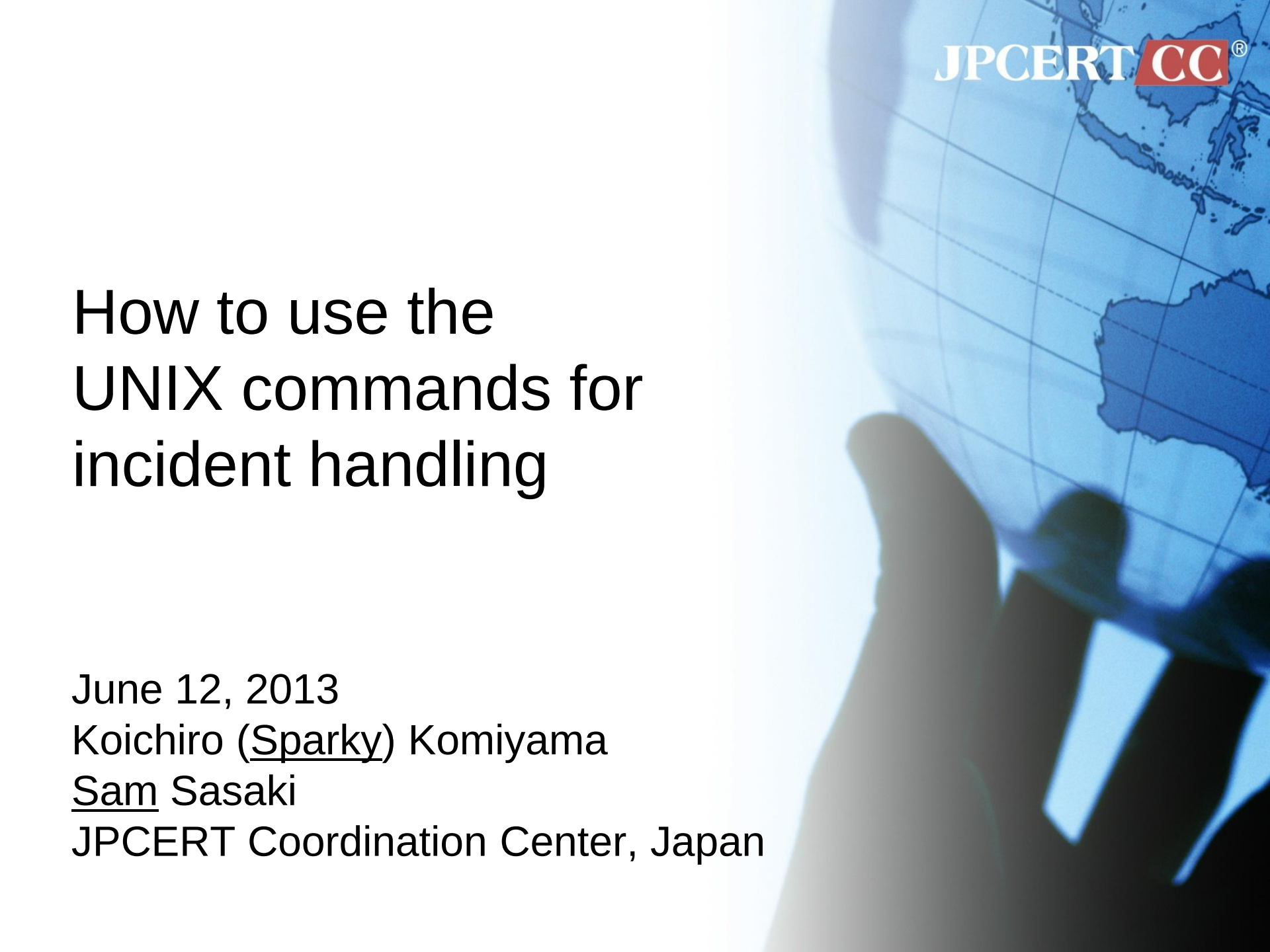


How to use the UNIX commands for incident handling

June 12, 2013

Koichiro (Sparky) Komiyama
Sam Sasaki
JPCERT Coordination Center, Japan

Agenda

- Training Environment
- Commands for incident handling
  – network investigation
- Commands for incident handling
  – file / text manipulation

Training Environment

- Command operation needs connection to Linux server with SSH
  - SSH client: putty
  - Server information
    - Host name:
    - User: ais01, ais02, …, ais20
    - Password: same as User

Tools for incident handling
- network investigation -

Command	Description
dig	Query the DNS to obtain domain name or IP address mapping for any other specific DNS record.
host	Identify the IP address from host name of URL, and vice versa.
whois	Identify the technical contact person(s) from IP address and/or domain name.

