

Testing for vulnerabilities

PURPOSE & MOTIVATION

- Information systems are inherently vulnerable
- Vulnerability: "System vulnerability is defined to be the intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw" [1]
- Presence of vulnerability
- Vulnerability identification
- Vulnerability Exploitation
- Exploitation of vulnerabilities by cybercriminals can cause a lot of inconvenience
- Financial losses, confidential information, human lives
- It is necessary to identify and repair vulnerabilities before they are exploited by attackers: pentesting

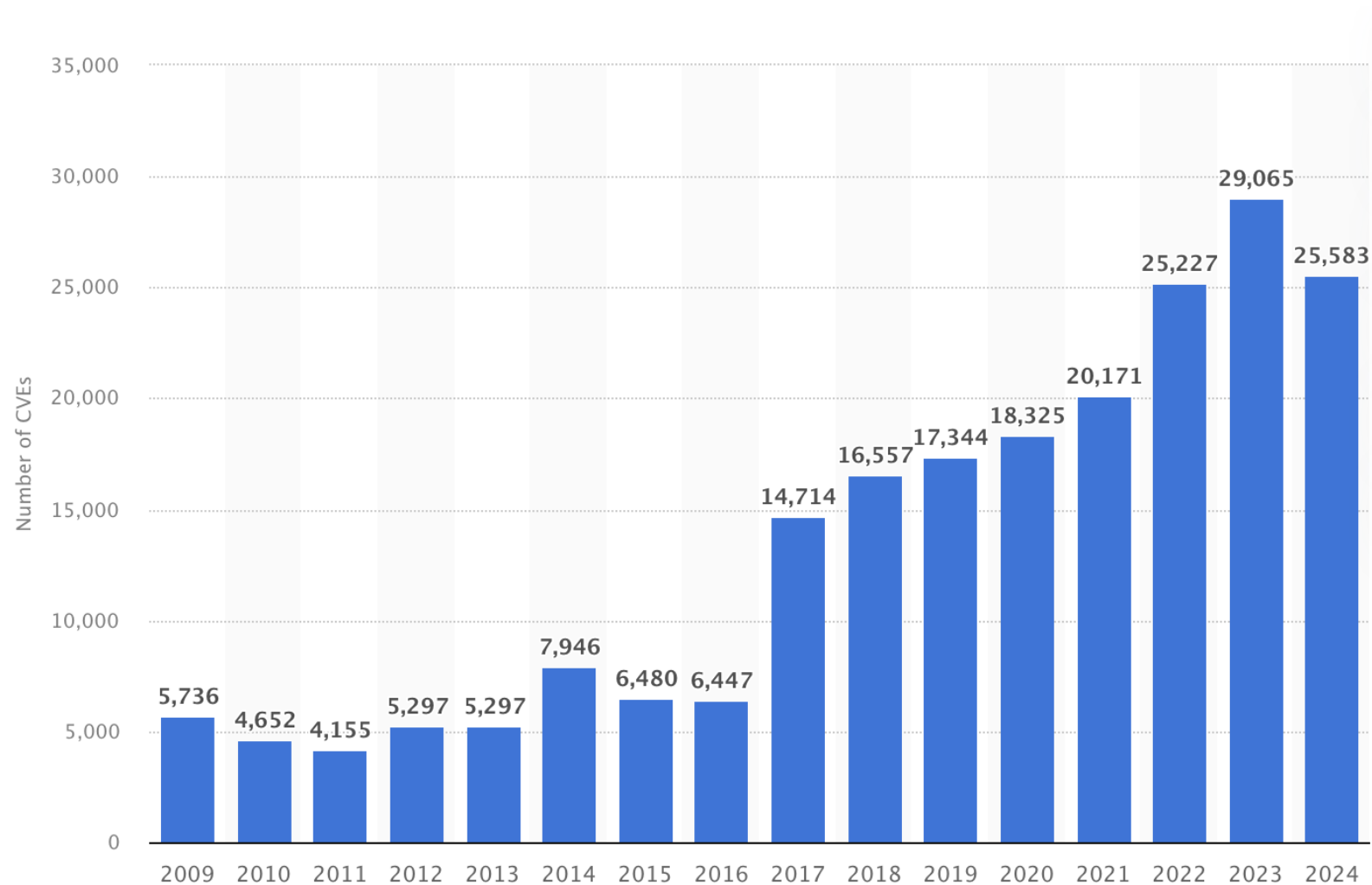
PURPOSE & MOTIVATION (2)

