.gz  stressrspec2.xml
fwtest.rspec             redeemticket.py         stressrspec.xml
getcredential.py         registerslice.py         test-common.py
getslicecredential.py   releaseticket.py        tuntest.py
getticket.py             renewsliver.py           unregisterslice.py
getversion.py            resolve-ch.py            updatesliver.py
handletcpclient.c       resolvename.c           waitforsliver.py
jaillink.rspec           resolve.py               server.c
jailtest.rspec
sshali@ubuntu:~/protogeni/test$ python getversion.py
1
sshali@ubuntu:~/protogeni/test$ python getticket.py -n mytestslice stressrspec
2.xml
Got my SA credential, looking up mytestslice
No such slice registered here:Creating new slice called mytestslice
New slice created
Asking for a ticket from the local CM
Got the ticket, doing a update on it.
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<signed-credential xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noN
```

```
sshali@ubuntu: ~/protogeni/test
File Edit View Terminal Help
dHBz0i8vd3d3LmVtdWxhYi5uZXQvcHJvdG9nZW5pL3htbHJwYy9jbTANBgkqhkiG
9w0BAQQFAA0BgQB6h72zQ4jfzPVMNDUHLJbRD8RH60Vqpyy593jUqrWkgknKKGj0
Ap0391+0Y43BSipxgY4kR9UhiEIBI r0yoB/cSs9JMcLV30pPNwJfjtQy3q59VUCS
GheZ/zG4H7kMvNY3/3KwEpl9LbKWxo5kFk1jWlHoN+E0NWFwq9rWRNFbuQ==
</target_gid>
<uid>3a34babb-5b7a-11df-ad83-001143e453fe</uid>
<expires>2010-05-09T14:55:36</expires>
<ticket>
  <can_delegate>1</can_delegate>
  <redeem before>2010-05-09T14:55:36</redeem before>
```

```
sshalini@ubuntu:~/protogeni/test$ python redeemticket.py -n mytestslice 360000
Got my SA credential
Asking for slice credential for mytestslice
Got the slice credential
Resolving the slice at the CM
{'urn': 'urn:publicid:IDN+emulab.net+slice+mytestslice', 'ticket_urn': 'urn:publicid:IDN+emulab.net+ticket+36360'}
Asking for the ticket
Got the ticket
Redeeming the ticket
Created the sliver
<rspec xmlns="http://protogeni.net/resources/rspec/0.1">
```

```
sshalini@ubuntu: ~/protogeni/test
File Edit View Terminal Help
sshalini@ubuntu:~$ cd protogeni
sshalini@ubuntu:~/protogeni$ cd test
sshalini@ubuntu:~/protogeni/test$ python sliverstatus.py -n mytestslice
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential, asking for a sliver credential ...
Got the sliver credential, asking for sliver status
{'status': 'ready', 'state': 'started', 'details': {'urn:publicid:IDN+emulab.net+sliver+9435': {'status': 'ready', 'state': 'started', 'component_urn': 'urn:publicid:IDN+emulab.net+node+pc144', 'error': ''}, 'urn:publicid:IDN+emulab.net+sliver+9436': {'status': 'ready', 'state': 'started', 'component_urn': 'urn:publicid:IDN+emulab.net+node+pc154', 'error': ''}}}
```

```
sshalini@ubuntu:~/protogeni/test$ python sliverstatus.py -n mytestslice
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Not your slice!: Could not get Slice credential
sshalini@ubuntu:~/protogeni/test$
```

Sliver creation requesting specific type of resources

```
sshalini@ubuntu: ~/protogeni/test
File Edit View Terminal Help
sshalini@ubuntu:~$ cd protogeni
sshalini@ubuntu:~/protogeni$ cd test
sshalini@ubuntu:~/protogeni/test$ sudo vim boundtype.xml
[sudo] password for sshalini:
sshalini@ubuntu:~/protogeni/test$ python createsliver.py -n specificpc0 boundtype.xml
Got my SA credential
No such slice registered here:Creating new slice called specificpc0
New slice created
Creating the Sliver ...
Could not map to resources: Could not create sliver
sshalini@ubuntu:~/protogeni/test$
```

boundtype.xml (with 1 PC of pc2000 type and 1 PC of pc2400w type)

```
<rspec xmlns="http://www.protogeni.net/resources/rspec/0.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.protogeni.net/resources/rspec/0.1
http://www.protogeni.net/resources/rspec/0.1/request.xsd" type="request">
  <node virtual_id="my-node1" virtualization_type="emulab-vnode"
exclusive="1">
    <node_type type_name="pc2000" type_slots="1"/>
    <interface virtual_id="control"/>
  </node>
  <node virtual_id="my-node2" virtualization_type="emulab-vnode"
exclusive="1">
    <node_type type_name="pc2400w" type_slots="1"/>
    <interface virtual_id="control"/>
  </node>
</rspec>
```



```
sshalini@ubuntu: ~/protogeni/test
File Edit View Terminal Help
sshalini@ubuntu:~/protogeni/test$ python createsliver.py -n specificpc boundtype.xml
Got my SA credential
No such slice registered here:Creating new slice called specificpc
New slice created
Creating the Sliver ...
Created the sliver
<rspec xmlns="http://www.protogeni.net/resources/rspec/0.1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.protogeni.net/resources/rspec/0.1 http://www.protogeni.net/resources/rspec/0.1/request.xsd" type="request">
  <node virtual_id="my-node1" virtualization_type="raw" exclusive="1" component_urn="urn:publicid:IDN+emulab.net+node+pc38" component_uuid="de978c7c-773e-102b-8eb4-001143e453fe" component_manager_urn="urn:publicid:IDN+emulab.net+authority+cm" component_manager_uuid="28a10955-aa00-11dd-ad1f-001143e453fe" sliver_uuid="de978c7c-773e-102b-8eb4-001143e453fe" hostname="pc38.emulab.net" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9432">
    <node_type type_name="pc600" type_slots="1"/>
  </node>
</rspec>
```

boundtype.xml (with both PCs of pc600 type)

