

SANS

www.sans.org

SECURITY 504
HACKER TECHNIQUES,
EXPLOITS AND
INCIDENT HANDLING

504.6

Hacker Tools Workshop

The right security training for your staff, at the right time, in the right location.

Copyright © 2012, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

IMPORTANT-READ CAREFULLY:

This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA. If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware. BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE. The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the SANS Institute. Additionally, user may not sell, rent, lease, trade, or otherwise transfer the courseware in any way, shape, or form without the express written consent of the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

Hacker Exploits Workshop and Capture the Flag Event

Security 504 Day 6

SANS and Ed Skoudis

Copyright 2012, Ed Skoudis and SANS
Version 1Q12

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

1

Welcome to Computer and Network Hacker Exploits and Capture the Flag Event. Today, we are going to apply what we have learned in this class by getting hands-on experience with the tools and exploits. These exercises will underscore the importance of the defensive techniques we've discussed.

THIS CLASS ASSUMES THAT YOU HAVE ATTENDED SECURITY 504, DAYS 1, 2, 3, 4, and 5.
YOU SHOULD BRING THE BOOKS FROM ALL OF THOSE CLASSES FOR REFERENCE FOR THIS CLASS.

Table of Contents

	Slide #
• Getting Networked.....	4
• Workshop Objectives	11
• Class Structure.....	13
• Keeping Track of Your Work.....	14
• Tools To Use Today.....	22
• Legal Lawyer Stuff	24
• Ground Rules.....	25
• Key Steps To Exploiting Systems	31
• Step 1: Reconnaissance.....	32
– Whois Lookup	34
– DNS Zone Transfer.....	39

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

2

These slides are essentially a table of contents.... Use them for future reference, if you'd like.

THE MOST IMPORTANT SECTION IN TODAY'S BOOK IS THE ONE SPELLING OUT THE GROUND RULES. MAKE SURE YOU FOLLOW THE GROUND RULES!

Ignoring the ground rules could subject you to ejection from the class and the conference! That would be very, very unfortunate, so do yourself a favor: FOLLOW THESE SIMPLE AND REASONABLE GROUND RULES!

Table of Contents

	Slide #
• Step 2: Scanning	41
• Step 3: Exploiting Systems	45
– Compromising Additional Machines	48
• Step 4: Keeping Access	49
• Step 5: Covering the Tracks	51
• Building a Lab at Home and Conclusions.....	53
• Capture the Flag Rules.....	55
• LET THE GAMES BEGIN!.....	59

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

3

These slides are essentially a table of contents.... Use it for future reference, if you'd like.

Good Morning! Getting Networked...

- Please get yourself networked
- Your Windows IP address is 10.10.76.X
 - X comes from the room monitors
 - Show them your MAC address, and they'll give you X
- Netmask=255.255.0.0
- DNS=10.10.10.45
- No Default Gateway
- Your Linux IP address will be 10.10.75.X
- If you need additional addresses, please use 10.10.77.X, and so on
 - X always stays the same for a given student
 - Network all of your Operating Systems (Windows, Linux, Mac OS X, MVS, VMS, BeOS, Vic 20, etc.)

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

4

Please get yourself networked.

--> You should be able to ping 10.10.10.45.

If you can ping it from all of your OSs, you are ready to go.

For help getting networked, please see me.

YOU DO NOT HAVE PERMISSION TO ATTACK YET!!! NO SCANS, NO ZONE TRANSFERS, NO PROBES... NOTHING!! ONLY ICMP ECHO REQUEST MESSAGES WITH NO PAYLOAD TO 10.10.10.45.

Getting Networked

- DON'T PLACE YOURSELF ON 10.10.10.X
 - You are asking to be attacked if you do
 - If you want to be attacked, let me know, and I'll give you an address on 10.10.10.X specifically for you
- If you really want to be a target, let the instructor know
 - The instructor will assign you an address on 10.10.10, and will announce that to the other people in the class

Our network is flat. No routers are in use here. Your focus should be on compromising the end systems to gather their flags, not on reverse engineering a network architecture.