- Security is often ignored
- Usability = $1 / \text{Security}$
- A lot of code, a lot of programmers
- Questionable quality...
- Theoretical solutions are insufficient
- Crypto, word, etc.
- Contemporary attacks are focused on financial gain or espionage

PURPOSE & MOTIVATION (3)

- New/unknown vulnerabilities
- CVE – Common Vulnerabilities and Exposures
- CVD – Coordinated Vulnerability Disclosure
- Notify the vendor!
- Get rid of potential legal problems
- You are credited with discovering vulnerability
- Be responsible!
- Most of the time, you'll be relying on known vulnerabilities
 - <https://www.exploit-db.com>

PURPOSE & MOTIVATION (4)



METHODOLOGY

1. information gathering
2. service enumeration
3. exploitation
4. persistence
5. post exploitation enumeration
6. house keeping

METHODOLOGY (II)

- service enumeration
 - port scanning, SNMP, DNS, SMTP, SQL, etc.

```
root@kali:~# nmap -sV 192.168.19.131
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-10-05 05:52 EDT
Nmap scan report for 192.168.19.131
Host is up (0.00047s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:C0:26:36 (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.03 seconds
root@kali:~#
```

METHODOLOGY (III)

- exploitation
 - obtaining access to the attacked system
 - usually using exploits for vulnerabilities discovered in step 2

```
msf exploit(vsftpd_234_backdoor) > exploit

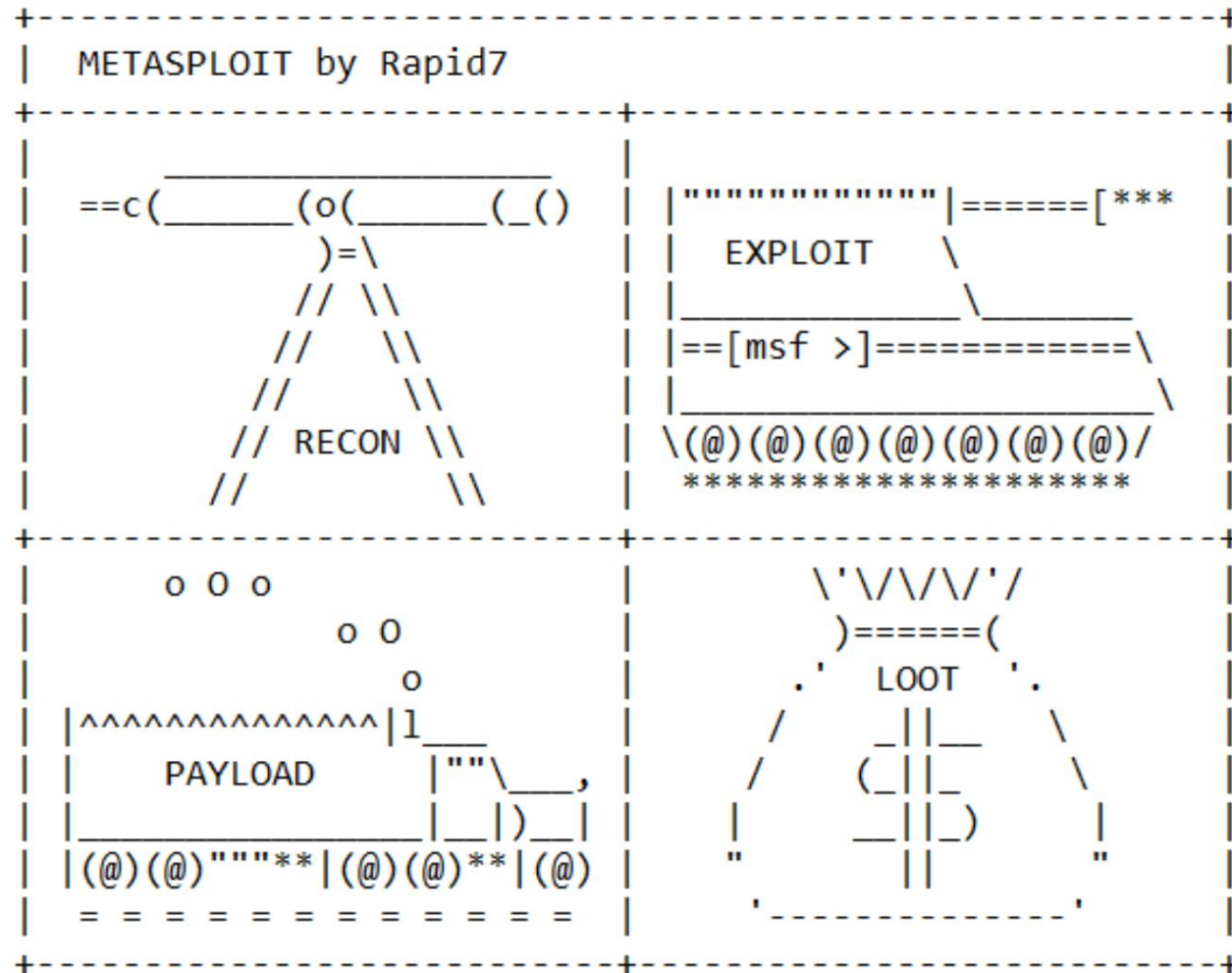
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.19.159:45371 -> 192.168.19.131:6200) at 2016-10-05 06:16:06 -0400

whoami
root
id
uid=0(root) gid=0(root)
```