```
<rspec xmlns="http://www.protogeni.net/resources/rspec/0.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.protogeni.net/resources/rspec/0.1
http://www.protogeni.net/resources/rspec/0.1/request.xsd" type="request">
  <node virtual_id="my-node1" virtualization_type="emulab-vnode"
exclusive="1">
  <node_type type_name="pc600" type_slots="1"/>
  <interface virtual_id="control"/>
</node>
<node virtual_id="my-node2" virtualization_type="emulab-vnode"
exclusive="1">
  <node_type type_name="pc600" type_slots="1"/>
  <interface virtual_id="control"/>
</node>
</rspec>
```


Port Scanning

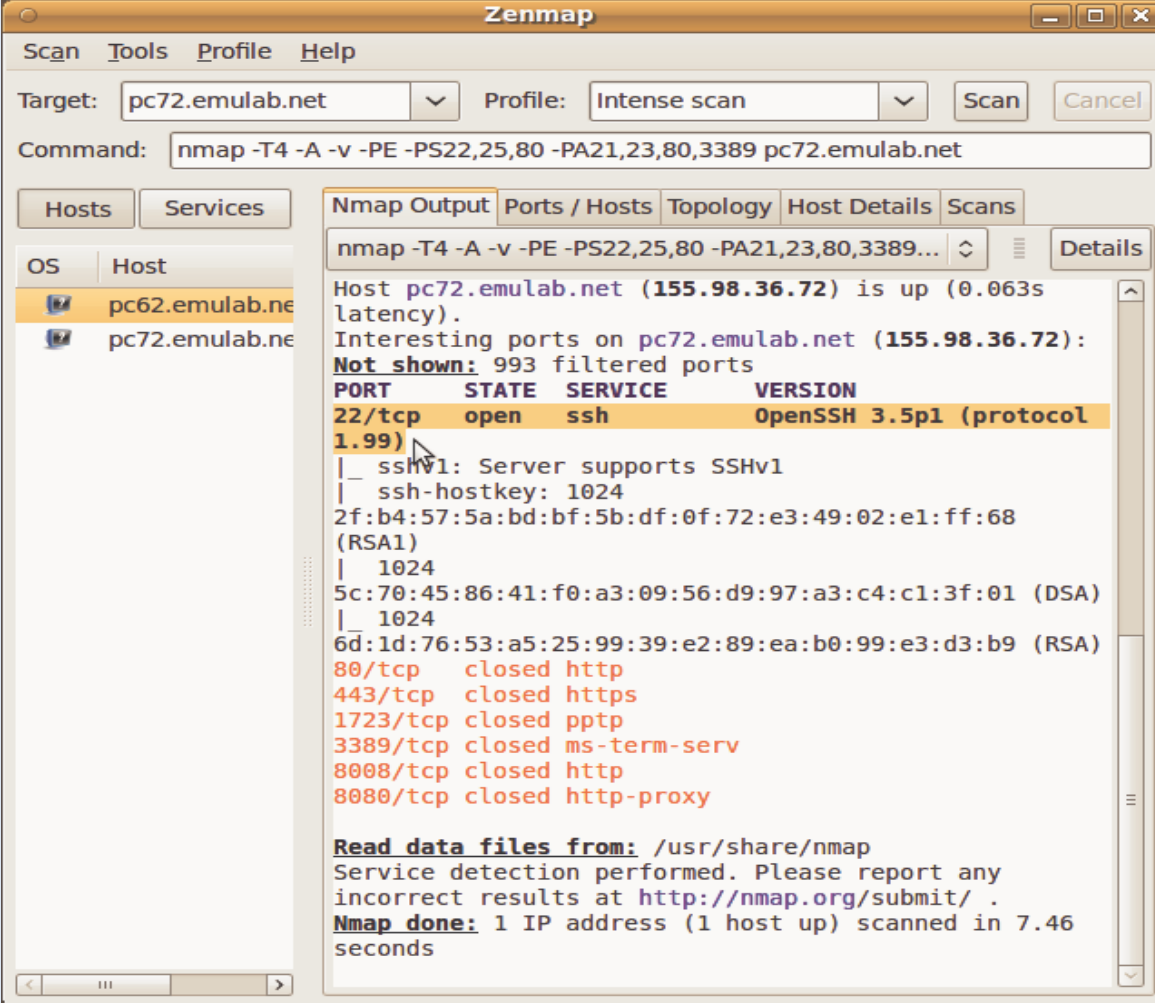
- Port scanning is a common method used by attackers to find out which ports are open and can be attacked.
- This experiment deals with scanning the ProtoGENI nodes both from outside ProtoGENI ie from our desktop and from within the nodes to check for open ports.

- First we scan the nodes from outside protoGENI i.e., from our desktop and check which ports are open in protoGENI that can be attacked.
- then, we login to the nodes and scan the node itself and the other node that we requested and check for the same thing.

Scanning for nodes from Outside ProtoGENI

- First we need to install a port scanner that can scan the nodes. In my experiment I used the NMap scanner.
- Scan the two nodes, i.e., geni1 and geni2 using their addresses.

Geni1 scanned by NMap scanner

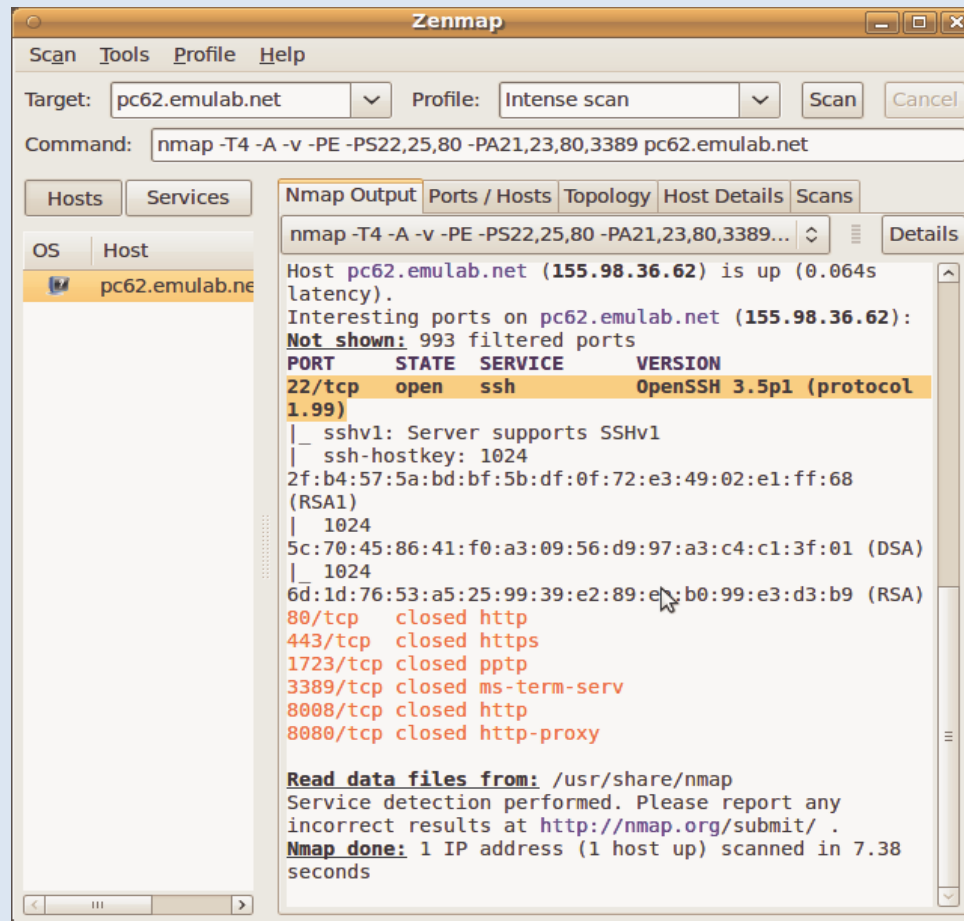


The screenshot shows the Zenmap application window. The target is set to `pc72.emulab.net` and the profile is `Intense scan`. The command entered is `nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 pc72.emulab.net`. The main output pane shows the following results:

