APRICOT2015 Security Workshop:

Detecting Sick Hosts

Sheryl Hermoso, APNIC
sheryl@apnic.net

Sick Hosts

- Host or end-user computers that have been “infected” or compromised
  - Servers, PC/Laptop, Smart phones
- Host can be infected by:
  - Virus, Malware, Trojan, Backdoor
- Host now becomes:
  - a bot
  - a spam engine
  - a ‘stepping stone’ for hiding tracks

Risks to/from hosts

- Keystroke Loggers, malware, etc
- Other infected hosts in network
- Misbehaved users/clients (PEBCAK)
- Social engineering

How can you detect infected hosts?

Logs

- Syslog (centralized)
- logwatch, swatch
- Key is to ensure you are informed of what is *important* as opposed to every possible event. (or you'll start to ignore the logs)

Syslog Facility Level

Facility Number	Keyword	Facility Description
0	Kern	Kernel message
1	User	User-level message
2	Mail	Mail system
3	Daemon	System daemon
4	Auth	Security/authorization messages
5	Syslog	Messages by syslogd
16	Local0	Local user 0
23	Local7	Local user 7

Logwatch Example

```
################### Logwatch 7.3.4 (02/17/07) ####################
      Processing Initiated: Sun Sep 30 04:12:38 2012
      Date Range Processed: yesterday
                          ( 2012-Sep-29 )
                          Period is day.
    Detail Level of Output: 10
          Type of Output: unformatted
        Logfiles for Host: irrashai.up.edu.ph
 ##################################################################

---------- Cron Begin ----------

Commands Run:
  User cacti:
    /usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1: 287 Time(s)
  User root:
    /etc/webmin/bandwidth/rotate.pl: 24 Time(s)
    /etc/webmin/cron/tempdelete.pl: 1 Time(s)
    /root/backupMySQL.sh #everyday at 6am: 1 Time(s)
    /usr/local/bin/refresh-dhcpdconf: 1440 Time(s)
    root      /usr/sbin/logwatch: 1 Time(s)
    run-parts /etc/cron.daily: 1 Time(s)
    run-parts /etc/cron.hourly: 24 Time(s)
    wget -O - -q -t 1 /var/www/html/drupal/cron.php: 24 Time(s)

**Unmatched Entries**
error: Job execution of per-minute job scheduled for 13:20 delayed into s

---------- Cron End ----------

---------- SSHD Begin ----------

Didn't receive an ident from these IPs:
  201.67.47.69: 1 Time(s)
  202.92.128.188: 1 Time(s)

Failed logins from:
  41.212.83.191 (41.212.83.191.wananchi.com): 138 times
    root/password: 138 times
  195.14.0.238 (195-14-0-238.nuxit.net): 1 time
    root/password: 1 time
  202.106.46.42: 34 times
    root/password: 34 times
  221.204.253.107 (107.253.204.221.adsl-pool.sx.cn): 1 time
    root/password: 1 time

Illegal users from:
  41.212.83.191 (41.212.83.191.wananchi.com): 1 time
    ____/password: 1 time


Received disconnect:
  11: Bye Bye
    202.106.46.42 : 34 Time(s)
    41.212.83.191 : 139 Time(s)

**Unmatched Entries**
reverse mapping checking getaddrinfo for 41.212.83.191.wananchi.com [41.212.83.191] failed - POSSIBLE BREAK-IN
ATTEMPT! : 139 time(s)
Address 221.204.253.107 maps to 107.253.204.221.adsl-pool.sx.cn, but this does not map back to the address -
POSSIBLE BREAK-IN ATTEMPT! : 1 time(s)

---------- SSHD End ----------
```

