Liasing with CERT Teams and logging

David Ford, OxCERT

Oxford University Computing Services

www.oucs.ox.ac.uk

What is a CERT?

- A Computer Emergency Response Team
- A team of people dedicated (in some sense) to dealing with computer security incidents

What is a CERT?

- Typically responsible (at least) for
- processing reports of abuse, liaising with external bodies and identifying potential incidents
- part of the initial investigation into an incident
- reporting and providing, providing guidance on the process of cleaning systems
- may well have some powers to isolate systems

How can they help?

- A CERT Team may well have logs which can be correlated with yours to identify what happened and when attackers got in
- They will have seen similar incidents before, so may be able to warn you of potential pitfalls with cleaning systems
- They may be able to advise you of the risks and extent of a compromise

Oxford University Computing Services
www.oucs.ox.ac.uk

How can you help them?

- Typically their focus will be on ensuring that the full extent of the incident is known as soon as possible
- NOT on "papering over the cracks" and getting something back up and running
- frequently one machine may be noticed as compromised, but there may be several machines with the same vulnerability

How can you help (2)

- Ensuring adequate logging exists and that the appropriate logs are available as soon as possible (either for you to analyse or for the CERT team) is critical
- Make sure you have the correct contact details registered - all too often incidents go through several steps before the appropriate administrator is found - you may want to have a security email address that contacts all cluster admins in a group

Oxford University Computing Services

www.oucs.ox.ac.uk

The typical process in Oxford

- Usually (although not always), we notice, or are informed from an external source of a compromised system.
- We will perform a preliminary analysis to verify the data we’re given, or to identify whether a system seems to be compromised. At this stage the analysis will be quite quick and will not identify all the details we may be able to find.

- Once we are confident we have a genuine (and sufficiently serious) incident which needs attention, we will take action, normally in the form of a router block - this will isolate the system from anything outside its own subnet.
- At this stage we notify the administrators

Sample notification

Hello,

A router block has been set-up for the following IP address:

163.1.1.1
example.ox.ac.uk

Reason: System was detected scanning on port 22

Could you please check the system(s) and let us know when you want the block to be removed? Please include above details in your reply.

What now?

- The systems administrators look at the system
- We also continue to look at the logs - this time in more detail
- Our aim to determine:
  - When was it compromised
  - Via what port/service
  - Did the attackers get elsewhere

- We can see some of this from our logs
- But we need the assistance of the local IT support to look at the logs from local systems
  - What account(s) were compromised
  - Were these present elsewhere
  - What access did those accounts give - sudo, ssh keys, was the system patched
  - Did the attackers succeed in elevating privileges (often impossible to tell)
- This process may then need repeating elsewhere

Then...

- Only once we're confident we know how the attackers got in, what access they gained, and what information they may have stolen can we begin the process of rebuilding
- In many cases we can never be sure privileges were not escalated, so it comes down to a case of assessing the risks.

The clean up

- Once the systems are rebuilt, and the holes that were exploited are filled, the process of removing blocks can commence
- In the case of major mass compromises this may often be done in stages - but beware, there may be compromised systems behind your firewall trying to attack your cleaned systems! It's strongly recommended to ensure the infected systems are isolated before rebuilding commences

When should you contact the CERT?

- In the event of any security incident - even if you're already dealing with it
- There's no benefit in duplicating work - they may spot it at some point
- If accounts/ssh keys/passwords have been compromised the CERT team may be able to alert other units

What else can the CERT do?

- The CERT team may be able to locate other systems attacked in the same way
- They may find copies of the malicious code useful - it can help generate signatures to spot future attacks, or to identify attackers to keep an eye on

Improving the process

- Centralised logging is extremely helpful when a host gets compromised, it reduces the risk of logs being tampered with when an end user system is compromised
- Lock down log servers
  - do they actually need port 22 open?
  - restrict access to people who actually need access to the logs, and don't put ssh keys on the grid nodes different passwords help too

Other things

- if your cluster is behind a NAT, logging NAT translations helps in tracing abuse, and may reduce the chance of an entire NAT being blocked when a single system is compromised
- Make sure logs are NTP synchronised, and make sure your NTP source is accurate

- discuss log retention policies with your local CERT or it may be defined in local policies
- We often find that incidents are not discovered until long after they first happen - this makes it important to keep logs for several months
- Consider backups of your log server in case of compromise

Other policy issues

- A lot of compromises are caused by administrator mistakes, sometimes robust configuration/ configuration management could protect against this:
  - trivial/weak passwords, especially on test accounts (password==username etc.)
  - systems open to the world via ssh that don't need to be
  - firewalls that have been turned off for testing

other things to think about

- Kernel updates - often are an issue for clusters - people don’t like reboots, this can increase the risk of a single compromised account leading to root access.
- User management - if a user account / password / ssh key is discovered to be compromised, how easily can you disable it on all nodes

Conclusions

- Good logging and liaison with CERT teams helps to speed up incident analysis
- Alert your teams if you have/suspect you have an incident (find out local procedures before hand)
- it's important to identify **how** a system was compromised before it is rebuilt

Resources/Thanks

- http://www.oucs.ox.ac.uk/network/security
- Guide for cleaning Compromised Unix Systems
- Netflow/Argus talks
- Thanks to: Robin Stevens (OUCS), Jonathan Ashton (OUCS)