```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389...
Host pc72.emulab.net (155.98.36.72) is up (0.063s latency).
Interesting ports on pc72.emulab.net (155.98.36.72):
Not shown: 993 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.5p1 (protocol 1.99)
|_ sshv1: Server supports SSHv1
|_ ssh-hostkey: 1024
2f:b4:57:5a:bd:bf:5b:df:0f:72:e3:49:02:e1:ff:68 (RSA)
|_ 1024
5c:70:45:86:41:f0:a3:09:56:d9:97:a3:c4:c1:3f:01 (DSA)
|_ 1024
6d:1d:76:53:a5:25:99:39:e2:89:ea:b0:99:e3:d3:b9 (RSA)
80/tcp    closed http
443/tcp   closed https
1723/tcp  closed pptp
3389/tcp  closed ms-term-serv
8008/tcp  closed http
8080/tcp  closed http-proxy

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.46 seconds
```


Geni2 scanned in Nmap scanner



Scanning for nodes from within ProtoGENI

- In this part of the experiment, we login to the node and scan itself and other nodes
- First we use the node1 ie Geni1 to scan itself and to scan the other node ie Geni2.

Geni1 scanning itself

```
File Edit View Terminal Help
[root@geni1 sneha]# nmap -A localhost
nmap: unrecognized option '-A'
Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[root@geni1 sneha]# nmap -sS localhost

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost (127.0.0.1):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp    open       ssh
25/tcp    open       smtp
111/tcp   open       sunrpc
32770/tcp open       sometimes-rpc3

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
[root@geni1 sneha]# exit
[sneha@geni1 ~]$ logout
Connection to pc72.emulab.net closed.
anil@anil:~$
```

Geni1 scanning geni2

```
root@geni1:~  
File Edit View Terminal Help  
anil@anil:~$ ssh -C sneha@pc72.emulab.net  
[sneha@geni1 ~]$ sudo /bin/bash  
[root@geni1 sneha]# nmap -sS pc62.emulab.net  
  
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )  
Interesting ports on pc62.emulab.net (155.98.36.62):  
(The 1599 ports scanned but not shown below are in state: closed)  
Port      State      Service  
22/tcp    open      ssh  
111/tcp   open      sunrpc  
  
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds  
[root@geni1 sneha]#  
[root@geni1 sneha]#  
[root@geni1 sneha]#  
[root@geni1 sneha]#  
[root@geni1 sneha]#
```


Geni2 scanning itself

```
anil@anil: ~
File Edit View Terminal Help
[root@gen1 sneha]#
[root@gen1 sneha]#
[root@gen1 sneha]#
[root@gen1 sneha]#
[root@gen1 sneha]#
[root@gen1 sneha]# exit
[sneha@gen1 ~]$ logout
Connection to pc72.emulab.net closed.
anil@anil:~$ ssh -C sneha@pc62.emulab.net
The authenticity of host 'pc62.emulab.net (155.98.36.62)' can't be established.
RSA key fingerprint is 6d:ld:76:53:a5:25:99:39:e2:89:ea:b0:99:e3:d3:b9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'pc62.emulab.net,155.98.36.62' (RSA) to the list of known
hosts.
[sneha@geni2 ~]$ sudo /bin/bash
[root@geni2 sneha]# nmap -sS localhost

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on localhost (127.0.0.1):
(The 1597 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open   ssh
25/tcp    open   smtp
111/tcp   open   sunrpc
32770/tcp open   sometimes-rpc3

Nmap run completed -- 1 IP address (1 host up) scanned in 2 seconds
[root@geni2 sneha]# exit
[sneha@geni2 ~]$ logout
Connection to pc62.emulab.net closed.
```

Geni2 scanning Geni1

```
anil@anil:~$ ssh -C sneha@pc62.emulab.net
[sneha@geni2 ~]$ sudo /bin/bash
[root@geni2 sneha]# nmap -sS pc72.emulab.net

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on pc72.emulab.net (155.98.36.72):
(The 1599 ports scanned but not shown below are in state: closed)
Port      State  Service
22/tcp    open   ssh
111/tcp   open   sunrpc

