# Investigating SSH port scans

This page provides a brief overview on how to deal with reported SSH scans **originating** from your own systems. It does not cover SSH scanning targeted at your systems and originating elsewhere.

Our netflow systems will from time to time detect hosts on Janet that appear to be sending a number of probes to the Internet, for systems listening on 22/tcp. The majority of these hosts will be port scanning for SSH services, with a view to performing a dictionary attack in the immediate to near future. In some cases the same host performs the dictionary attack, and in others the results of the port scan are transferred to other systems which later perform the dictionary attack.

Once we have detected this activity we will open an incident and send you information similar to the following:

```
An IP at Harwell College, 212.219.244.66 was scanning for port
22/tcp sending at least 18321 flows between 2010-08-
13T21:10:43+00:00 and 2010-08-13T21:42:26+00:00.

Log sample:
2010-08-13
21:11:03Z TCP 212.219.244.66:35556 -> 194.198.16.41:22 -A---F 1 52
21:11:03Z TCP 212.219.244.66:35357 -> 194.198.17.129:22 -A--SF 2 100
21:11:03Z TCP 212.219.244.66:60273 -> 194.198.16.12:22 -A---F 1 52
...
2010-08-13
21:41:11Z TCP 212.219.244.66:60246 -> 194.198.254.192:22 ----S- 1 60
21:41:12Z TCP 212.219.244.66:35930 -> 194.198.255.159:22 ----S- 1 60
21:41:12Z TCP 212.219.244.66:37777 -> 194.198.255.98:22 ----S- 1 60

Legend:
{start_day}{start_time}Z {protocol} {srcaddress}:{srcport} ->
{dstaddress}:{dstport} {str_tcp_flags} {dpackets} {doctets}
```

We may also send logs that have been sent to us by a third party, illustrating a dictionary attack against their systems:

```
Aug 30 18:50:35 gorgon sshd[429]: [ID 800047 auth.info] Failed
password for root from 212.219.244.66 port 37781 ssh2
Aug 30 18:50:35 gorgon sshd[429]: [ID 800047 auth.info] Failed
password for root from 212.219.244.66 port 37781 ssh2
```

The initial steps in your investigation should be to block the outbound SSH traffic from the source IP address, and then locate the originating host. For many networks this is a simple task, but it will be complicated by NAT and proxy devices if sufficient logging is not already in

place.

Experience has shown that these systems are usually, but not always, compromised through the same methods of the attacks originating from them. The source is a likely a Linux, OS X, or other UNIX system on which a poorly chosen password has allowed a successful dictionary attack against an account. Often the attack ends here and no attempt is made to gain root or administrative privileges.

The next step of the investigation should be to analyse the system to identify the process and user account sending the SSH probes, and locate the executable file used to launch the process. These should provide clues as to the extent of the compromise, and when and how it was compromised.

Using the information gathered so far, available logs on the system, and any network logs or netflow data, try to determine how the system was compromised. If root privileges were gained then you may not be able to trust the system logs. It may be useful to run a password auditing tool such as john the ripper against the system’s passwords, as weak passwords are such a common root cause of these incidents.

Once the source of the compromise has been found; consider mechanisms to protect against future compromise. Perhaps a required security patch was missing, or a strong password policy was not been properly enforced. Check similar systems within your organisation for similar vulnerabilities.

---