LAB 05: DOCUMENTATION

Introduction to
Penetration Testing

TOPICS

- Final analysis of findings.
- Reporting.

FINAL ANALYSIS

- Regardless of risk rating reported by automated scanners, each finding should be assessed manually.
- During risk assessment, the following should be taken into consideration:
  - The environment.
  - Policies & procedures.
  - Complexity & skill level required for exploitation.
  - Impact.

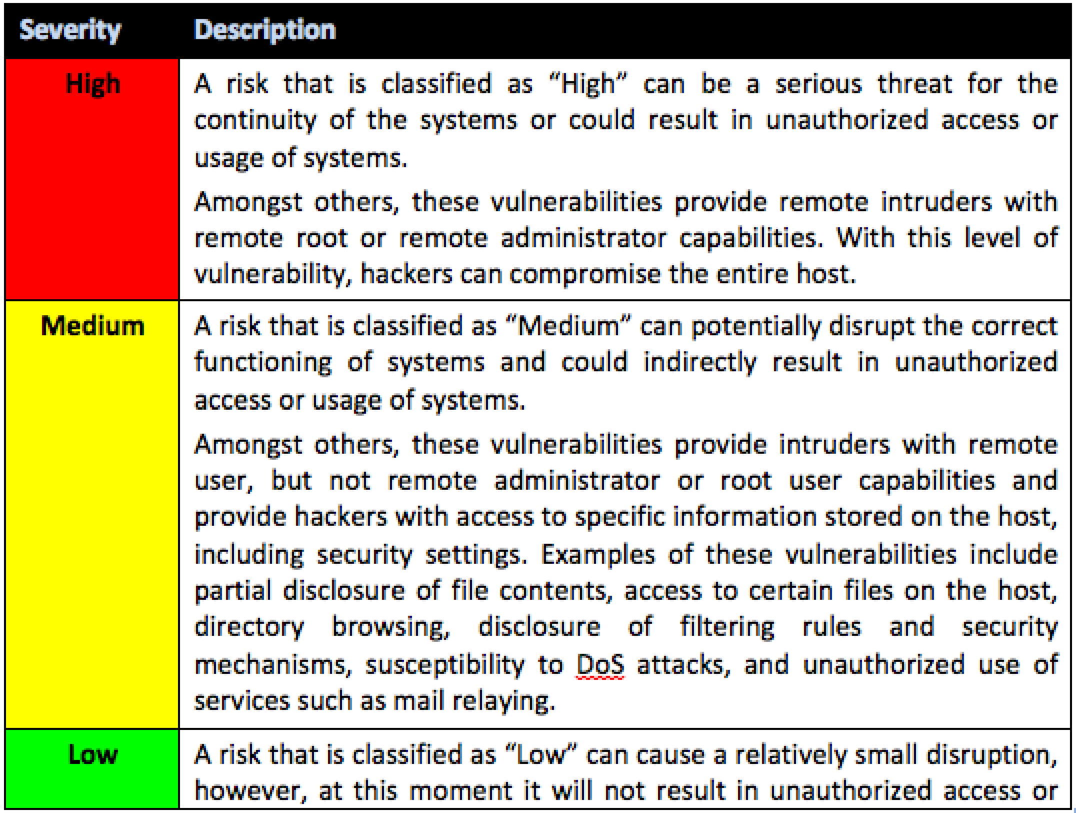
FINAL ANALYSIS

List of findings

No	Finding	Affected Host(s)
1	Remote File Inclusion (RFI)	172.16.184.7
2	RealVNC Remote Authentication Bypass	172.16.184.9
3	HTTP TRACE / TRACK Method	172.16.184.7
4	FTP Clear Text Protocol	172.16.184.9
5	Sharing of passwords	172.16.184.9 10.2.1.9 10.2.1.20