“dig” command

- Query the DNS to obtain domain name or IP address mapping for any other specific DNS record.

- How to use “dig”
  - Inquire the domain name / IP address

    $ dig [domain name]
    - List up the information associated with the domain name

    $ dig –x [IP address]
    - List up the information associated with the IP address.

“host” command

- Inquire host name and IP address with both forward and reverse resolution
- How to use “host”
  - Inquire IP address from host name

    $ host [host name]
    - List up the IP addresses associated with the host name
  - Inquire host name from IP address

    $ host [ip adress]
    - In the case that IP address is configured with reverse resolution

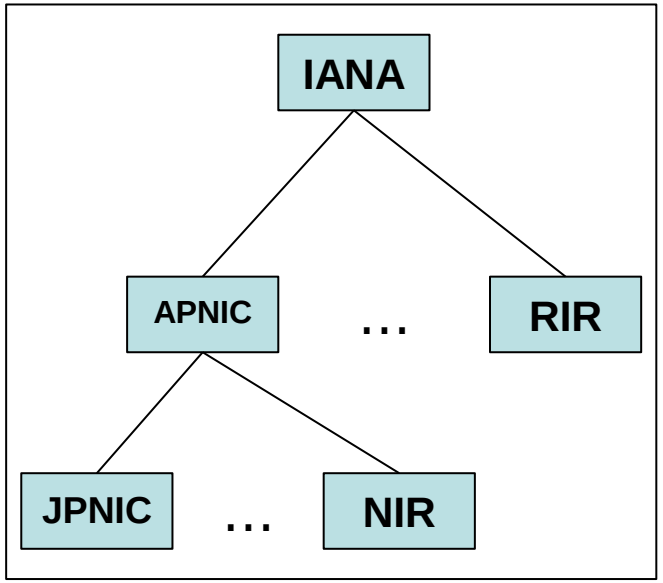
“whois” command (1)

- Anyone on the Internet can identify IP address, domain name, and registrant, etc
  - We mainly use “whois” to identify the notifying organization

- Information derived by “whois”
  - Information related to the IP address
    - Assigned / distributed organizations of the IP address
  - Information related to the contact person(s)
    - Information about the contact person(s) regarding assignment of IP address and AS number
      - Individual information about the contact
      - Group information about the department of the contact
  - Information related to the domain
    - Information about the domain, registrar, name server of the domain, and technical contact person

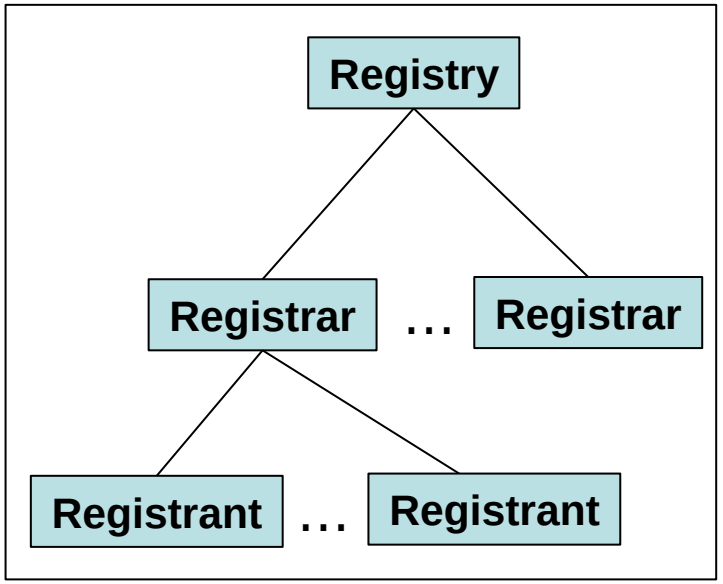
“whois” command (2)

- Administrative organization for IP address
  - RIR（Regional Internet Registry）
    - AfriNIC (whois.afrinic.net)
      - Africa
    - APNIC (whois.apnic.net)
      - Asia Pacific region
    - ARIN (whois.arin.net)
      - North America
    - LAC NIC (whois.lacnic.net)
      - Latin America, and Caribbean region
    - RIPE NCC (whois.ripe.net)
      - Europe
  - NIR（National Internet Registry）
    - Operative organizations under RIR
    - Japan is under JPNIC (whois.nic.ad.jp)



“whois” command (3)

- Administrative organization for domain
  - Registry
    - Manage domain name
    - Operate whois server
  - Registrar
    - Selling Domain name
    - Manage DNS record belongs to them
  - Registrant
    - Domain users. Can be an individual or an organization



“whois” command (4)

- How to use “whois”
  - Inquire by IP address

    $ whois -h whois.afrinic.net [ip address]
    - If you do not find the address, need to inquire to other RIR
    - Some RIRs link automatically to other RIR
  - Search for technical contact person

    $ whois -h whois.afrinic.net [technical contact]
  - Inquire by domain name

    $ whois [domain name]
    - Picks up an appropriate admin organization from TLD (top level domain)

Short exercise (1)

- dig / host
  - Let's see "internetsummitafrica.org"
    - IP address?
- whois
  - Let' see " 196.216.2.136"
    - Under which RIR?
    - IP range?
    - Who is the technical contact?

