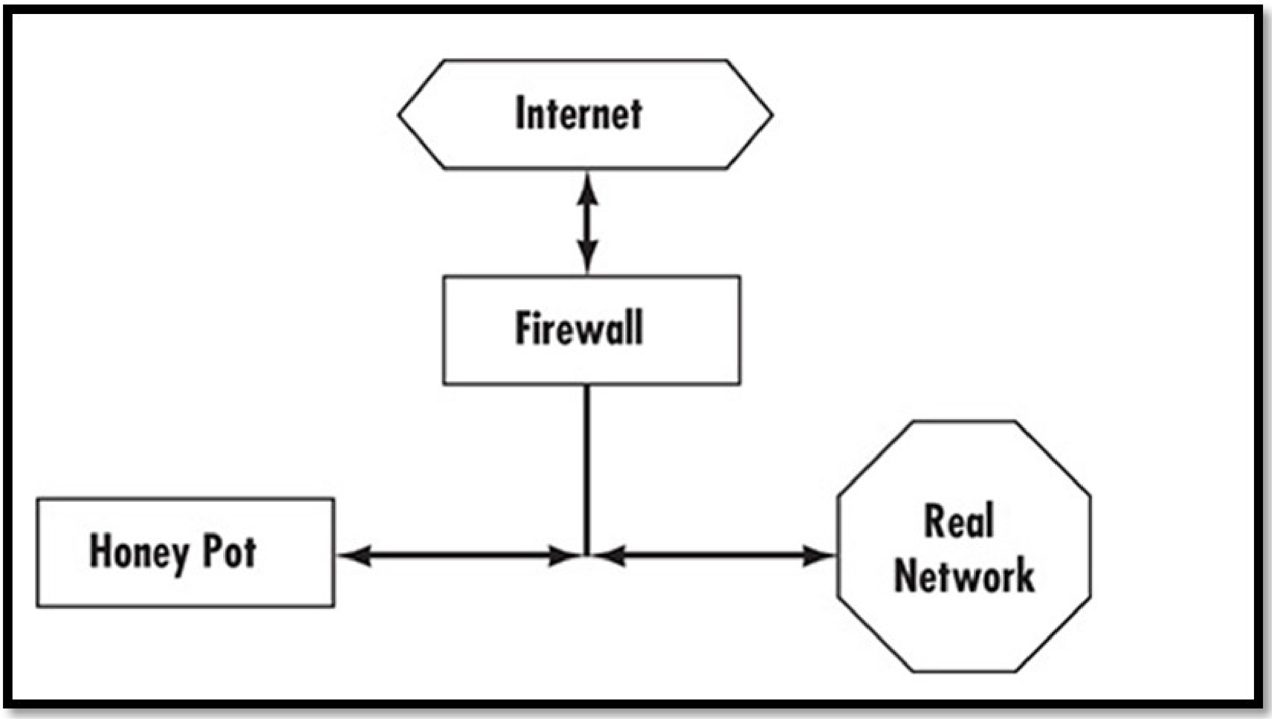
4.5 Honeypots

A honeypot is a single machine set up to simulate a valuable server or even an entire subnetwork. The concept is to make the honeypot so attractive that if a hacker breaches the network's security, he/she would be attracted to the honeypot rather than to the real system. The software can closely monitor everything that happens on that system, enabling tracking and perhaps identification of the intruder.

The underlying premise of the honeypot is that any traffic to the honeypot machine will be considered as suspicious. As the honeypot is not a real machine, no legitimate users should have a reason to connect to it. Therefore, anyone attempting to connect to that machine can be considered a possible intruder. The honeypot system can entice the potential hacker to stay connected long enough in order to trace where that person is connecting from. Figure 5-3 illustrates the honeypot concept.



4.5.1 Specter

Specter is a software honeypot solution. Complete product information is available at www.specter.com. The Specter honeypot is comprised of a dedicated PC with the Specter software running on it. The Specter software can emulate the major Internet protocols/services such as HTTP, FTP, POP3, SMTP, and others, thus appearing to be a fully functioning server. The software has been designed to run on Windows 2000 or XP but it will also execute on later versions of Windows. It can simulate AIX, Solaris, UNIX, Linux, Mac, and Mac OS X.

Specter works by appearing to run a number of services common to network servers. In fact, in addition to simulating multiple operating systems, it can also simulate the following services:

- SMTP
- FTP
- TELNET
- FINGER
- POP3
- IMAP4
- HTTP
- SSH
- DNS
- SUN-RPC

Even though Specter appears to be running these servers, it is actually monitoring all incoming traffic. Because it is not a real server for your network, no legitimate user should be connecting to it. Specter logs all traffic to the server for analysis. Users can set it up in one of five modes:

- Open: In this mode, the system behaves like a badly configured server in terms of security. The downside of this mode is that you are most likely to attract and catch the least skilful hackers.
- Secure: This mode makes the system behave like a secure server.
- Failing: This mode is quite interesting. It causes the system to behave like a server with various hardware and software problems. This might attract some hackers because such a system is likely to be vulnerable.
- Strange: In this mode, the system behaves in unpredictable ways. This sort of behaviour is likely to attract the attention of a more talented hacker and perhaps cause him to stay online longer trying to figure out what is going on. The longer the hacker stays connected, the better the chance of tracing him.
- Aggressive: This mode causes the system to actively try to trace back the intruder and identify his/her identity. This mode is the most useful for catching the suspected intruder.

In all modes, Specter logs the activity, including all information it can derive from the incoming packets. It also attempts to leave traces on the attacker’s machine, which can provide clear evidence for any criminal action. Users can also configure a fake password file in all modes. These are particularly useful because most hackers attempt to access a password file to crack the passwords. If they are successful, they can then log on as a legitimate user. The holy grail of hacking is getting the administrator’s password. There are multiple ways to configure this fake password file:

- **Easy:** In this mode the passwords are easy to crack, leading an intruder to believe that she has actually found legitimate passwords and usernames. Most of the times a hacker with a legitimate logon will be less cautious to cover their tracks. If you know that logon is fake and the system is set up to monitor it, you can track it back to the hacker.
- **Normal:** This mode has slightly more difficult passwords than the easy mode.
- **Hard:** This mode has even harder passwords to crack. There is even a tougher version of this mode called mean, in which the passwords are very difficult to break so that the hacker can be traced while he is taking time to crack the passwords.
- **Fun:** This mode uses famous names as usernames.
- **Warning:** In this mode the hacker gets a warning. He/she will then receive a message telling them that they have been detected if he/she is able to crack the password file. The theory behind this mode is that most hackers are simply trying to see if they can crack a system and do not have a specific objective. Letting this sort of hacker know he has been detected is often enough to scare them off.

4.5.2 Symantec Decoy Server

Because Symantec is such a prominent vendor for both antivirus software and firewall solutions, it should come as no surprise that it also has a honeypot solution. The first Symantec honeypot product was Decoy Server. It simulated a real server by simulating many server functions, such as incoming and outgoing e-mail traffic.

As the Decoy Server works as a honeypot, it also works as an IDS monitoring the network for signs of intrusion. If an attack is detected, all traffic related to that attack is recorded for later use in whatever investigative, criminal, or civil procedures that may arise.

Decoy Server is designed to be part of a suite of enterprise security solutions that work together, including enterprise versions of Symantec’s antivirus software, firewall software, and antispyware.