
Top 5 Log Reports

By Chris Brenton
chris@chrisbrenton.org

What Is The Top 5 Essential Log Reports?

- Top 5 security reports worthy of review
 - Not intended as a complete list
 - Low hanging fruit
- Designed to be portable
 - Suit a wide range of job titles
 - Suit a wide range of environments
- Designed to be timeless
 - Defined two years ago but still applicable
 - Attacks change but diligence does not

The List

1. Attempts to gain access through existing accounts
2. Failed file or resource access attempt
3. Unauthorized changes to users, groups or services
4. Systems most vulnerable to attack
5. Suspicious or unauthorized network traffic patterns

Why Are The Reports So General?

- This is a “feature”
- Every job title and environment is different
 - No “one size fits all”
- Attack vectors change over time
 - Processes to catch them stay relatively consistent

Example –Firewall Logs

- 1999 = Check the log for inbound drops which may indicate someone knocking on your door
- 2009 = Check the log for outbound connections which may indicate an internal host has been compromised
- The focus has changed but the process (check logs for suspect activity) remains the same

Sample Reports

- Let's look at some sample reports in each category
- We'll break them out
 - Low false positive rate
 - Higher false positive rate
- Note that while we call them "reports" real time alerting can be used when appropriate
 - Low noise examples are good choices

#1 Attempts to gain access through existing accounts

- Brute force password guessing has always been a major point of attack
 - Just the authentication mechanism changes
- Can be mitigated with
 - Public/Private keys
 - One time password

Access Attempts – Low Noise

Attempted failed logins to disabled accounts.
Logon type not permitted (Microsoft event ID 534).
Direct logons as root/administrator.
High number of failed logon attempts in a short amount of time.
Same account, logon from source IPs.

Access Attempts – High Noise

Total failed logins per day.

Top 5 users with most failed logins per day.

Failed authentications to servers sorted by number.

Unauthorized access attempts (logon failures per account with time/count threshold).

Any statistically significant increase in failed logons.

Auditing on DC's (Domain Controllers) for logon/logoff events.

Intruder attempts, both for normal workstation users and Admin server users.

Failed remote access attempts.

Any unexpected logon attempts through the VPN.

#2 Failed File Or Resource Access Attempts

- Could indicate unauthorized access
 - Incorrect permissions
- Could indicate a possible attack
 - Probe for known vulnerable files
 - Probe for known vulnerable services

File or Resource Attempts – Low Noise

HR-based reporting. User termination and activation. Post termination activity.
High Web server 403 error rates from a single IP.
Port scans and/or Ping sweeps (source internal).
Failed zone transfers.
Failed recursion attempts.
Failed write access to files or directories, especially sensitive ones.
Read attempts to honeypot files or records.
Failed mail relay attempts.

File or Resource Attempts – High Noise

Sensitive resource (e.g. files, dbtables, servers) access reports and anomalies.
Unauthorized/inappropriate web/file access.
Any statistically significant increase in errors.
Web site abnormal file activity, abnormal time period access,
abnormal access to zones/areas of the web site.
Port scans and/or Ping sweeps (source external).

#3 Unauthorized Changes To Users, Groups or Services

- Could indicate a system compromise
 - Purp creates an account for later access
 - Account association with high level groups
 - Initializing new services
 - Especially ones that open sockets

User, Group, Service Change – Low Noise

Changes involving high level accounts (Admin equiv, same group as root, etc).
Report on AD configuration changes.
Abnormal OS/Application level activity – especially time based and zone based.
Services or drivers launched more than 5 minutes after boot.
Service or drivers disabled more than 5 minutes before shutdown.

User, Group, Service Change– High Noise

Audit log of all administrator level activity.

All account management (creation, password changes, group membership changes).

Privilege & policy changes.

Changes to sensitive Active Directory (AD) groups.

Changes to Schema Administrators group membership.

Tracking of changes to user permissions at folder level.

Abnormal OS/Application level activity – especially time based and zone based.

Abnormal process activity (processes created by unusual accounts or at unusual times, e.g. command prompt running as local system).

