



[Staff Only HOME](#)  
[Trouble Tickets](#)

- [Login screen](#)
- [Ticket list](#)

[ECS SPONG](#)  
[Student Schedule](#)  
[Create Account \(RATS\)](#)

[Web cameras](#)

- [DSV lab](#)
- [SRAC lab](#)
- [Machine Room](#)

[Backup](#)

- [Legato on thebrain](#)

[Network](#)

- [Engineering Router Graphs](#)

[Windows Services](#)

- [Windows](#)

# Installing, Configuring and Running find\_ddos

Written by: [Eddie Konczal](#)

Date: Nov 07 2000

Last updated: Sep 25 2001

## • About find\_ddos

The find\_ddos utility is provided by the [National Infrastructure Protection Center \(NIPC\)](#) for scanning UNIX filesystems for Distributed Denial of Service (DDoS) tools. It has been compiled for use at Rutgers by RUCS.

If the program "find\_ddos" generates a log file revealing unlawful access of a tested system, system administrators are encouraged to contact their local FBI field office or the NIPC. The [CIRT](#) division of RUCS has contacts at the FBI, so it may be desirable to go through them when reporting a DDoS-compromised system.

## • Installing find\_ddos

- Log on to target host
- **nslide**
- Create or verify that the following directory exists: /sos/tint.
- Verify that /sos/tint has access mode 775. If not, run **chmod -R 775 /sos**
- Mount the Tint server: **mount tint.rutgers.edu:/sos/tint /sos/tint**
- Change to the Tint packages directory: **cd /sos/tint/packages**
- Search for latest find\_ddos package:  
**ls -al | grep find\_ddos**. The latest package as of the writing of this document is **find\_ddos\_4.2\_RUSOS\_1**.
- Change to the scripts directory: **cd /sos/tint/bin**
- Install find\_ddos. Example: **./strap\_install /sos/tint/packages/find\_ddos\_4.2\_RUSOS\_1**
- A successful installation will result in the following messages (example):
  - Installing find\_ddos\_4.2\_RUSOS\_1
  - Done. find\_ddos\_4.2\_RUSOS\_1 has been installed
- If this installation of find\_ddos must be removed for any reason (e.g. to install a newer version), uninstall it by running: **/sos/tint/bin/strap\_remove /sos/tint/packages/find\_ddos\_4.2\_RUSOS\_1**
- If no more Tint packages are to be installed, unmount the server: **umount /sos/tint**.
- Exit the slide session and log out from the target host.

## • Configuring find\_ddos

[Services on Unix](#)

Rutgers  
Computational  
Grid

- [RCG statistics](#)
- [RCG web page](#)

Contacts

- [Rutgers](#)
- [Vendors](#)

Links to other sites

- [RU Open System Support](#)
- [TD subnets](#)
- [TD Spong](#)
- [DNS servers](#)



- Log onto target host
- **nslide**
- **cd /usr/local/find\_ddos**
- Review the README file: **more README**
- Create a directory for suspicious files to be located: **mkdir grab**
- Create a log file: **touch find\_ddos.log**
- Exit the slide session and log out from the target host.

- **Testing find\_ddos**

- Log onto target host
- **nslide**
- **cd /usr/local/find\_ddos**
- Run find\_ddos using the following syntax: **nice ./find\_ddos -g grab -l find\_ddos.log -p -y [scandir]**.
- *Explanation of syntax:*
  - **nice** is used because find\_ddos is highly resource intensive.
  - **-g grab** copies suspected DDOS tools to the /usr/local/find\_ddos/grab directory.
  - **-l find\_ddos.log** appends activity to the log file.
  - **-p** scans running processes.
  - **-y** accepts the disclaimer.
  - **[scandir]** defines the target directory or filesystem to be scanned. Specifying / as the scandir will scan the entire filesystem for DDOS tools. The **-x [exclude1]** argument will exclude directory "exclude1" from scanning.
  - Exit the slide session and log out from the target host.

- **Automating find\_ddos**

- Log onto target host
- **nslide**
- **cd /usr/local/find\_ddos**
- Determine location of sh shell: **which sh**. Typical results are "/usr/bin/sh" and "/sbin/sh".
- Create a shell script to run find\_ddos with the desired arguments. For example, create a text file **find\_ddos\_script** with the following text:
  - **#!/sbin/sh** #replace with correct path to sh
  - **cd /usr/local/find\_ddos**
  - **nice ./find\_ddos -g grab -l find\_ddos.log -p -y /**
- If the system is a mail server, append the argument "**-x /var/mail**" to the command line in the script that invokes find\_ddos. This is necessary since find\_ddos will alter the access time of mail files.
- Change the permissions on find\_ddos\_script to make it executable by root: **chmod 700 find\_ddos\_script**
- Edit the cron file for root: **crontab -e root**
- Create an entry in the root crontab to call the find\_ddos script at regular intervals. For example, the following entry in the root crontab will run the script find\_ddos\_script every Sunday night at 16:00 and mail the output to

root: **0 16 \* \* 0 /usr/local/find\_ddos/find\_ddos\_script 2>&1 | mail root**

- Save the crontab and exit the text editor. Verify the changes by running **crontab -l root**
  - Exit the slide session and log out from the target host.
- 

## HISTORY

- Nov 07, 2000 - Created document
  - Nov 08, 2000 - Corrected minor errors
  - Apr 18, 2001 - Included "-x /var/mail" option for mail servers
  - Sep 25, 2001 - Added "About find\_ddos" section
- 