FINAL ANALYSIS

Risk Rating Chart



Severity	Description
High	A risk that is classified as "High" can be a serious threat for the continuity of the systems or could result in unauthorized access or usage of systems. Amongst others, these vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host.
Medium	A risk that is classified as "Medium" can potentially disrupt the correct functioning of systems and could indirectly result in unauthorized access or usage of systems. Amongst others, these vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities and provide hackers with access to specific information stored on the host, including security settings. Examples of these vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to DoS attacks, and unauthorized use of services such as mail relaying.
Low	A risk that is classified as "Low" can cause a relatively small disruption, however, at this moment it will not result in unauthorized access or

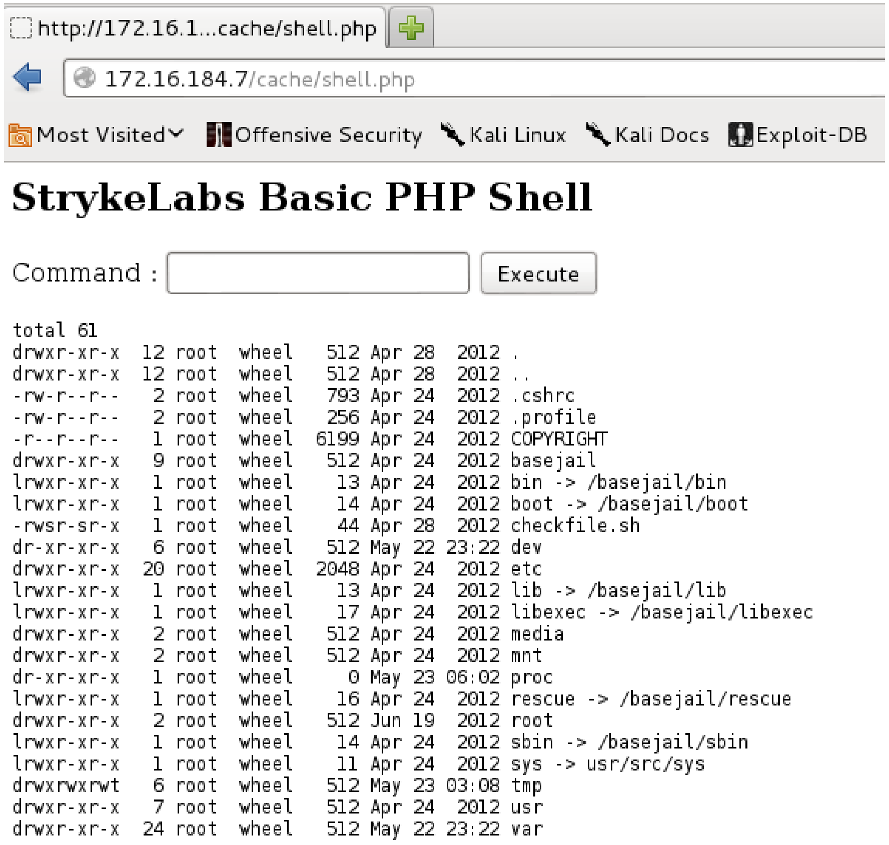
FINAL ANALYSIS

Finding #1: Remote File Inclusion (RFI)

- Vulnerability is easy to exploit.
- Likelihood of exploitation is high.
- Exploitation result in remote command execution with limited privileges.
- Possible for attacker to attach malicious code in web pages to attack unsuspecting visitors.
- Vulnerability is remotely exploitable and exposed to the Internet.
- Risk Rating: High

FINAL ANALYSIS

Finding #1: Remote File Inclusion (RFI) Evidence


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

```
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
```