METHODOLOGY (IV)

- Persistence of access
 - Installation of backdoors
 - Adding new users
 - Obtaining hashes/passwords for later access
- Post-attack enumeration
 - Confidential information, hashes, documents, etc.
- House-keeping
 - Rootkits for hiding components "installed" on the attacked system
 - Cleaning traces
 - Cleaning access logs, history, etc.
 - Delete installed files/components

METHODOLOGY (V)



Tools

- Operating System
 - Kali Linux
 - Debian-based distribution
 - Contains a lot of specific tools
- Mass scanning/mining tools (not recommended)
 - OpenVAS, CoreImpact, SAINT, Nessus, NeXpose
- Basic tools
 - Metasploit, nmap

Tools (II)

- Obtaining information
 - Netdiscover, nmap, Maltego, etc.
- Vulnerability analysis
 - Nmap, Golismero, OpenVAS, etc.
- Web Application Analysis
 - Burpsuite, WebScarab, etc.
- Database analysis
 - SQLMap, SQLNinja, etc.
- Password attacks
 - John, Hashcat, Rainbowcrack, etc.

Tools (III)

- For wireless networks
 - aircrack-ng, etc.
- Reverse engineering
 - OllyDbg, NASM, clang, apktool, etc.
- Exploitation
 - Metasploit, SQLMap, armitage, etc.
- Sniffing & spoofing
 - Wireshark, ettercap, reply, etc.
- Post-exploitation
 - ProxyChains, bdfproxy, etc.

Report

- The pentesting procedure ends with a report
- The report must include:
 - Every vulnerable system
 - Each vulnerability identified
 - Methodology/Exploitation Steps
 - Risk analysis
 - Solutions
- The report is prepared by the pentester and handed over to the customer
- Information must be communicated clearly and effectively
 - The client may not be very educated in the field of security...