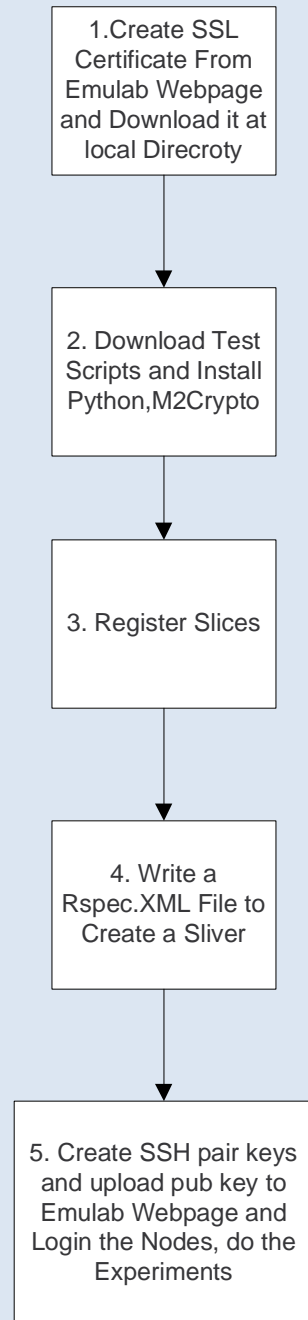
Nmap run completed -- 1 IP address (1 host up) scanned in 5 seconds
[root@geni2 sneha]#
```

Scan Result

- From the experiments conducted , it was seen that port 22 which is ssh port is open

Three Level Attacks

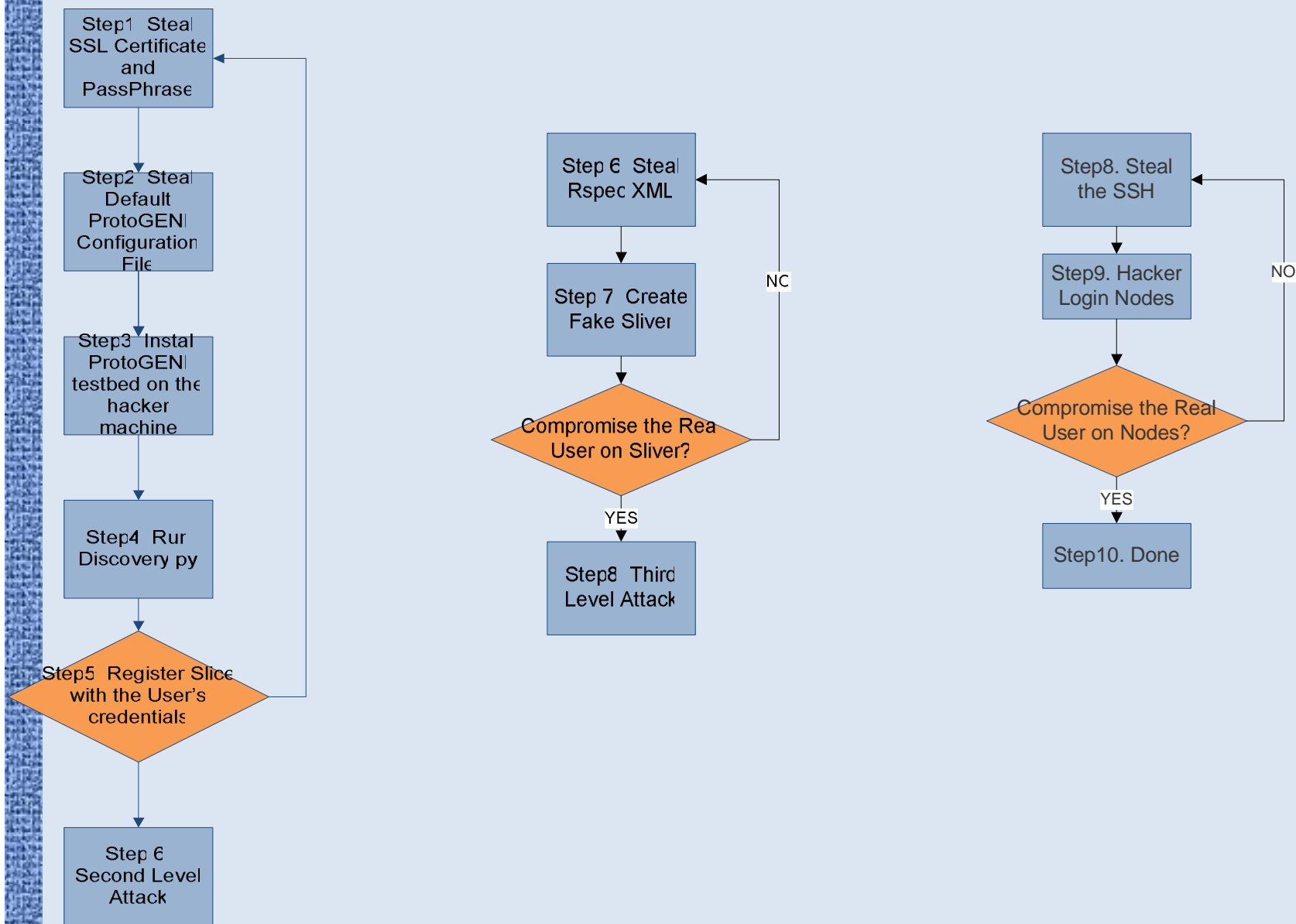
- Attack the ProtoGENI from both inside the nodes and outside nodes.
- Three levels on ProtoGENI, which are based on the procedure of interacting with ProtoGENI



How to Attack it

- one hacker Netinfinity[1] showed that if the hacker can combine a victim's shell with a port, then the hacker can connect and execute arbitrary commands on the victim's computer, without his knowledge.
- Thus, there is a remote shell available to the attacker. As most users are invariably logged in as root, it is highly probable that this would end up becoming a remote root shell.

3-Level Attack



First Level Attack

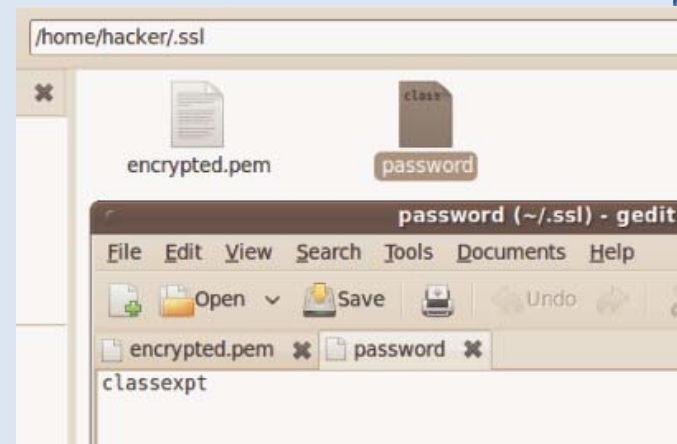
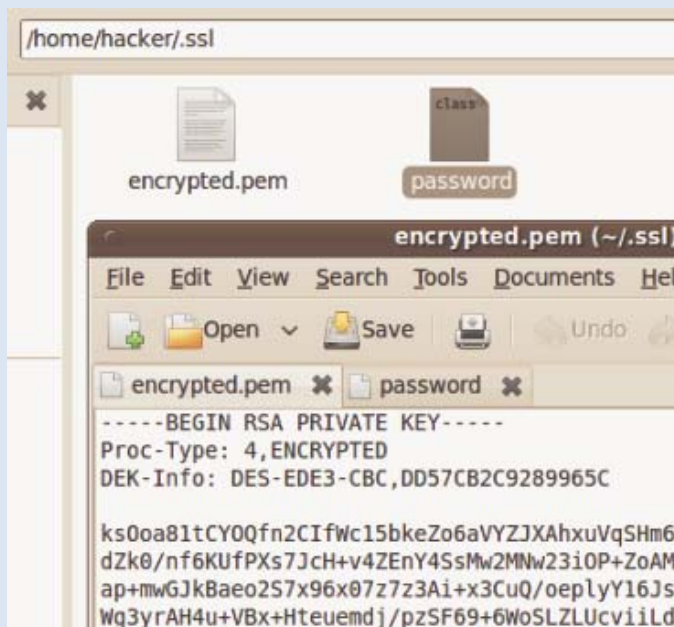
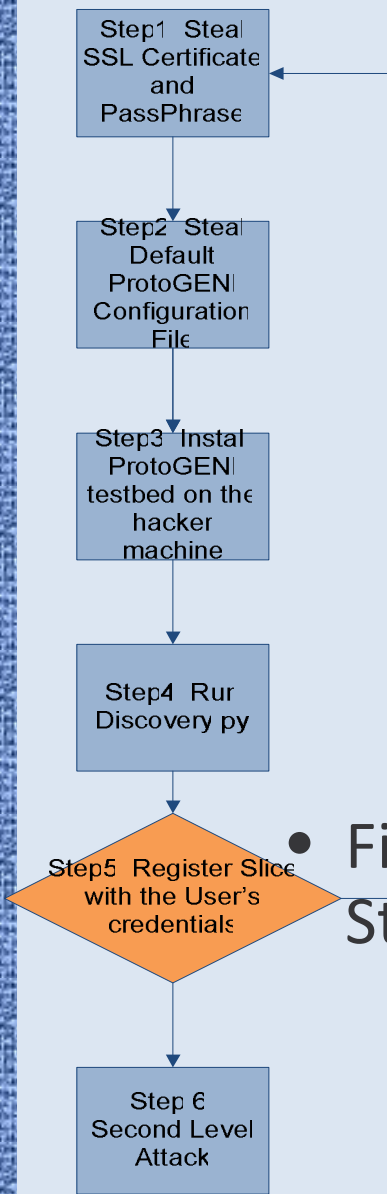
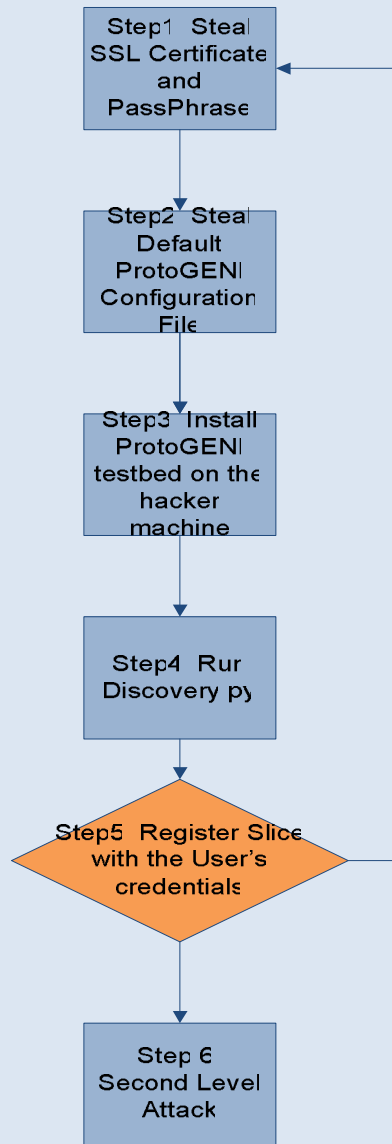


Figure 5. Setup the Stolen Passphrase

• Figure 4. Setup the Stolen SSL

First Level Attack

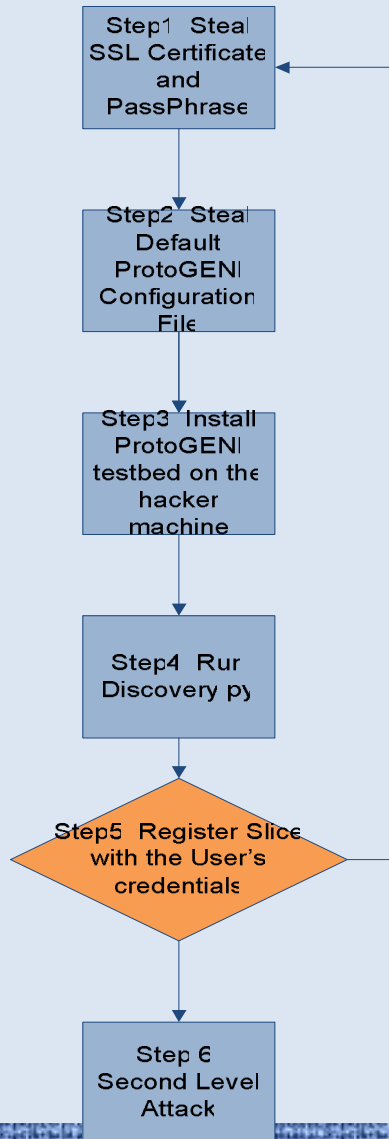


