OS Hardening

An unsung hero

By Ryan Nolette

Agenda

- Who am I and what do I do?
- What is OS hardening?
- Hardening Basics
- Examples of OS hardening steps and their benefits
  - Identify Management (IM)
  - User Access Control (UAC)
  - Logging and Scripting
    - Securing SSH
    - Logging all users bash history in real time
    - Elevated privilege monitoring
- Recap and Questions

$whoami

- My name is Ryan Nolette
- I am currently the Security Operations Lead at Carbon Black
  - Manage Security Operations (SecOps)
  - Act as Senior Security Architect for Carbon Black
- I am a 10+ year veteran of IT, Incident Response, Threat Intelligence, and Computer Forensics
- Carbon Black blog link
  - https://www.carbonblack.com/author/ryan-nolette/
- Responsibilities:
  - Monitor Endpoint Events, Network Based Events, and Physical Security Events
  - User Education and Outreach
  - IT Oversight and Assistance
  - Security Oversight of Enterprise Projects
  - Incident Response
  - System Forensics
  - Vulnerability and Risk Assessments
  - Threat Research
  - ETC

What is OS hardening?

Hardening is the process of securing a system by reducing its surface of vulnerability

Hardening Basics

- Hardening guidelines/tools examples
  - Automated tools
    - Bastille
    - Lynis
    - CIS Toolkit
    - Tripwire
  - Guidelines
    - NIST
    - CIS
    - STIG
    - Cat I/II/III
  - Scripting/Custom solutions

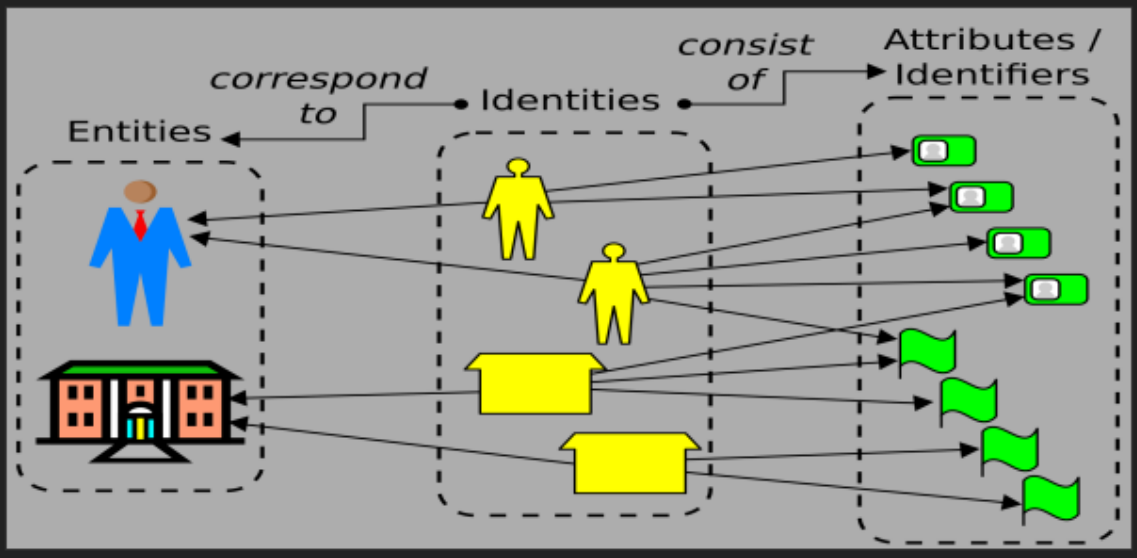
OS hardening steps and their benefits

Who

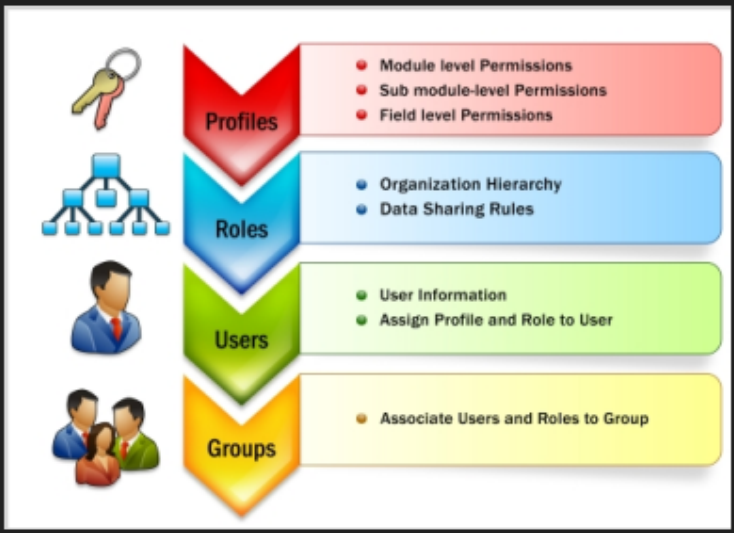
Identity Management

1. Verify users in a system
2. Control access to resources within that system
3. Associate privileges and restrictions with the established identity

Identity Management



User access control



- UAC helps prevent unauthorized changes to a system.
- These changes can be initiated by applications, viruses or other users.
- UAC makes sure changes are made only with approval of a privileged user.
- If the changes are not approved by a privileged user, they are not executed and system remains unchanged.

