



What is security?

Hyounghick Kim

Department of Software

College of Software

Sungkyunkwan University

What is “security”?

- Security – “safety, or freedom from worry”

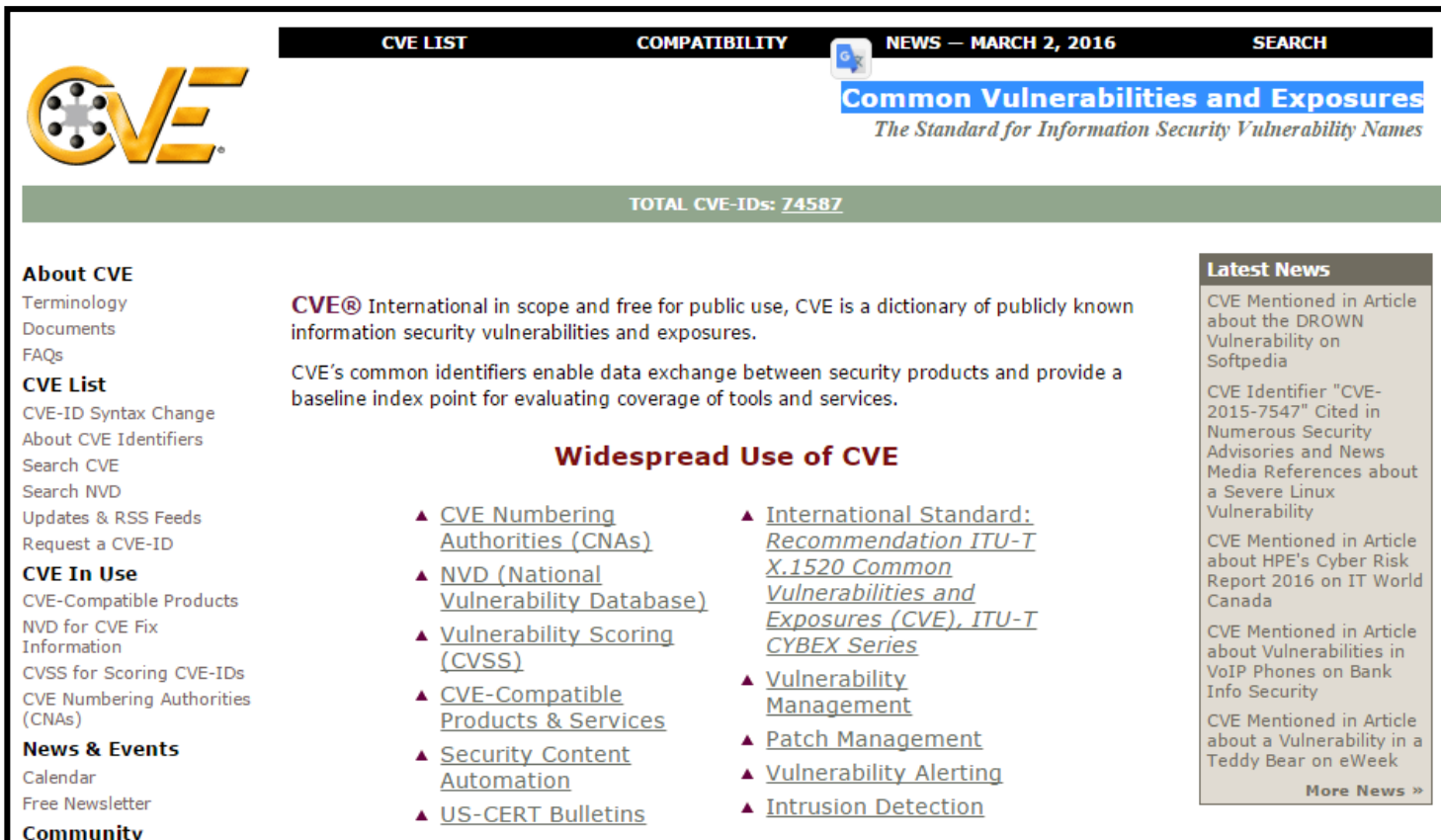


Threat terminology

- **Attack:**
an intentional attempt to breach system security (e.g., buffer overflow attack)
- **Threat:**
a possible scenario that can harm a system (e.g., natural disaster, human mistake)
- **Vulnerability:**
the “hole” that allows an attack to succeed (e.g., buffer overflow bug)
 - Vulnerability vs. Security bug
 - Security bug is the vulnerability related to software
- **Exploit:**
an implementation of attack (e.g., a code which lead to a buffer overflow attack)