```
<link component_manager_uuid="urn:publicid:IDN+emulab.l
t_name="link-pc18:ath0-airswitch:air" component_uuid="
t+link+link-pc18%3Aath0-airswitch%3Aair" >
  <interface_ref component_node_uuid="urn:publicid:IDN+
component_interface_id="urn:publicid:IDN+emulab.net+inter
  <interface_ref component_node_uuid="urn:publicid:IDN+
" component_interface_id="urn:publicid:IDN+emulab.net+
  <bandwidth>54000</bandwidth>
  <latency>0</latency>
  <packet_loss>0</packet_loss>
  <link_type type_name="80211g" />
  <link_type type_name="80211b" />
  <link_type type_name="80211a" />
</link>
</rspec>

hacker@kofawp-desktop:~/ProtoGENI$
```

- Figure 6. Hacker Successfully Ran Discovery

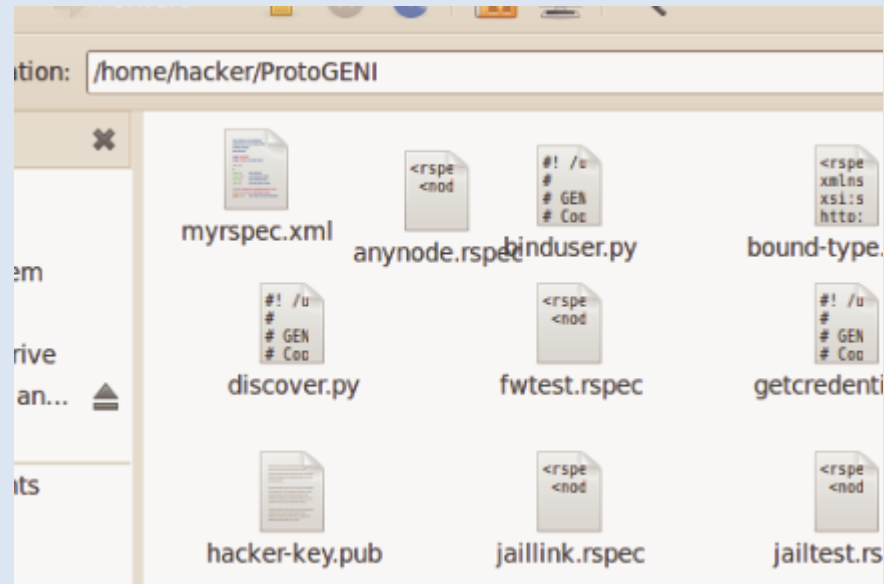
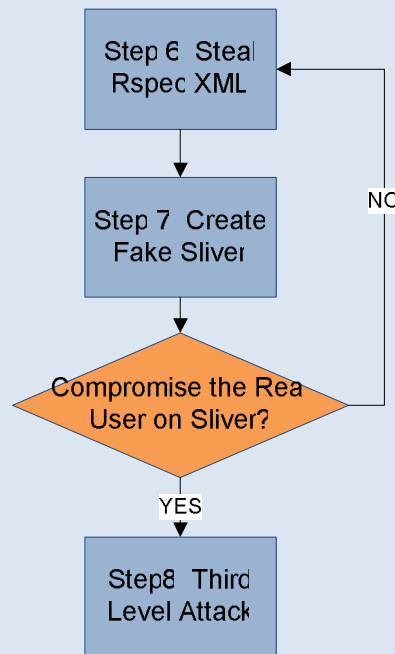
First Level Attack



```
kofawp@kofawp-desktop:~/protogenis python registerslice.py -n myslice
Got my SA credential
No such slice registered here:Creating new slice called myslice
New slice created
kofawp@kofawp-desktop:~/protogenis
```

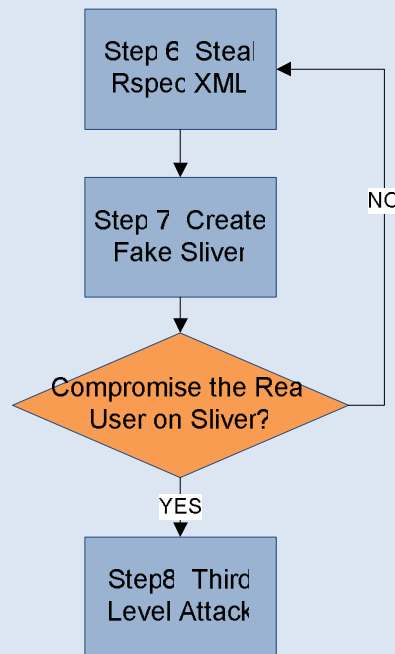
- Figure8. User Still can create a Slice after been hacked

Second Level Attack



- Figure 9. Stolen myrspec.xml

Second Level Attack