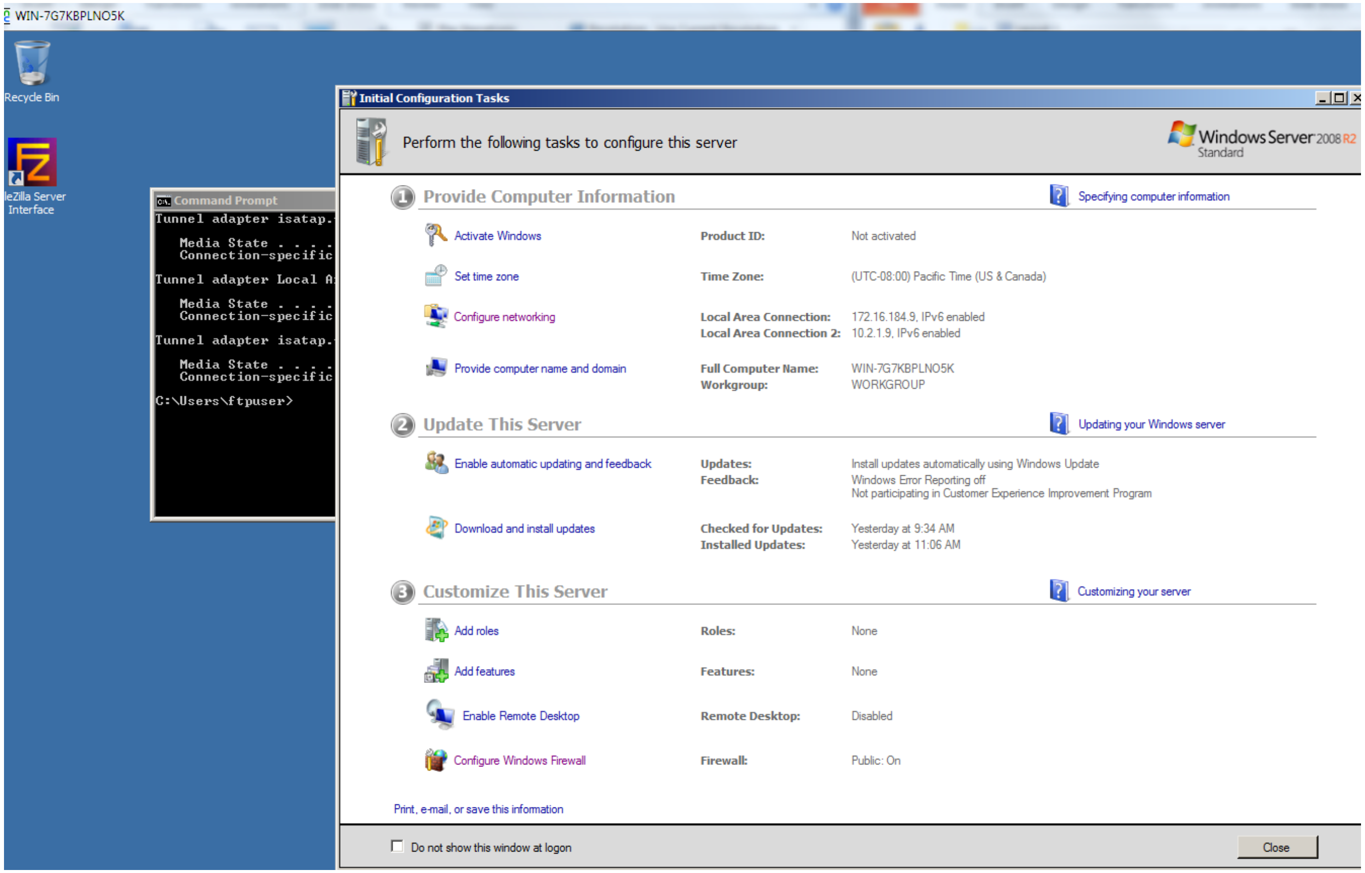
FINAL ANALYSIS

Finding #2: RealVNC Remote Authentication Bypass

- Vulnerability is easy to exploit.
- Likelihood of exploitation is high.
- Exploitation result in total compromise with SYSTEM privileges.
- Compromised server is connected to the internal network.
- Vulnerability is remotely exploitable and exposed to the Internet.
- Risk Rating: High

FINAL ANALYSIS

Finding #2: RealVNC Remote Authentication Bypass Evidence



```
Tunnel adapter isatap.
   Media State . . . .
   Connection-specific

Tunnel adapter Local A

   Media State . . . .
   Connection-specific

Tunnel adapter isatap.

   Media State . . . .
   Connection-specific

C:\Users\ftpuser>
```