Trends and alerts

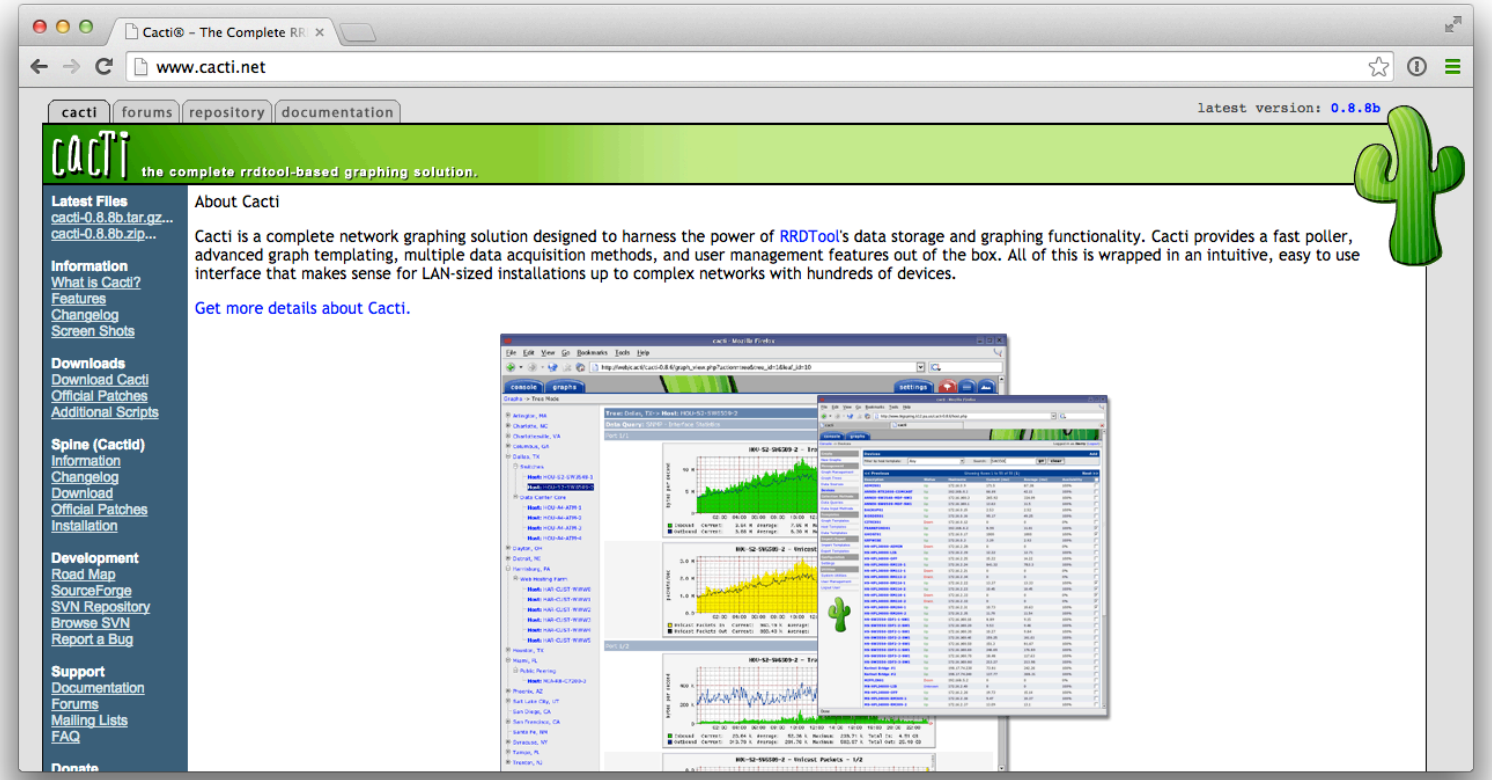
- Bandwidth usage: CACTI
- Network events: NAGIOS
- Packet analyzers/dumpers for tracking down individual events.
- All the above depend on sanely designed network infrastructure.

Monitoring Tools

- Zabbix
- Observium
  - Provides auto-discovery of devices
  - Uses RRDTools for graphing
- Icinga
  - Modular design
- Cacti
  - Collects data via snmp