```
hacker@kofawp-desktop:~/ProtoGENIS python createsliver.py -n hackerslice myrspec.xml
Got my SA credential
Asking for slice credential for hackerslice
Got the slice credential
Creating the Sliver ...
Created the sliver
<rspec xmlns="http://protogeni.net/resources/rspec/0.1">

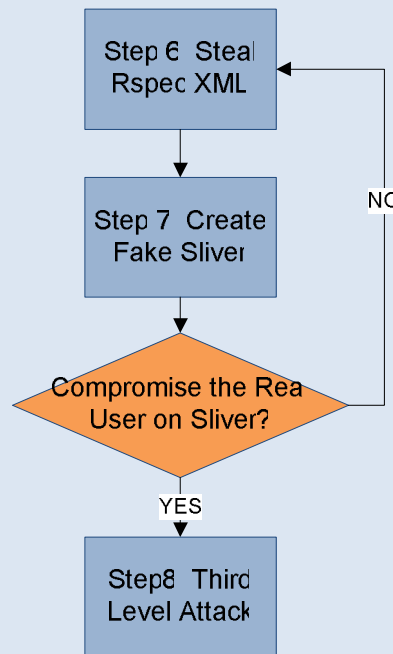
  <node virtual id="geni1" virtualization type="raw" exclusive="1" component urn="urn:publicid:IDN+emulab.net+authority+cn+de98f209-773e-102b-8eb4-001143e453fe" component manager urn="urn:publicid:IDN+emulab.net+authority+cn+de98f209-773e-102b-8eb4-001143e453fe" hostname="pc116.emulab.net" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9486">
    <interface virtual_id="virt0" component_id="eth3"/>
  </node>

  <node virtual id="geni2" virtualization type="raw" exclusive="1" component urn="urn:publicid:IDN+emulab.net+authority+cn+de994f1f-773e-102b-8eb4-001143e453fe" component manager urn="urn:publicid:IDN+emulab.net+authority+cn+de994f1f-773e-102b-8eb4-001143e453fe" hostname="pc165.emulab.net" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9487">
    <interface virtual_id="virt0" component_id="eth3"/>
  </node>

  <link virtual id="link0" sliver uuid="c2dbe45a-5be4-11df-ad83-001143e453fe" sliver urn="urn:publicid:IDN+emulab.net+sliver+9486">
    <interface ref virtual interface id="virt0" virtual node id="geni1" sliver uuid="urn:publicid:IDN+emulab.net+sliver+9486" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9486">
    <interface ref virtual interface id="virt0" virtual node id="geni2" sliver uuid="urn:publicid:IDN+emulab.net+sliver+9487" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9487">
    </link>
  </link>
</rspec>
hacker@kofawp-desktop:~/ProtoGENIS
```

- Figure 9. Hacker Created A Sliver

Second Level Attack

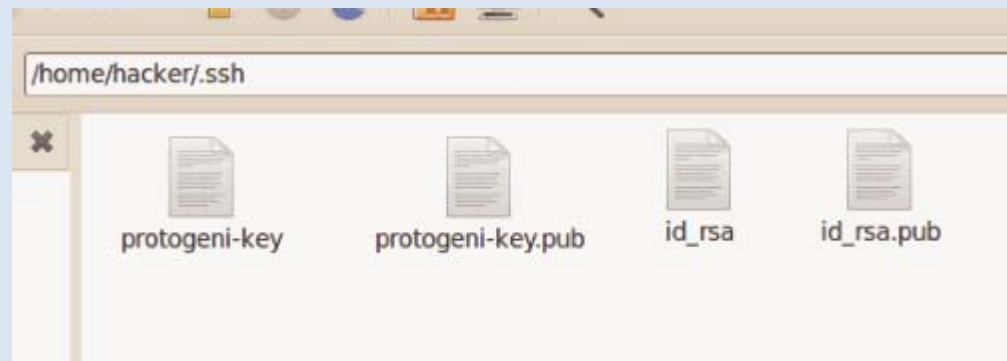
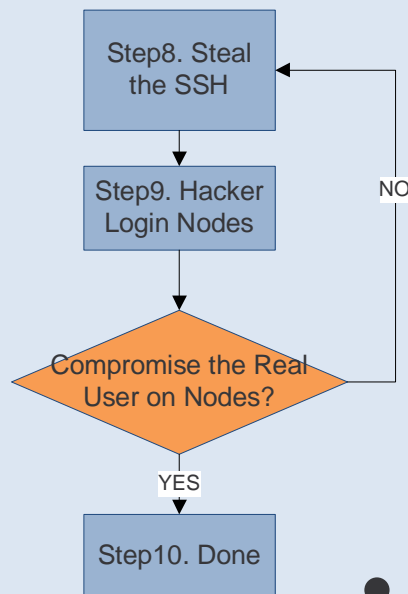


```
kofawp@kofawp-desktop:~/protogeni$ python createsliver.py -n myslice myrspec.xml
Got my SA credential
Asking for slice credential for myslice
Got the slice credential
Creating the Sliver ...
Created the sliver
<rspec xmlns="http://protogeni.net/resources/rspec/0.1">

  <node virtual_id="geni1" virtualization_type="raw" exclusive="1" component_urn="urn:
eb4-001143e453fe" component_manager_urn="urn:publicid:IDN+emulab.net+authority+cm" c
"de98dfdb-773e-102b-8eb4-001143e453fe" hostname="pc125.emulab.net" sliver_urn="urn:p
  <interface virtual_id="virt0" component_id="eth3"/>
</node>
  <node virtual_id="geni2" virtualization_type="raw" exclusive="1" component_urn="urn:
eb4-001143e453fe" component_manager_urn="urn:publicid:IDN+emulab.net+authority+cm" c
"de9942f4-773e-102b-8eb4-001143e453fe" hostname="pc158.emulab.net" sliver_urn="urn:p
  <interface virtual_id="virt0" component_id="eth3"/>
</node>
  <link virtual_id="link0" sliver_uuid="72fa1856-5be5-11df-ad83-001143e453fe" sliver_
  <interface ref virtual_interface_id="virt0" virtual_node_id="geni1" sliver_uuid="7
ab.net+interface+pc125:eth3" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9492" MA
  <interface ref virtual_interface_id="virt0" virtual_node_id="geni2" sliver_uuid="7
ab.net+interface+pc158:eth3" sliver_urn="urn:publicid:IDN+emulab.net+sliver+9493" MA
</link>
</rspec>
kofawp@kofawp-desktop:~/protogeni$
```

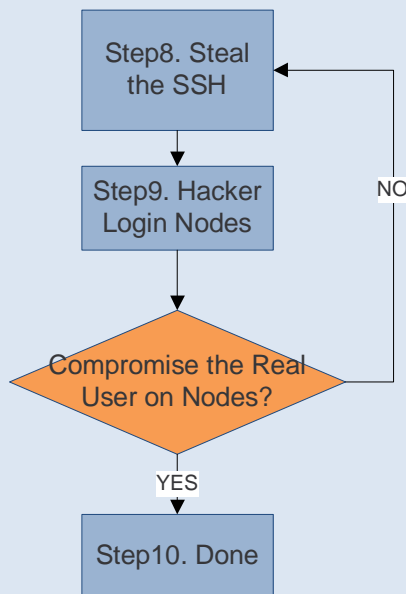
- Figure 10. User Created Sliver After Been Hacked

Third Level Attack



- Figure 11. Stolen SSH Key

Third Level Attack