Perform the following tasks to configure this server

1 Provide Computer Information — Specifying computer information

Activate Windows	**Product ID:**	Not activated
Set time zone	**Time Zone:**	(UTC-08:00) Pacific Time (US & Canada)
Configure networking	**Local Area Connection:** **Local Area Connection 2:**	172.16.184.9, IPv6 enabled 10.2.1.9, IPv6 enabled
Provide computer name and domain	**Full Computer Name:** **Workgroup:**	WIN-7G7KBPLNO5K WORKGROUP

2 Update This Server — Updating your Windows server

Enable automatic updating and feedback	**Updates:** **Feedback:**	Install updates automatically using Windows Update Windows Error Reporting off Not participating in Customer Experience Improvement Program
Download and install updates	**Checked for Updates:** **Installed Updates:**	Yesterday at 9:34 AM Yesterday at 11:06 AM

3 Customize This Server — Customizing your server

Add roles	**Roles:**	None
Add features	**Features:**	None
Enable Remote Desktop	**Remote Desktop:**	Disabled
Configure Windows Firewall	**Firewall:**	Public: On

Print, e-mail, or save this information

☐ Do not show this window at logon

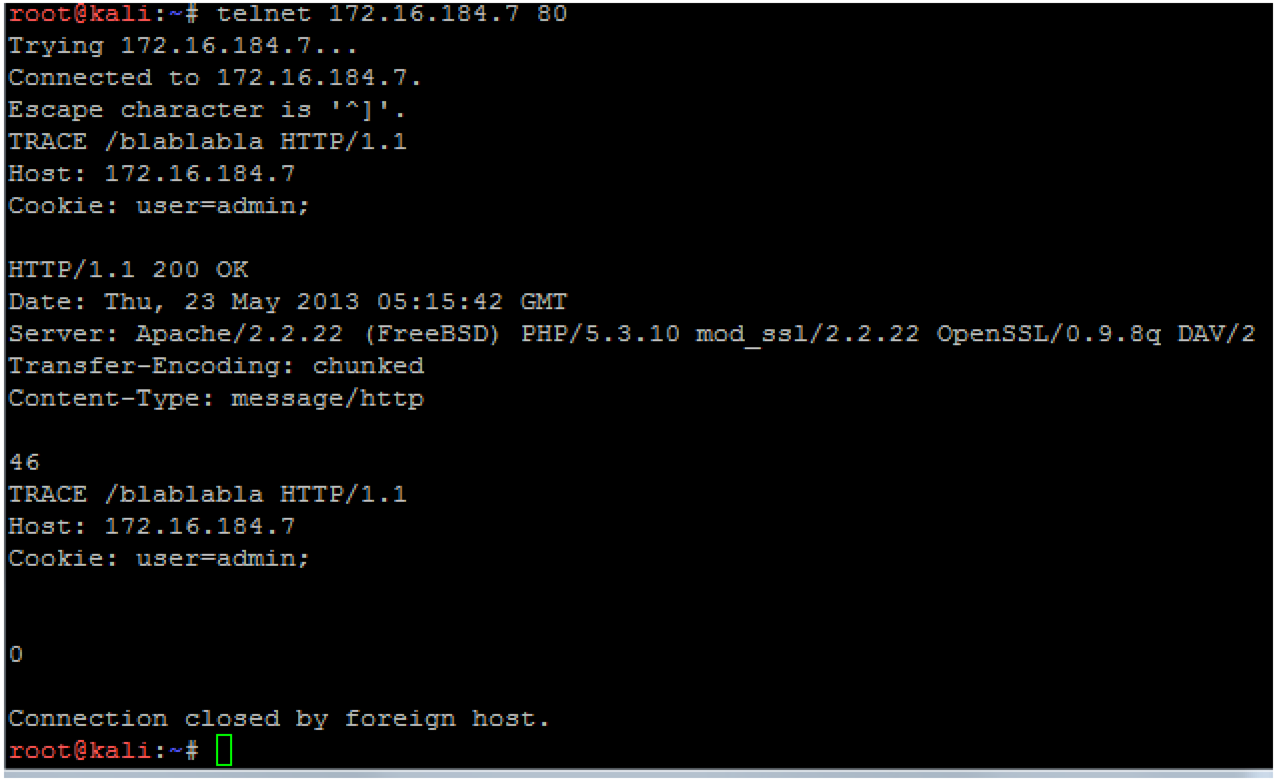
FINAL ANALYSIS

Finding #3: HTTP TRACE / TRACK Method

- Vulnerability requires dependencies to achieve full potential.
- Likelihood of exploitation is low.
- Successful exploitation may result in theft of credentials.
- Risk rating: Low

FINAL ANALYSIS

Finding #3: HTTP TRACE / TRACK Method Evidence



```
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:~# 
```

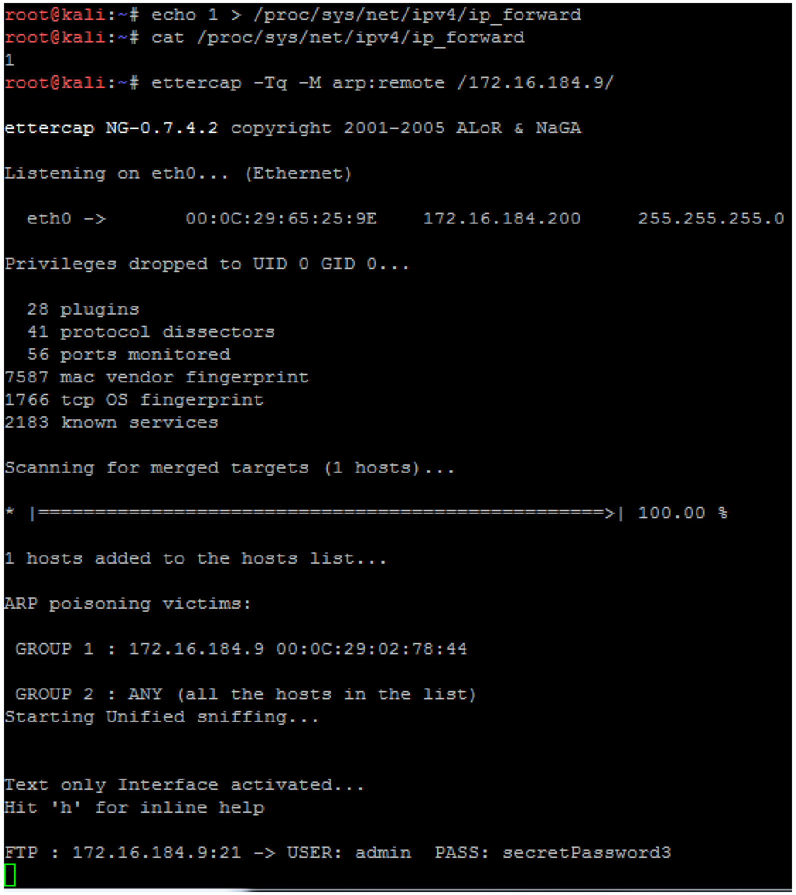
FINAL ANALYSIS

Finding #4: FTP Clear Text Protocol

- FTP transmission in plain text.
- FTP credentials may be stolen via packet sniffing / MITM attacks.
- Likelihood of exploitation is low
- Risk rating: Medium

FINAL ANALYSIS

Finding #4: FTP Clear Text Protocol Evidence



```
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
```

