LINUX FORENSICS

Hal Pomeranz

WHO IS HAL POMERANZ?

Started as a Unix Sys Admin in the 1980s

Independent consultant since 1997

Digital forensics, incident response, expert witness

Have done some interesting Linux/Unix investigations

hrpomeranz@gmail.com

@hal_pomeranz

https://archive.org/details/HalLinuxForensics

https://wildwesthackinfest.com/deadwood/training/

LINUX LOGS

Generally found under /var/log

Logs are primarily text

Easy to modify and manipulate

Logging is discretionary

Amount and format of logs left to developers

SAMPLE LOG MESSAGES

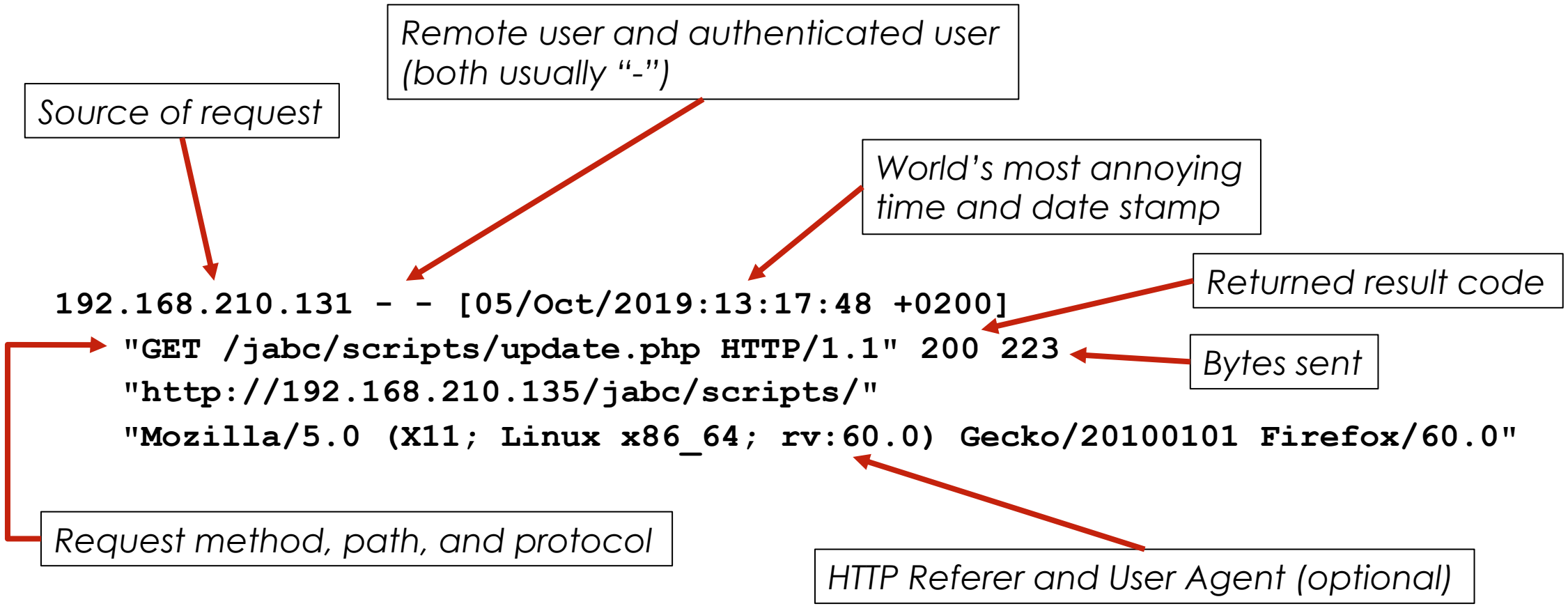
```
Oct  5 13:13:53 VulnOSv2 sshd[2624]: Accepted password for mail from
   192.168.210.131 port 57686 ssh2

Oct  5 13:13:53 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session
   opened for user mail by (uid=0)

Oct  5 13:14:04 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ;
   USER=root ; COMMAND=/bin/su -

Oct  5 13:14:04 VulnOSv2 sudo: pam_unix(sudo:session): session opened
   for user root by mail(uid=0)

Oct  5 13:14:04 VulnOSv2 su[2721]: pam_unix(su:session): session
   opened for user root by mail(uid=0)

Oct  5 13:18:48 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session
   closed for user mail
```

Timestamp in local time zone

Host where log originated

Process [and PID]

WEB LOGS


Remote user and authenticated user (both usually "-")
Source of request
World's most annoying time and date stamp
Returned result code
192.168.210.131 - - [05/Oct/2019:13:17:48 +0200]
"GET /jabc/scripts/update.php HTTP/1.1" 200 223
Bytes sent
"http://192.168.210.135/jabc/scripts/"
"Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
Request method, path, and protocol
HTTP Referer and User Agent (optional)

DELETED LOGS REGEX RECOVERY

Standard Linux Syslog

'[A-Z][a-z]* *[0-9]* [0-9]*:[0-9]*:[0-9]* *hostname* ‘

Apache Web Logs

'\[[0-9]*/[A-Z][a-z]*/[0-9]*:[0-9]*:[0-9]*:[0-9]* [-+][0-9]*\]'

blkls /dev/mapper/vg00-root > root-unallocated
strings –a root-unallocated | egrep *pattern* **>recovered-logs**

LAST LOGIN HISTORY

`wtmp` – User logins and system reboots [read with **`last`**]

File may be truncated weekly or monthly

`btmp` – Failed logins [read with **`lastb`**]

Often not kept due to risk of password disclosure

`lastlog` – Last login for each user [read with **`lastlog`**]

Varying formats make decoding tricky

LINUX KERNEL AUDITING

Kernel-level activity monitor can see everything
- System booting
- User logins and privilege change/escalation
- Scheduled task execution
- SELINUX security policy violations

With additional configuration can log
- File access, modification, execution
- Any specific system call(s) across all processes
- User keystrokes
- Locally defined tags or keywords for later searching

ALL HAIL AUSEARCH!

```
# ausearch -if /mnt/evidence/var/log/audit -c useradd
----
time->Thu Feb 20 13:26:44 2020
type=PROCTITLE msg=audit(1582223204.906:342):
    proctitle=2F7573722F7362696E2F7573657261646402D64002F7573722F706870002D6D0
    02D2D737973746564002D2D7368656C6C002F62696E2F62617368002D2D736B656C002F6574
    632F736B656C002D4700776865656C00706870
type=PATH msg=audit(1582223204.906:342): item=0 name="/etc/passwd"
    inode=135568 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00
    obj=system_u:object_r:passwd_file_t:s0 objtype=NORMAL
    cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
type=CWD msg=audit(1582223204.906:342):  cwd="/var/mail"
type=SYSCALL msg=audit(1582223204.906:342): arch=c000003e syscall=2
    success=yes exit=5 a0=55d79f171ce0 a1=20902 a2=0 a3=8 items=1 ppid=9425
    pid=9428 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
    tty=pts1 ses=3 comm="useradd" exe="/usr/sbin/useradd"
    subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="auth-files"
```

OTHER TOOLS

`aureport`

Generate summary reports for different event types
Get detailed breakdowns with **`ausearch -a`**

`aulast`

`aulastlog`

Produce output like **`last`** and **`lastlog`** using audit logs

THANK YOU!

Any final questions?
Thanks for listening!

hrpomeranz@gmail.com
@hal_pomeranz

https://archive.org/details/HalLinuxForensics
https://wildwesthackinfest.com/deadwood/training/