#4 Systems Most Vulnerable To Attack

- Combination of four metrics
 - Is the system properly configured?
 - Is it patched and up to date?
 - IS the OS locked down?
 - HIPS and/or Application whitelisting
 - In which security zone is it located?
- Tools to test the first three conditions
- The fourth is the responsibility of the admin
- Relative system risk is a combination of all four metrics
 - Vulnerability scanning only looks at first two

Relative Risk Example

- Finger is listening on a router
 - Border router with no ACL's
 - Border router with default deny
 - Internal router with no ACL's
 - Internal router with ACL's limiting access to the NOC's IP address
- Same condition in each case, but different risks apply

What Makes A System Vulnerable?

- It's about "remote accessing to software running on the system"
 - Not just accessible sockets
- Some less obvious examples
 - Desktop running a Web browser
 - Firewall, NIDS, NIPS with no open sockets
- In each case software is accessed remotely without the need of a persistent socket
- System may still be exploitable
 - Lockdown tools are the deciding factor

Vulnerable Systems – Low Noise

Missing patch report, low security zone.
Open sockets, low security zone.
Vulnerability scan results.

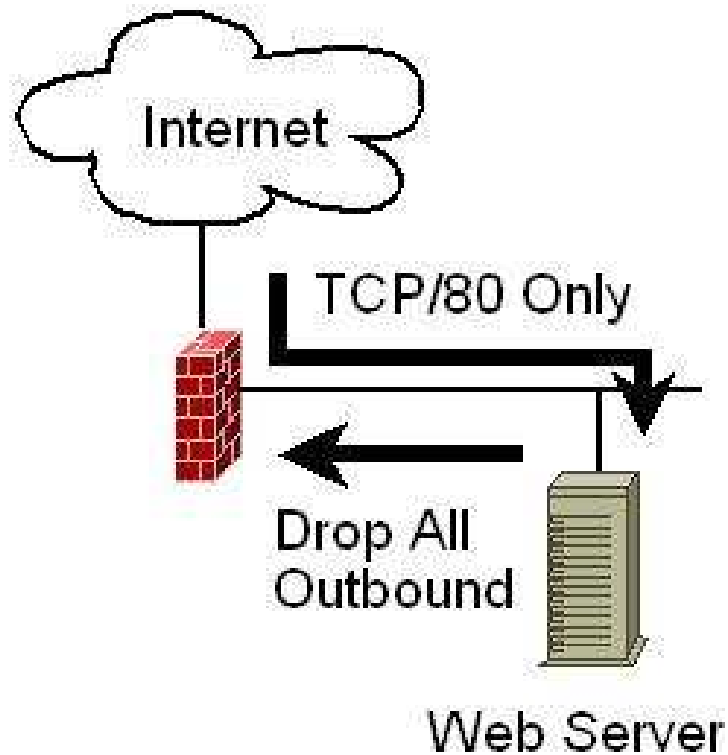
Vulnerable Systems – High Noise

Missing patch report, high security zone.
Open sockets, high security zone.
Variations from the corporate policy template.
Systems in a low security zone which are not locked down.

#5 Suspicious Network Traffic Patterns

- Anything you do not expect
 - Or can explain via access policy
- Should scrutinize all patterns
 - Inbound
 - Outbound
 - Internal
- Assumes you can define “normal”

Suspicious Traffic Example



Why is my Web server trying to TFTP to China?

Suspicious Network Traffic – Low Noise

Top internal systems receiving ICMP errors or TCP/RST's.

Any outbound ICMP error packets from the internal network.

Source IPs listed in the Dshield watch list.

Layer 2 error reports. (Arpwatch).

Email attachments sent to multiple external addresses.

Email sent to competitors.

Outbound rejects from DMZ.

Suspicious Network Traffic– High Noise

Top transmitting systems.

Top receiving systems.

Top highest bandwidth-consuming sessions.

Top protocols.

Top list of accessed web sites.

Top IDS signature destinations per day.

Top firewall blocked sources per day.

Top firewall blocked destinations per day.

Top list of rejected packets, both source and destination.

Denied outbound connections from internal network.

SIM Possibilities

- Combine items from multiple categories to increase accuracy
- Item #1 = Multiple failed logon attempts via SSH
- Item #5 = Outbound TFTP session detected
- Conclusion = System is compromised and purp is attempting a toolkit transfer

Questions?

chris@chrisbrenton.org