Common Vulnerabilities and Exposures (CVE)

<http://cve.mitre.org/about/index.html>



The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for CVE LIST, COMPATIBILITY, NEWS — MARCH 2, 2016, and SEARCH. The CVE logo is on the left. Below the navigation bar, the title "Common Vulnerabilities and Exposures" is displayed, followed by the tagline "The Standard for Information Security Vulnerability Names". A green bar indicates "TOTAL CVE-IDs: 74587". The main content area is divided into three columns. The left column contains links for "About CVE" (Terminology, Documents, FAQs), "CVE List" (CVE-ID Syntax Change, About CVE Identifiers, Search CVE, Search NVD, Updates & RSS Feeds, Request a CVE-ID), "CVE In Use" (CVE-Compatible Products, NVD for CVE Fix Information, CVSS for Scoring CVE-IDs, CVE Numbering Authorities (CNAs)), "News & Events" (Calendar, Free Newsletter), and "Community". The middle column features a paragraph about CVE's international scope and public use, followed by a section titled "Widespread Use of CVE" with two columns of links: "CVE Numbering Authorities (CNAs)", "NVD (National Vulnerability Database)", "Vulnerability Scoring (CVSS)", "CVE-Compatible Products & Services", "Security Content Automation", "US-CERT Bulletins", "International Standard: Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures (CVE), ITU-T CYBEX Series", "Vulnerability Management", "Patch Management", "Vulnerability Alerting", and "Intrusion Detection". The right column is titled "Latest News" and contains four news items with links to articles about DROWN, CVE-2015-7547, HPE's Cyber Risk Report, and VoIP phones on Bank Info Security, followed by a "More News" link.

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

TOTAL CVE-IDs: 74587

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVSS for Scoring CVE-IDs
CVE Numbering Authorities (CNAs)

News & Events
Calendar
Free Newsletter

Community

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ [CVE Numbering Authorities \(CNAs\)](#)
- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [Vulnerability Scoring \(CVSS\)](#)
- ▲ [CVE-Compatible Products & Services](#)
- ▲ [Security Content Automation](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [International Standard: Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)
- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)

Latest News

CVE Mentioned in Article about the DROWN Vulnerability on Softpedia

CVE Identifier "CVE-2015-7547" Cited in Numerous Security Advisories and News Media References about a Severe Linux Vulnerability

CVE Mentioned in Article about HPE's Cyber Risk Report 2016 on IT World Canada

CVE Mentioned in Article about Vulnerabilities in VoIP Phones on Bank Info Security

CVE Mentioned in Article about a Vulnerability in a Teddy Bear on eWeek

[More News »](#)

CVE prefix + Year + Arbitrary Digits (e.g., CVE-2014-9999)

Exploit database archive

<https://www.exploit-db.com/>

Offensive Security's Exploit Database Archive

36832

Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

The Exploit Database

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

EXPLOIT DATABASE

CVE Compliant



Remote Exploits



This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2017-03-06				FTPSHELL Client 6.53 - Buffer Overflow	Windows	Peter Baris
2017-03-01				SysGauge 1.5.18 - Buffer Overflow	Windows	Peter Baris

How do hackers use them?