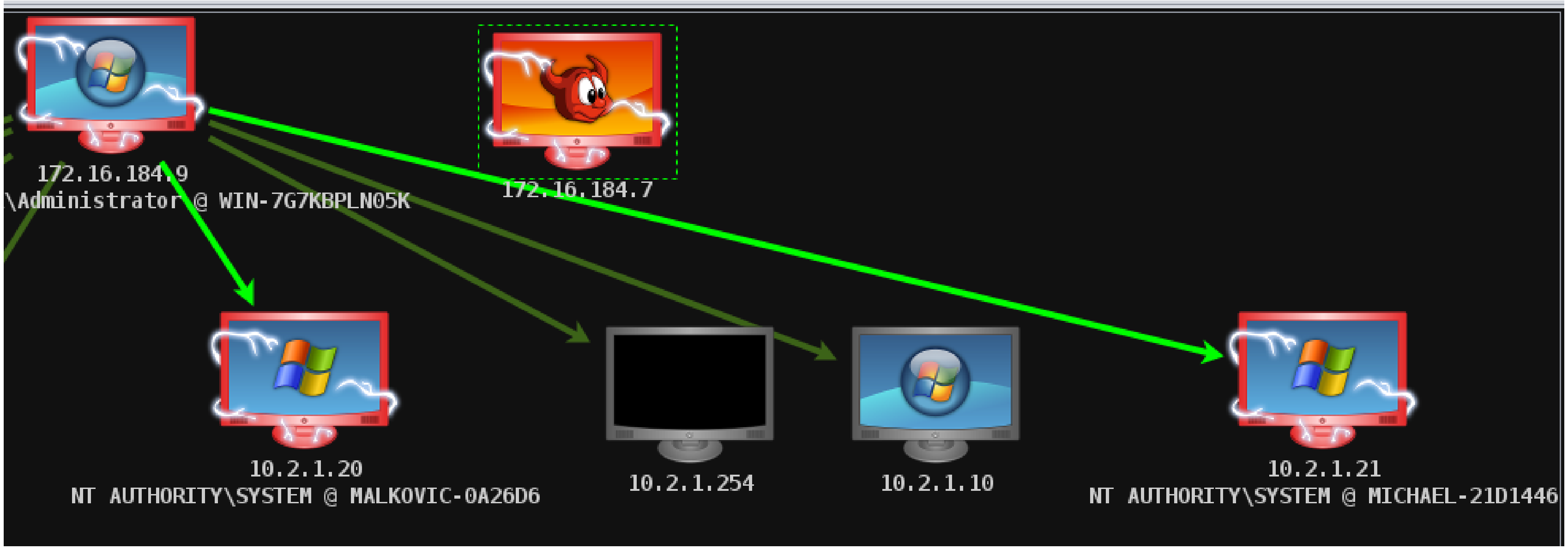
FINAL ANALYSIS

Finding #5: Sharing of passwords

- Local system credentials on FTP server is used in another internal server.
- Gives SYSTEM privileges.
- Likelihood of exploitation is high.
- Exploitation results in full system compromise.
- Risk rating: High

FINAL ANALYSIS

Finding #5: Sharing of passwords Evidence


172.16.184.9
\Administrator @ WIN-7G7KBPLN05K
172.16.184.7
10.2.1.20
NT AUTHORITY\SYSTEM @ MALKOVIC-0A26D6
10.2.1.254
10.2.1.10
10.2.1.21
NT AUTHORITY\SYSTEM @ MICHAEL-21D1446

REPORTING

- A pentest is not useful without comprehensive documentation/reporting.
- The report serves as an explanation of the various vulnerabilities that were discovered and the criticality of each vulnerability.
- Reports should contain the following sections
  - Executive summary.
  - Technical findings.
  - Evidence.

REPORTING

- Executive Summary - A summarization of the overall pentest and critical findings. It must also include the following information:
  - Summary of results.
  - Scope of work.
  - Project objectives.
- Technical Findings - Technical details of each finding. Should include the following:
  - Risk rating.
  - Vulnerability description.
  - Affected hosts / URL's.
  - Impact.
  - Recommendations.
- Evidence – Screenshots of each vulnerability discovered.

REVIEW

- Findings must be assessed to conclude the final risk rating.
- A report must accommodate the following audiences:
  - Management & Executive staff.
  - Technical IT staff.
  - The management summary must be easy for management staff members to comprehend.
  - Each finding must be accompanied by a piece of evidence.