Cacti

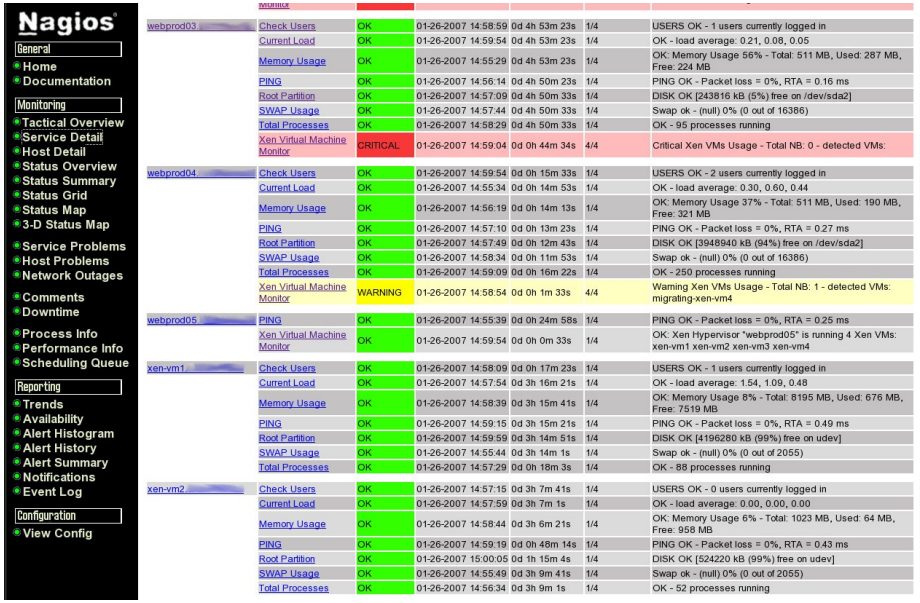
- Network monitoring and graphing tool



http://www.cacti.net/

Nagios

- IT infrastructure monitoring
- Used for alerting and reporting
- Monitors
  - Applications
  - Operating systems
  - Network protocols
  - System metrics
    - CPU, memory, load



BAYU

- Be aware you are uploading:
- http://filesharing.uoregon.edu/bayu_notification.html
- On a single enterprise/campus network you may have the ability (think permission) to move users into a “disciplinary pen” if their machine misbehaves.
- ISPs should not do as much policing, but some is possible

Policies

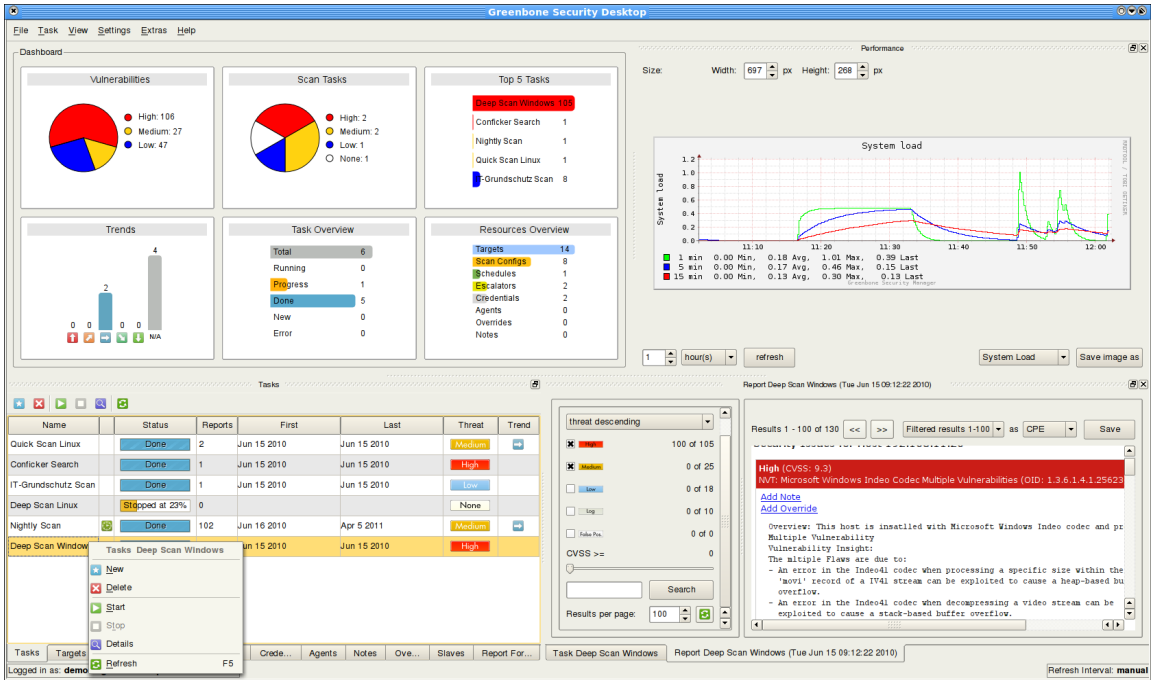
- Submit to a “scan” on connection
- Scan your own machines regularly
- Run an IDS
- What do you do with the results of that data? How do you scan?