Short exercise (2)

- Advanced
  - Let's see technical contact of IP address "www.dns-ok.jpcert.or.jp"
    - Use "whois.apnic.net"

Tools for incident handling
- file / text manipulation -

Command	Description
wget	To see web contents without web browser(IE, Firefox…).
grep	Display strings specified by the command.
cat	Display contents of the file.
more / less	Display contents of the file (less: allowing both forward and backward navigation through the file).
head / tail	Display head / tail part of contents of the file.
cut	Display any columns specified by any delimiting characters.
sort	Sort rows.
uniq	Merge the duplicated rows.
wc	Count the number of words / lines / bytes in the text file.

“wget” command

- To check phishing sites and/or web defacement securely
- How to use “wget”
  - Get contents from the web site

    $ wget [url]
    - Save the contents to the current directory
  - Let’s get contents from the website, and output it to stdout

    $ wget [url] -O -
    - Display the contents on the screen

“grep” command

- To handle tons of texts contained in the file, such as access log, etc
- How to use “grep”
  - Search for any strings from the file

    $ grep [keyword] [file name]
    - Display the rows that contains specified keyword in the file
  - Search for rows that do NOT contain specified keyword

    $ grep -v [keyword] [file name]
    - With an option “-v”, display the rows that does NOT contain specified keyword in the file

“cat” command

- How to use “cat”
  - Display contents of the file on the screen

    $ cat [file name]

    - Display contents of the specified file on the screen

“more / less” command

- How to use “more”
  - Display contents of the file

    $ more [file name]

- How to use “less”
  - Display contents of the file, allowing both forward and backward navigation through the file

    $ less [file name]

“head / tail” command

- How to use “head”
  - Display head part of contents of the file.

    $ head [file name]

- How to use “tail”
  - Display tail part of contents of the file.

    $ less [file name]

“cut” command

- To extract necessary columns from specified file.

- How to use “cut”
  - Display any columns specified by any delimiting characters, from specified file.

    $ cut -d[delimiter] -f[column No.],... [file name]

    - Display the specified columns specified by the delimiters, from the specified rows in the file

“sort” command

- How to use “sort”
  - Sort the contents of the file
    - $ sort [file name]
      - Sort the rows of the specified file
  - Sort the contents of the file in reverse
    - $ sort -r [file name]
      - With an option “-r”, sort the contents of the file in reverse
  - Sort the contents of the file, based on any columns
    - $ sort -k[n] [file name]
      - With an option “-k”, sort the rows of the file based on “n”th column with delimiters (space/ tab/ camma)

“uniq” command

- How to use “uniq”
  - Merge the duplicated rows in the specified file

    $ uniq [file name]

  - Count the duplicated rows in the specified file

    $ uniq -c [file name]

    - With “-c” option, count the duplicated rows in the file

“wc” command

- How to use “wc”
  - Count the number of lines / words / bytes in the specified file.

    $ wc [file name]

  - Count the number of lines / words / bytes separately.

    $ wc -l [file name]

    - With “-l” option, count the lines in the file

    $ wc -w [file name]

    - With “-w” option, count the words in the file

    $ wc -c [file name]

    - With “-c” option, count the bytes/characters in the file

Short exercise (3)

- “wget” command
  - Get the contents from http://www.jpcert.or.jp/
  - Get the contents from http:// www.jpcert.or.jp/, and display them on the screen
- “grep” command
  - Search for the rows that contain <script> tag, from the contents acquired by “wget” command

Short exercise (4)

- “cat” command
  - Display access.log.
- “more / less / head / tail” command
  - Display access.log.
- “cut” command
  - Display IP addresses from access.log.

Short exercise (5)

- “sort” command
  - Sort access.log with IP address.
- “uniq” command
  - Merge the duplicated rows in access.log.
- “wc” command
  - How many lines / words / characters in access.log?

Short exercise (6)

- Advanced
  - Search for the rows that contain “404” from access.log.
  - Display the number of rows according to the IP addresses
  - Who is the technical contact of most frequent visitor(IP) to this web site?