Ghost Hosts :

Vivek Ramachandran
IIT Guwahati

Background :

One of the first steps taken by an experienced hacker to compromise a network is to chalk out it's network topology accurately . By network toplogy i mean the hosts which are up , the services they provide (open ports) , if they run a vulnerable service or not ?? also if a firewall protects them then what all does the firewall allow to pass through ??

This stage is also called "knowledge gathering" stage . It is only after this that any hacker worth his salt would proceed towards a more sophisticated attack .

Objective of my tool : Ghost Host

The motto of my tool is to provide a wrong topology of the network to any scanning procedure . Note that most corporate houses always have some free ip's in their allocated ip address space which are used by Ghost Host to put up virual hosts . I will put up "false hosts" which will reply to ARP replies , ping replies , scanning probes etc but never actually exist . These Ghost hosts may even be placed outside the firewall and impersonate valid hosts behind it . The ghost hosts will have open ports with maybe some vulnerable services so as to act as a honeypot which would attract any hacker towards an easy kill . Also when the hacker is trying to compromise this "ghost system" , his digital fingerprints will be backtraced to it's orign .

Working of this tool :

This tool once installed on a host will impersonate any host of choice , it binds to a specific ip address , hardware address as well as "virtually open" up some predefined ports . An ideal initialisation would be :

```
[root@ece19 root]# ./ghost_host eth0 202.141.82.21 a1:a2:a3:a4:a5:a6 -p 22,25,79
```

The above initialistaion would create a ghost host with ip 202.141.82.21 having a MAC a1:a2:a3:a4:a5:a6 with open ports 22 (ssh) , 25 (smtp) , 79 (finger) & 80 (http) .

Ghost_host starts sniffing the network for valid requests (arp , icmp and port scan probes) for the given ip and replies to them . Note that as a new MAC is also given to these ghost hosts hence the PC which is hosting these ghosts is never detectable .

The attacker totally beleives that this host is up with some vulnerable services and tries to connect, to it but fails as say for eg a syn to an open

port will return an ack and nothing else , thus the attacker tries and tries and finally fails . Note that during this period a backtracing is possible using other methods . The difference between a true host and a fake host is that , in normal cases it is tough to differntiate between legitimate connections and attack connections but in this case we can be sure that it is an attack as why would someone want to connect to a pc which actually never existed ??

Tool :

I have already written a beta version of this tool and it seems to work quite well . Another good point is that a host can very easily home dozens of such ghost hosts without any problem thus reducing even the necessity of adding new pc's which do this .