1. Reconnaissance for finding vulnerabilities
 - ✓ Ping sweeps, fingerprinting and port scanning
2. Exploitation with the discovered vulnerabilities
 - ✓ Implementing exploits
3. Hiding evidence that they have been there
 - ✓ Removing log files

Reconnaissance (Demo)



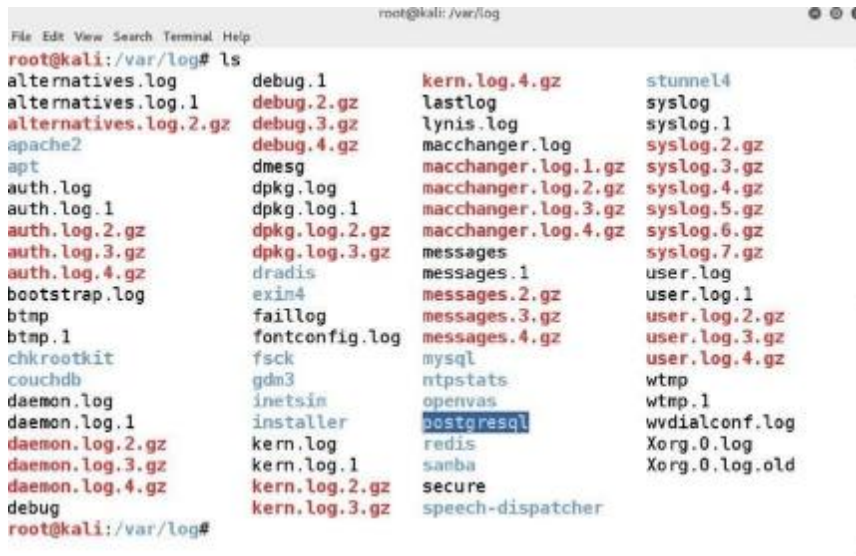
Exploitation (Demo)



The screenshot shows a web browser window with the URL <https://www.exploit-db.com>. The page title is "Exploits Database by Offensive Security". The main heading is "EXPLOIT DATABASE" with a bug icon. Below this, the text reads "Offensive Security's Exploit Database Archive" and "36832 Exploits Archived". A description states: "The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#)." At the bottom, there is a banner for the "Google Hacking Database" (GHDB) with the text: "The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more." The banner also features the text "GOOGLE HACKING DATABASE" in large, stylized letters.

Hiding evidence

- Finding the log files
 - The log files are stored in the /var/log directory.



```
File Edit View Search Terminal Help
root@kali: /var/log
root@kali: /var/log# ls
alternatives.log      debug.1              kern.log.4.gz        stunnel4
alternatives.log.1    debug.2.gz           lastlog              syslog
alternatives.log.2.gz debug.3.gz           lynis.log            syslog.1
apache2               debug.4.gz           macchanger.log        syslog.2.gz
apt                  dmesg               macchanger.log.1.gz  syslog.3.gz
auth.log             dpkg.log             macchanger.log.2.gz  syslog.4.gz
auth.log.1           dpkg.log.1           macchanger.log.3.gz  syslog.5.gz
auth.log.2.gz        dpkg.log.2.gz        macchanger.log.4.gz  syslog.6.gz
auth.log.3.gz        dradis              messages             syslog.7.gz
auth.log.4.gz        exin4               messages.1           user.log
bootstrap.log        faillog             messages.2.gz        user.log.1
btm                 fontconfig.log      messages.3.gz        user.log.2.gz
btm.1                fsck                messages.4.gz        user.log.3.gz
chkrootkit           gdm3               mysql                user.log.4.gz
couchdb              inetd               ntpstats             wtmp
daemon.log           installer           openvas              wtmp.1
daemon.log.1         kern.log            postgresql            wvdialconf.log
daemon.log.2.gz      kern.log.1          redis                Xorg.0.log
daemon.log.3.gz      kern.log.2.gz       samba                Xorg.0.log.old
daemon.log.4.gz      kern.log.3.gz       speech-dispatcher
debug
root@kali: /var/log#
```

- ✓ /var/log/messages: general system activity
- ✓ /var/log/secure: authentication and authorization privileges
- ✓ /var/log/lastlog: recent logins
- ✓ /var/log/faillog: failed logins

- Deleting events related to the hack, or erasing all entries

Questions?