Nessus

- Comprehensive vulnerability scanner
- Free of charge for personal use
- Can scan for
  - Vulnerabilities that allow remote access
  - Misconfiguration
  - Default and common passwords (dictionary attack)
- Finds open ports, tries various exploits

OpenVAS

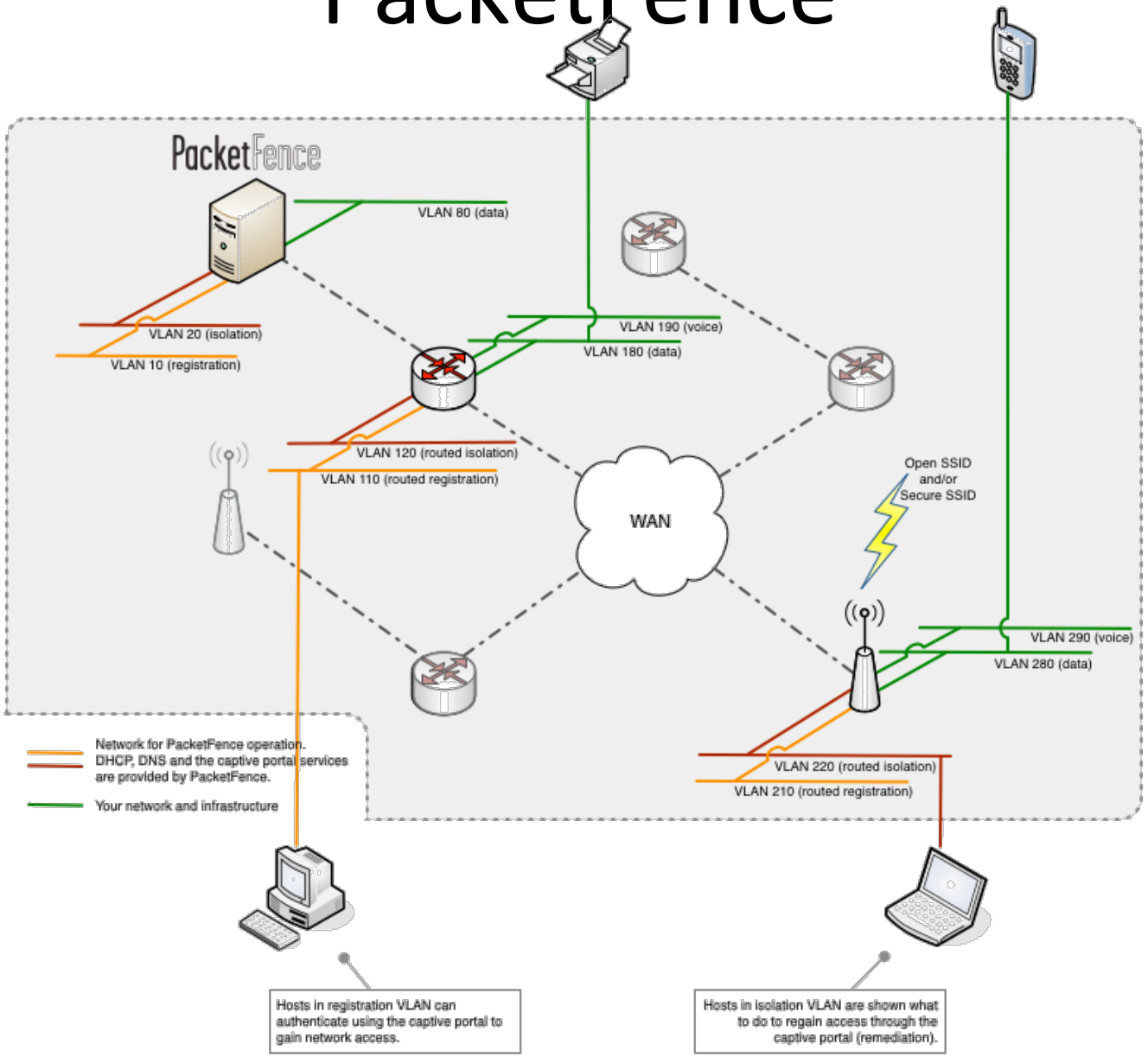
- Open-source vulnerability scanner and manager
- Started as a fork to Nessus



