SIT327 - Network Forensics

Distinction Task 1: Flow Records Investigation

Overview

In this task we will use Nfsdump and Argus to examine firewall and flow records, to determine what happened during an attack.

Internet	DMZ	LAN
172.30.1.0/24	10.30.30.0/24	192.168.30.0/24

Nat Table	
External Address	Internal Address
172.30.1.231	10.30.30.20
172.30.1.227	192.168.30.101

Having examined the firewall logs, we will now look at the internal flows of our network. Using your knowledge of the IP that was attacked, and the NAT table above, see if you can see any unusual network flows in the internal traffic. You can discount all traffic on port 53 and 514 as administrative.

```
ra -z -nn -r argus-collector.ra - 'src host IP and not port 53 and not port 514'
 | more
```

Look through the list of events. The attack here went through two stages. What were those stages? If there was any success, what IP addresses were victimized? What application do you think was involved here?

Report Submission:

- What were the stages of the attack?
- What IPs were involved?
- How did the attacker try to make use of any open ports?
- Was the attacker successful?