



[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](#)

Guidelines to Security Best Practices

Written by: [Eddie Konczal](#)

Date: 18-Jul-2001

Last updated: 19-Jul-2001

Guidelines to Security Best Practices

This document contains a list of recommended "best practices" for enhancing systems security. The list is presented in outline form and is a set of guidelines rather than formal policy. Staff members are encouraged to periodically review these guidelines and implement them where appropriate. The list is considered a "work in progress" and staff are encouraged to suggest additional best practices for inclusion.

Table of Contents

- [Subscribe to security bulletins](#)
- [Implement OS patches](#)
- [Implement applications patches](#)
- [Change passwords regularly](#)
- [Run McAfee Virus Scan on servers and workstations](#)
- [Scan for DDOS tools on UNIX workstations](#)
- [Review access logs regularly](#)
- [Maintain secure configuration of workstations \(in progress\)](#)
- [Install OpenSSH on publicly accessible servers \(in progress\)](#)
- [Install firewalls \(TBD\)](#)
- [Attend UNIX and PC administrator meetings](#)

Subscribe to security bulletins

The following is a sample of mailing lists that provide updates on security vulnerabilities:

- Rutgers administrators lists:
 - UNIX_ADMIN@EMAIL.RUTGERS.EDU
 - PC_LAN_ADMIN@EMAIL.RUTGERS.EDU
- SANS Weekly Security News Overview (sans@sans.org)

[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](#)



- Security Alert Consensus, Network Computing and the SANS Institute (<http://www.sans.org/sansnews/>)
- Sun Microsystems, Inc. Security Bulletin (security-alert@sun.com)

Implement OS patches

- Review patches announced via mailing list for Solaris, IRIX, Linux, and Windows
 1. Determine if patches are applicable to departmental systems
 2. Determine priority of incident and schedule task appropriately
 3. Download patches
 4. Test patches (if possible)
 5. Implement patches on servers and shared workstations
 6. Announce patches to user community if personal systems are affected.
- Install Solaris patches available from <http://Sunsolve.sun.com>
 - Install full patch clusters periodically (at least twice a year) on all Sun workstations
 - Install announced individual security patches on affected systems.
- Install Windows patches directly from <http://windowsupdate.Microsoft.com> (must use Internet Explorer 4.0 or later for automated web-based installation).
 - Run Windows Update periodically (at least twice a year) on Windows NT servers and lab workstations
 - Encourage PC users to run Windows Update periodically

Implement application patches

- Review patches announced via mailing list for cross-platform applications such as Apache, Sendmail, Samba, Internet Explorer, Netscape
 1. Determine if patches are applicable to departmental systems
 2. Determine priority of incident and schedule task appropriately
 3. Download patches
 4. Test patches (if possible)
 5. Implement patches on affected systems
- Announce patches to user community if personal systems are affected.

Change passwords regularly

- Change root and administrator passwords on central servers at regular intervals, and after departure of staff members in possession of root passwords.
- Keep passwords guarded in secure locations.
- Keep administrator access groups up to date.

Run McAfee Viruscan on servers and workstations

McAfee Viruscan is available for free for all University PCs. It can be downloaded from:
<http://mssg-ftp.rutgers.edu/mcafee.html>.

- Run McAfee NetShield on Windows NT servers.
 - Schedule regular (nightly or weekly) scans of all drives
 - Schedule automatic updates of virus definitions
 - Perform periodic scan engine updates.
- Run McAfee UNIX Viruscan on central UNIX file servers

This is documented at [uvscan.php3](#)

- Run McAfee Viruscan 4.5 on PC Lab workstations
- Regularly remind users to keep personal computers updated with latest McAfee software and virus definitions.

Scan for DDoS tools on UNIX workstations

- This is documented at [findddos.php3](#)
- If DDoS tools are found contact the local field office of the FBI or the NIPC (<http://www.nipc.gov/>)

Review access logs regularly

- Review access logs on UNIX systems and Event Viewer on Windows NT Servers to check for any unauthorized attempts to access systems.
- Report port scans or suspicious activity from external systems in the following manner:
 1. Determine the responsible person of the external host:

```
whois -h whois.abuse.net [external host]
```

2. Generate text output of the suspicious activity:

```
grep [external host]/var/adm/messages*
```

3. Report the suspicious activity to the responsible person. Copy abuse@rutgers.edu on the notice.

Maintain secure configuration of workstations (in progress)

- Make sure that automated installation tools and/or procedures for installing operating systems include the following steps for enhancing systems security:
 - Installation of most recent OS version (where applicable and licensed)

- Removal of unnecessary packages or bundled applications
- Installation of latest vendor patches
- Disabling of unnecessary services and ports
- Running system hardening scripts (e.g. Bastille Linux for Linux systems)
- Installing and configuring tcp wrappers for UNIX systems

Install ssh on publicly accessible servers (in progress) - this will eliminate the use of unencrypted passwords

- Install OpenSSH on publicly accessible servers.
- Inform user community on how to download, install and use alternatives to telnet/ftp (e.g. TTSSH, putty, MacSSH, OpenSSH client, etc.)
- Disable telnet/ftp access on publicly accessible servers

Install firewalls where appropriate

(Section to be done)

Make use of University resources for enhancing systems security

- Attend monthly UNIX and PC administrator meetings to learn about any University-wide initiatives involving systems security.
- Report root compromises, port scans, or other breaches of security to abuse@rutgers.edu
- Review the following web sites:
 - Open Systems Support: <http://oss.rutgers.edu/>
 - Computing Incident Response Team: <http://cirt.rutgers.edu/>

HISTORY

- Date created: 18-Jul-2001
 - Updated: 19-Jul-2001
-