

Security Essentials for Fermilab System Administrators

Why Computer Security?

Civilization is Risk.
-- Not Big Brother

Why Computer Security?

Civilization is Risky.



Dealing With Risk

Recognize | Reduce | Recover



Recognizing Risks

High Bandwidth
Enormous Storage
Push *.gov* Location

Nothing Marketable



Recognizing Risks

High Bandwidth
Enormous Storage
Push *.gov* Location

Nothing Marketable*



Recognizing Risks

IP & *warez*

SPAM

Malware

Botnets

DDoS attacks



Recognizing Risks

Stolen Credentials

Destruction Of Data

Waste Of Bandwidth

Waste Of Time

Frustration



Recognizing Risks

Default root/admin privs

Visiting malicious sites

Watering Hole infections

Visitor systems

Promiscuous USB sharing

Lack of gruntlement



Recent News

LinkedIn & other password hashes

Stuxnet/Duqu/Flame

Flashback/SabPub

Trojan-Downloader:Java/GetShell.A



Critical Vulnerabilities

- 12/2011: telnetd remote code execution
- 03/2012: RDP vulnerability (MS12-020)
- 06/2012: Cumulative IE (MS012-037)
- 06/2012: CERN/FNAL Hypernews
- 10/2012: ColdFusion



TLAs for TCB: ISM? DID.

Integrated Security Management (ISM)

Defense In Depth (DID)



Recognizing Risks: ISM

Computer Security not an add-on
Not "one size fits all"
Largely common sense



DID: Perimeter Controls

Protocols blocked at border

Proxies

Transient blocks

Mail virus scanning



DID: Central Authentication

Primary passwords off the net

Single turn-off point

No visible services w/o Strong Auth

Lab systems scanned for compliance



DID: Services Accounts

Unkerberizable:

Service Now

Kronos

Exchange

...



Patch/Configuration Mgmt

Baselines: Linux, Mac, Windows

All systems must meet their baseline

All systems must be regularly patched

Non-essential services off

Windows, especially, must run AV



Patch/Configuration Mgmt

Exceptions/Exemptions:

Documented case why OS is "stuck"

Patch and manage as securely



Grid Security Training

Grid Sysadmin

GUMS/VOMS Admin

Griddleware Developer

Security Essentials for Grid
System Administrator



Major Applications

Critical to the mission of the Laboratory
Most things do not fall in this category
Very stringent rules & procedures
You'll know if you're in this category



Minor Applications

Important to the mission of the Laboratory

Most things do not fall in this category

Stringent rules & procedures

You'll know if you're in this category



Anti-Virus

Windows & Mac Baselines

Linux with Samba/CIFS

Central Update Server & Logging

Respond to alerts!



Central Logging

Use clogger

Attackers will sanitize local logs

Aids forensic investigations

Problems may get noticed earlier



Critical Vulnerabilities

Active exploits declared critical

Pose a clear and present danger

Must patch by a given date or be blocked

Handled via Tissue events

Similarly, OS End-Of-Life



AV Alerts & Automatic Blocking

Some bad viruses cause an immediate block
May require a "Wipe & Reinstall"
If not, a thorough scan is performed
May be returned to service, if successful
Inconvenience is unavoidable, alas



Computer Security Incidents

Report suspicious/urgent events to x2345

or email computer_security@fnal.gov

Follow FIR instructions during incidents

Keep infected machines off the network

Preserve system for expert investigation

Not to be discussed!



Fermi Incident Response (FIR)

Triage initial reports

Coordinate investigation

Work with local Sysadmins, experts

May take control of affected systems

Maintain confidentiality



Prohibited Activities

Blatant disregard of computer security

Unauthorized or malicious actions

Unethical behavior

Restricted central services

Security & cracker tools

<http://security.fnal.gov/policies/cpolicy.html>



Mandatory Sysadmin Registration

All Sysadmins must be registered
Primary Sysadmin is responsible for
configuring and patching

<http://security.fnal.gov> ->

"Verify your node registration"



Sysadmins Get Risk-Roled

System manager for security

Assist and instruct users to do it right

Vigilant observer of your systems

(and sometimes users') behavior



Role of Sysadmins

Manage your systems sensibly, securely

Services comply with Strong Auth rules

Report potential incidents to FIR

Act on relevant bulletins

Keep your eyes open



Protecting Your Systems

Shut off unneeded services

Set up needed services properly

Set up a suitable firewall

Keep informed & patched on OS issues

Use clogger



Users: We Get Mail

You haven't won £10 Million

Don't open (most) attachments

Best not to click links in mail

Disable scripting for mail



Users: Pass the Word

Use strong passwords

Longer is better

Use different passwords

Or *variants*, at least



Other Duties As Assigned

Guard against malicious web code

Protect your Kerberos password

Report possible security incidents x2345

or email computer_security@fnal.gov

(if it's not urgent)



Data Backup Policy For Users

Decide what data requires protection
How to be recovered, if needed
Arrange backups with Sysadmins
Or do your own backups
Occasionally test retrieval



The Incidental Computist

Some non-Lab-business use is allowed:
<http://security.fnal.gov/ProperUse.htm>

(I prefer personal iPhone/iPad/Droid
via an external network ...)



Activities to Avoid

Anything that:

- Is illegal

- Is prohibited by Lab/DOE policy

- May embarrass the Lab

- Interferes with job performance

- Consumes excessive resources



Activities to Avoid

Services like Skype and BitTorrent
not forbidden but very easy to misuse!



Data Privacy

Generally, Fermilab respects privacy
You are required to do likewise
Special cases for Sysadmins during
Security Incidents
Or *written* Directorate approval



Privacy of Email and Files

May not use information in another person's files seen incidental to any activity (legitimate or not) for any purpose w/o explicit permission of the owner or "reasonable belief the file was meant to be accessed by others."



Offensive Materials

Material on computer \approx Material on desk
A line management concern
Not a computer security issue *per se*



Software Licensing

Fermilab is strongly committed to respecting intellectual property rights. Use of unlicensed commercial software is a direct violation of lab policy.



Summary: User Responsibilities

Appropriate use of computing resources

Prompt incident reporting

Proper PII handling (separate training)

Know how your data is backed up

Respect privacy of electronic information



Summary: Admin Responsibilities

System registration

AV, patching, configuration mgmt

Strong Authentication access control

No restricted services (email, dns, etc.)

Questions?

nightwatch@fnal.gov

for questions about security policy

computer_security@fnal.gov

questions about security incidents

<http://security.fnal.gov/>

Security Essentials for Fermilab System Administrators