```
</rspec>
kofawp@kofawp-desktop:~/protogenis$ SSH -C kofawp@pc264.emulab.net
SSH: command not found
kofawp@kofawp-desktop:~/protogenis$ SSH -C kofawp@pc264.emulab.net
SSH: command not found
kofawp@kofawp-desktop:~/protogenis$ ssh -C kofawp@pc264.emulab.net
The authenticity of host 'pc264.emulab.net (155.98.39.64)' can't be established.
DSA key fingerprint is 5c:70:45:86:41:f0:a3:09:56:d9:97:a3:c4:c1:3f:01.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'pc264.emulab.net,155.98.39.64' (DSA) to the list of known hosts.
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California. All rights reserved.

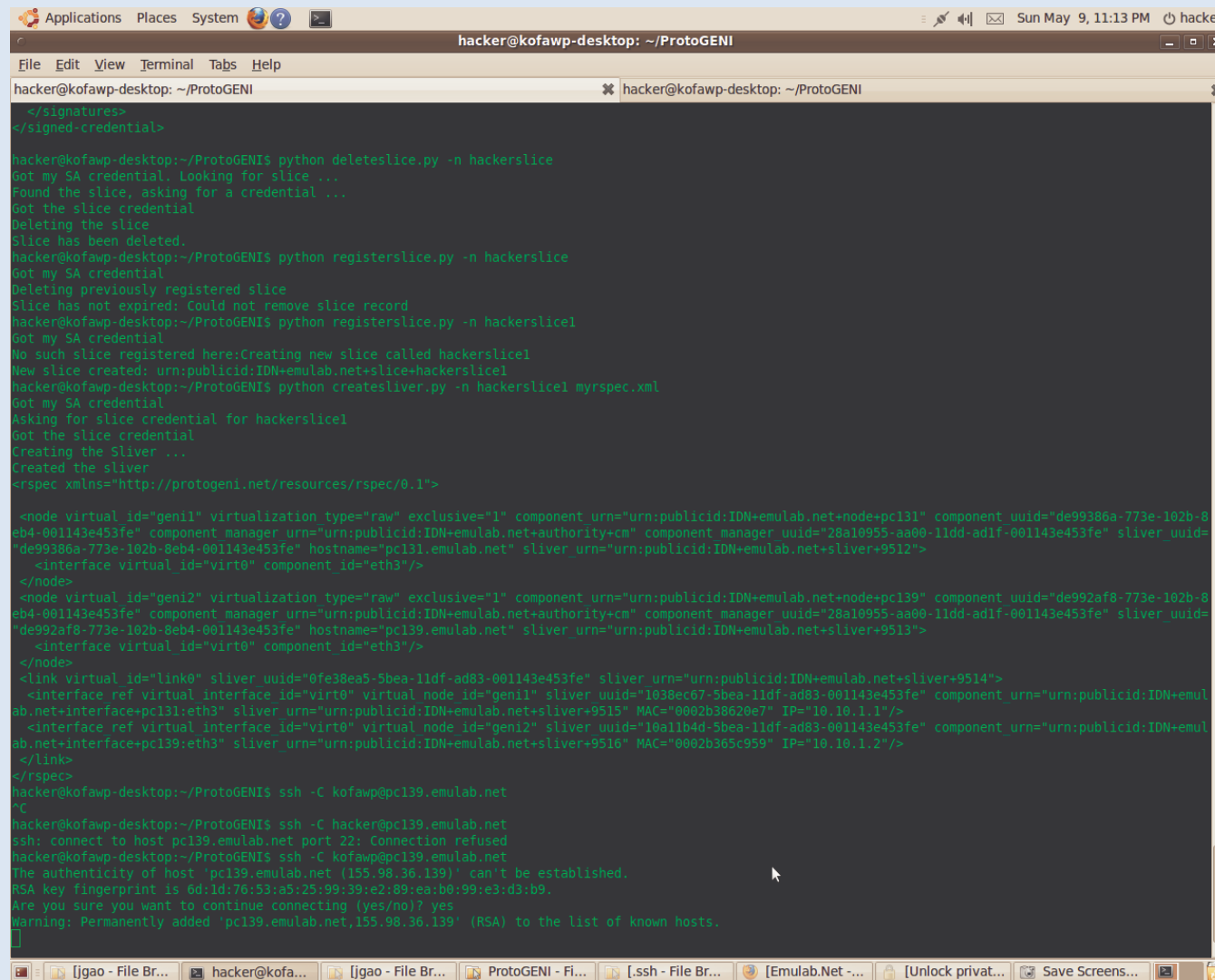
FreeBSD 4.10-RELEASE (TESTBED) #0: Mon Feb  2 15:49:28 MST 2009

Welcome to FreeBSD!