What

Logging


SYSLOG
ALL THE THINGS!
RSYSLOG ALL THE THINGS
scribe
elastic
kibana
logstash
splunk
Finding your faults, just like mom.

Securing SSH

#if you run a command through SSH directly without going interactive (EX: ssh root@system COMMAND), the command won't be logged anywhere.

#this line will fix that

```
ForceCommand if [[ -z \$SSH_ORIGINAL_COMMAND ]]; then bash; else printf "\x23\`date +%s\`\n\$SSH_ORIGINAL_COMMAND\n" >> .bash_history; bash -c "\$SSH_ORIGINAL_COMMAND"; fi
```

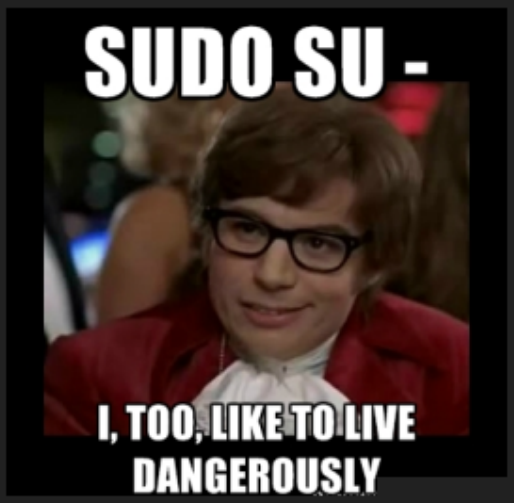
```
## Enforce SSH Protocol 2 only. More security options
Protocol 2

## Disable direct root login,
PermitRootLogin no

#allows use of username and passwd for authentication
PasswordAuthentication yes

#allows use of ssh keys for authentication
PubkeyAuthentication yes

#verbosity of logging
LogLevel INFO

#do not allow authentication without a password
PermitEmptyPasswords no

## Add users or groups that are allowed to log in
AllowGroups serveradmins applcationadmin
```

Logging all users bash history in real time

```
echo "--- Enabling Real time bash_history for all current users ---"
for user in `ls /home`; do
        echo 'export HISTCONTROL=ignoredups:erasedups  # no duplicate entries' >> /home/$user/.bashrc
        echo 'export HISTSIZE=100000                   # big big history' >> /home/$user/.bashrc
        echo 'export HISTFILESIZE=100000               # big big history' >> /home/$user/.bashrc
        echo 'export HISTTIMEFORMAT="%m/%d/%y %T "     # Add timestamp' >> /home/$user/.bashrc
        echo "shopt -s histappend                      # append to history, don't overwrite it" >> /home/$user/.bashrc
        echo '# After each command, append to the history file and reread it' >> /home/$user/.bashrc
        echo 'export PROMPT_COMMAND="history -a; history -c; history -r; $PROMPT_COMMAND"' >> /home/$user/.bashrc
done
```

Elevated privilege monitoring

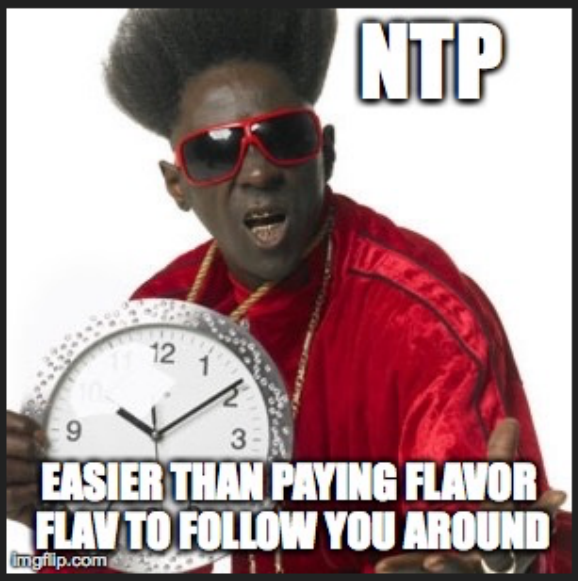
#This will allow auditd to get the calling user's uid correctly when calling sudo or su.
echo -e "session\trequired\tpam_loginuid.so" >> /etc/pam.d/login
echo -e "session\trequired\tpam_loginuid.so" >> /etc/pam.d/gdm
echo -e "session\trequired\tpam_loginuid.so" >> /etc/pam.d/sshd



When

Centralized Time Server

- A time server distributes the actual time from a reference clock to its clients.
- The time server may be a local network time server or an internet time server.
- Having a single point of time to work from across the enterprise allows for an accurate timeline of events in logs and in investigations.



Recap

- OS hardening is about reducing risk and the vulnerability surface of a system.
- You do this through policy and technological controls aimed at increasing visibility and accountability
- This is broken down further into 3 questions for every event. Who did What and When.

Conclusion and Questions