# I received a UDP reflection attack notice

## Q: I received a UDP reflection attack notice

## Answer

> Periodically, IS&T's Security Operations Team will scan MITnet for known bad behaviors that indicate a system compromise. When these behaviors are detected, notices are sent to registered host owners asking them to investigate and address the issue.

### Why did I receive this notification?

You received this notification because a host registered to you, or in your area of responsibility, was observed participating in a Denial of Service attack against other hosts on MITnet and/or the greater Internet.

### What triggers this alert?

A host on MIT's network sending out an exceptionally large volume of traffic using a known-and-frequently-abused UDP service. This behavior, called a UDP amplification attack, is used to overwhelm a victim system.

### What should I do?

If you have a locale IT support liaison, we recommend contacting them for support.

If you are the administrator of the host in question, we recommend you:

- disable the service if it's not necessary;
- adjust your firewall configuration so it only serves certain IP ranges;

If you do not have a local IT support liaison, you can contact the IS&T Help Desk.

### What if I have additional questions?

Additional questions can be directed to the IS&T Help Desk or the Security Operations Team.

### Notices sent out to host owners will be in the following format:

> Greetings,
>
> IS&T has observed activity which indicates a computer registered to you (or in your area of responsibility) is actively participating in a UDP-based Denial of Service attack that is impacting networks outside of MIT. The following computer is generating malicious and egregious amounts of $service_name traffic:
>
> Host: [HOST-NAME.MIT.EDU]
> IP Address: [18.1.2.3]
> Observed: [DATE]
> Behavior: [DESCRIPTION OF REFLECTION ATTACK]
>
> Please take steps to resolve this issue immediately.
>
> If you need assistance, please contact IS&T's Computing Help Desk (ist.mit.edu/help).
>
> Regards,
>
> Security Operations