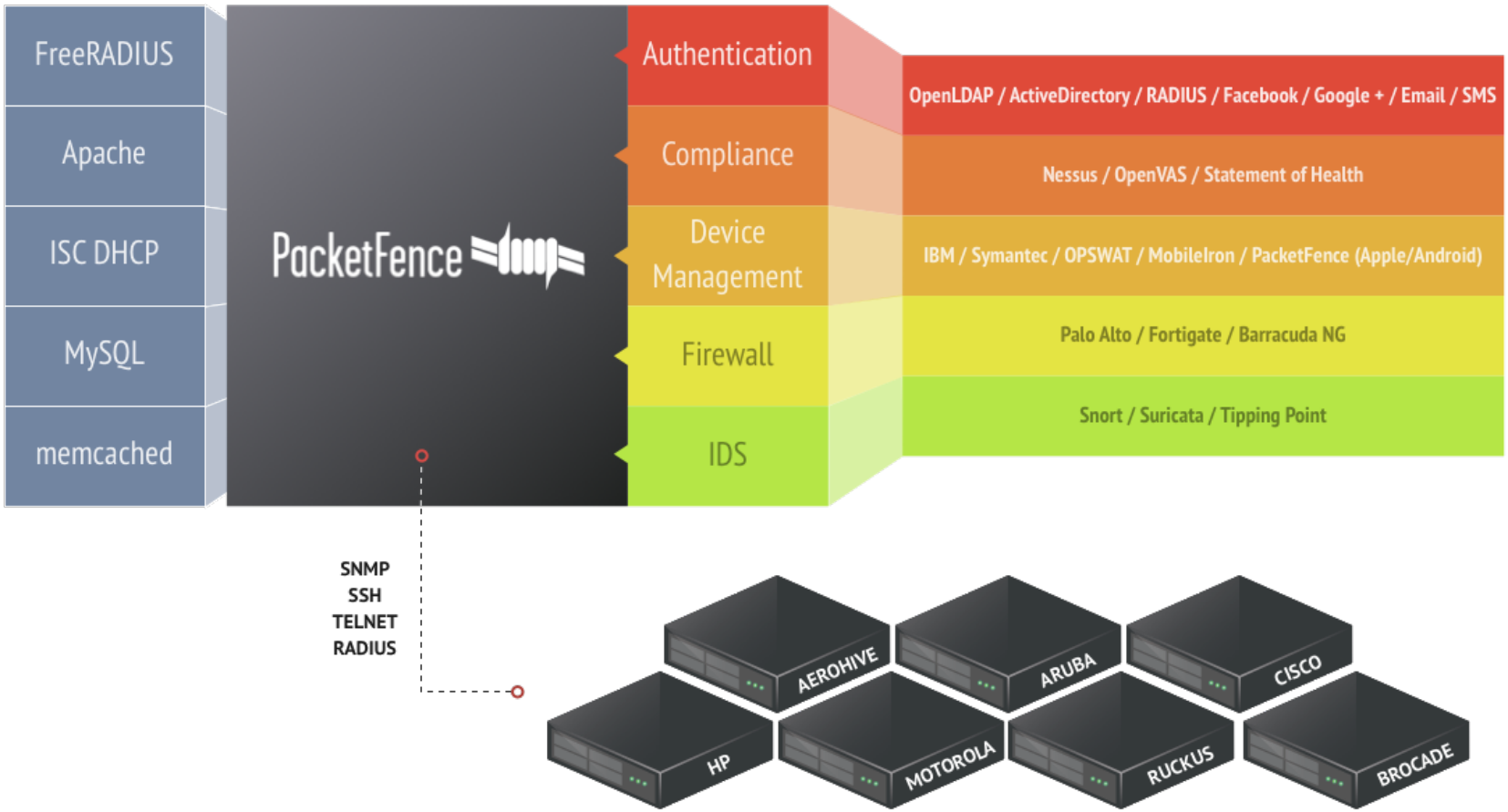
PacketFence

- Used for Network access control (NAC)
- Features:
  - Captive portal for registration and remediation
  - Centralized management
  - Detection of abnormal network activity with Snort
  - Vulnerability scans with Nessus
  - Isolation of problematic devices
- Zero-Effort NAC (ZEN) edition can be used to rapidly deploy PacketFence in your network

PacketFence



Packetfence



Principles

- Do not scan inline – you end up adding a point of failure as well as a bottleneck. You do need a “mirror” or “monitor” port
- Need supported hardware with SNMP (Ubiquity support still in progress)
- In ISPs you can trigger custom Perl scripts based on particular “events” from network scanners.

Principles

- In enterprises you can drop the users access port in a VLAN with restricted filters.
- For scalability you could have more boxes in different parts of the network.
- FreeNAC is an alternative piece of software (also opensource)

Snort

- An open source network intrusion detection system
- A rule-based language combining signature, anomaly, and protocol inspection
- Must be placed close to the “choke point”
  - Where all traffic flows in/out of the network
  - Close to the border router or firewall
- Use a span/port mirror port to send traffic from

http://www.snort.org/

Data gathering

- IDS systems
- Active scanners
- Netflow

Questions