If you are in the C shell and have just installed a new program, you won't
be able to run it unless you first type "rehash".
-- Dru <genesis@istar.ca>
```

- Figure 12. User Login

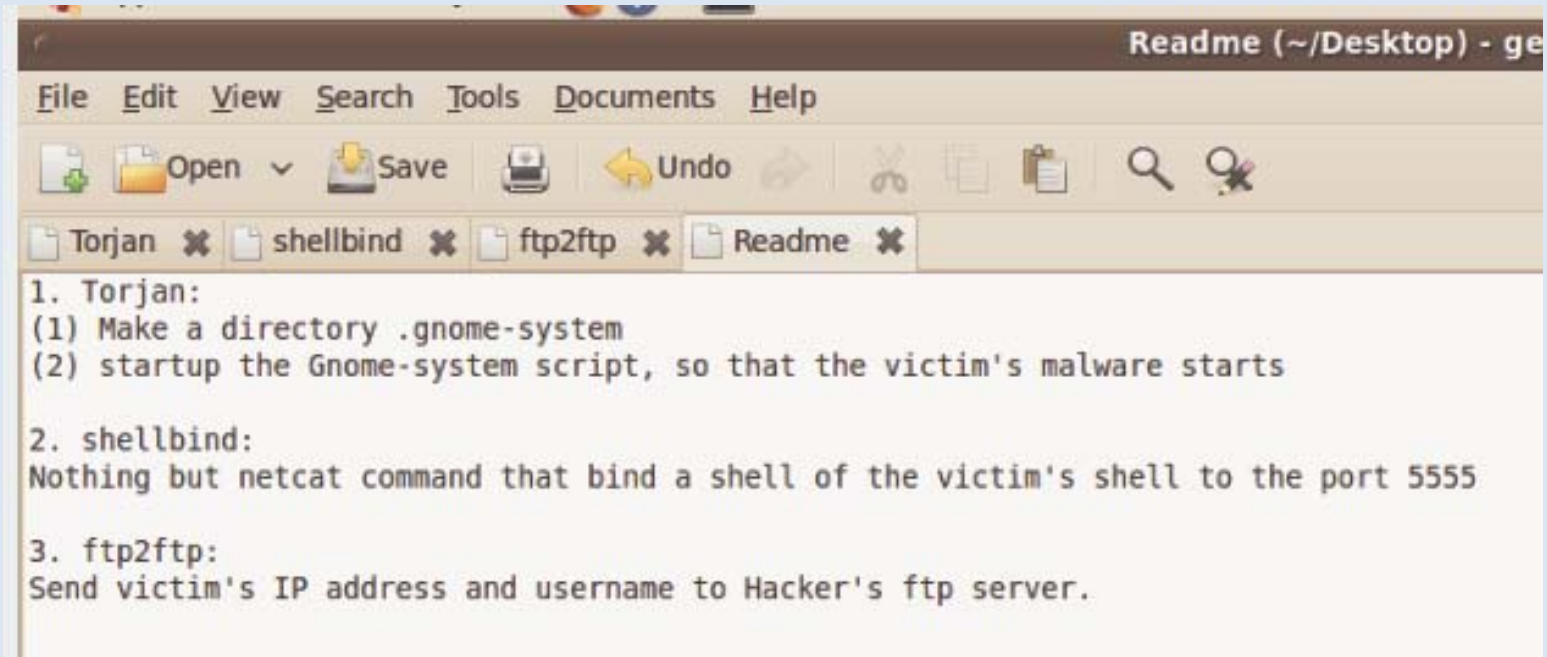
Third Level Attack



```
hacker@kofawp-desktop: ~/ProtoGENI
~/signed-credential>
~/signed-credential>
hacker@kofawp-desktop:~/ProtoGENI$ python deleteslice.py -n hackerslice
Got my SA credential. Looking for slice ...
Found the slice, asking for a credential ...
Got the slice credential
Deleting the slice
Slice has been deleted.
hacker@kofawp-desktop:~/ProtoGENI$ python registerslice.py -n hackerslice
Got my SA credential
Deleting previously registered slice
Slice has not expired: Could not remove slice record
hacker@kofawp-desktop:~/ProtoGENI$ python registerslice.py -n hackerslice1
Got my SA credential
No such slice registered here:Creating new slice called hackerslice1
New slice created: urn:publicid:IDN+emulab.net+slice+hackerslice1
hacker@kofawp-desktop:~/ProtoGENI$ python createsliver.py -n hackerslice1 myrspec.xml
Got my SA credential
Asking for slice credential for hackerslice1
Got the slice credential
Creating the sliver ...
Created the sliver
<rspec xmlns="http://protogeni.net/resources/rspec/0.1">
  <node virtual id="geni1" virtualization type="raw" exclusive="1" component urn="urn:publicid:IDN+emulab.net+node+pc131" component uuid="de99386a-773e-102b-8eb4-001143e453fe" component manager urn="urn:publicid:IDN+emulab.net+authority+cm" component manager uuid="28a10955-aa00-11dd-ad1f-001143e453fe" sliver uuid="de99386a-773e-102b-8eb4-001143e453fe" hostnames="pc131.emulab.net" sliver urn="urn:publicid:IDN+emulab.net+sliver+9512">
    <interface virtual id="virt0" component id="eth3"/>
  </node>
  <node virtual id="geni2" virtualization type="raw" exclusive="1" component urn="urn:publicid:IDN+emulab.net+node+pc139" component uuid="de992af8-773e-102b-8eb4-001143e453fe" component manager urn="urn:publicid:IDN+emulab.net+authority+cm" component manager uuid="28a10955-aa00-11dd-ad1f-001143e453fe" sliver uuid="de992af8-773e-102b-8eb4-001143e453fe" hostnames="pc139.emulab.net" sliver urn="urn:publicid:IDN+emulab.net+sliver+9513">
    <interface virtual id="virt0" component id="eth3"/>
  </node>
  <link virtual id="link0" sliver uuid="0fe38ea5-5bea-11df-ad83-001143e453fe" sliver urn="urn:publicid:IDN+emulab.net+sliver+9514">
    <interface ref virtual interface id="virt0" virtual node id="geni1" sliver uuid="1038ec67-5bea-11df-ad83-001143e453fe" component urn="urn:publicid:IDN+emulab.net+interface+pc131:eth3" sliver urn="urn:publicid:IDN+emulab.net+sliver+9515" MAC="0002b38620e7" IP="10.10.1.1"/>
    <interface ref virtual interface id="virt0" virtual node id="geni2" sliver uuid="10a11b4d-5bea-11df-ad83-001143e453fe" component urn="urn:publicid:IDN+emulab.net+interface+pc139:eth3" sliver urn="urn:publicid:IDN+emulab.net+sliver+9516" MAC="0002b365c959" IP="10.10.1.2"/>
  </link>
</rspec>
hacker@kofawp-desktop:~/ProtoGENI$ ssh -C kofawp@pc139.emulab.net
^C
hacker@kofawp-desktop:~/ProtoGENI$ ssh -C hacker@pc139.emulab.net
ssh: connect to host pc139.emulab.net port 22: Connection refused
hacker@kofawp-desktop:~/ProtoGENI$ ssh -C kofawp@pc139.emulab.net
The authenticity of host 'pc139.emulab.net (155.98.36.139)' can't be established.
RSA key fingerprint is 6d:1d:76:53:a5:25:99:39:e2:189:ea:b0:99:e3:d3:b9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'pc139.emulab.net,155.98.36.139' (RSA) to the list of known hosts.
[
```

- Figure 13. Hacker Can Not Login

the Program



The image shows a screenshot of a text editor window titled "Readme (~/Desktop) - ge". The window has a menu bar with "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". Below the menu bar is a toolbar with icons for "Open", "Save", "Undo", and other standard editing functions. The window contains a list of instructions for three different tools: Torjan, shellbind, and ftp2ftp. The text is as follows:

```
1. Torjan:  
(1) Make a directory .gnome-system  
(2) startup the Gnome-system script, so that the victim's malware starts  
  
2. shellbind:  
Nothing but netcat command that bind a shell of the victim's shell to the port 5555  
  
3. ftp2ftp:  
Send victim's IP address and username to Hacker's ftp server.
```


Three Level attack summary

- Credentials are possibly Stolen by hackers insert Trojan Horse into the victim's machine
- 3-Level Attack is proposed and tested
- Attack ProtoGENI is applicable, but takes too much effort, mainly because the unreliability of ProtoGENI itself right now.

Other Experiments

- Please see
 - ExptsSec-milestone3-findings-b.pdf (it will be posted on the project website)