Whatever you do, please do not place yourself on 10.10.10.X. That's the line of fire, and you very well may get hacked on that network. All of our targets will be on 10.10.10.X. If you really do want to be attacked, let me know, and I'll give you an address on 10.10.10.X specifically for you. I'll announce to the other participants that this is a student who has volunteered to enter the target network, so they know that this new target isn't one that is officially part of the game.

Setting Up Windows

- Access your network set-up
 - Access your network interfaces by running `ncpa.cpl`
`C:\> ncpa.cpl`
 - Choose your Local Area Connection
 - Select TCP/IPv4 and click on "Properties"
 - Set this to your given IP address: 10.10.76.X
 - Subnet mask should be 255.255.0.0
 - Preferred DNS Server is 10.10.10.45
 - No default gateway (leave it blank)

You should know how to configure your Windows networking. Just in case you don't, here are some hints.

Setting Up Linux Networking

- Edit the network config using your favorite editor, such as:
gedit /etc/sysconfig/network-scripts/ifcfg-eth0
- In these files, edit the following lines to give them these values:
BROADCAST=10.10.255.255
IPADDR=[Your Assigned Address, such as 10.10.75.X]
NETMASK=255.255.0.0
NETWORK=10.10.0.0
DNS1=10.10.10.45
- For the changes to take effect, you must restart your interface by typing:
service network restart

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

7

In Linux, give yourself the following network settings by editing **/etc/sysconfig/network-scripts/ifcfg-eth0**:

```
BROADCAST=10.10.255.255
IPADDR=[Your Assigned Address, such as 10.10.75.X]
NETMASK=255.255.0.0
NETWORK=10.10.0.0
DNS1=10.10.10.45
```

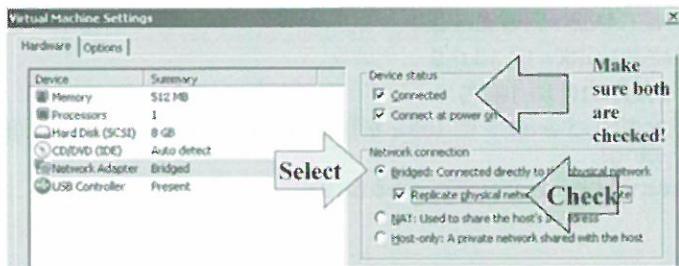
To apply these changes, run this command:

```
# service network restart
```

VMware Bridged Networking

- In VMware, used Bridged networking
 - Host-only doesn't make sense
 - NAT will get in your way

VMware
Under VM→
Settings



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

8

Configure your guest machine to use bridged networking. In VMware (Workstation or Player), go to VM→Settings. Click on “Network Adapter”, and select “Bridged” networking. Select “Replicate physical network connection state.” Then, make sure that you have a check next to “Connected” and “Connect at power on”.

Now, Disable Firewalls and Attempt to Ping

- Disable your Linux firewall by running:
`# service iptables stop`
- Disable your Windows firewall by running:
`C:\> netsh firewall set opmode disable`
- From your Windows machine, attempt to ping 10.10.10.45
`C:\> ping 10.10.10.45`
- From Linux, attempt the same thing:
`$ ping 10.10.10.45`
- If you are networked, you are ready to go
 - Please wait for the instructor to officially begin the Capture the Flag exercise

Once you have configured your host and guest IP addresses, as well as VMware for Bridged networking, please disable the firewalls on both operating systems so you can communicate freely across the network, using the commands on the slides above. Then, attempt to ping 10.10.10.45 from both Windows and Linux.

If it is working, you have successfully networked your system for the Capture the Flag event. Please do not attack the target machines yet. Instead, wait for the instructor to officially begin the Capture the Flag exercise.

If your networking doesn't work, it may be due to a bug in VMware, described on the next slide.

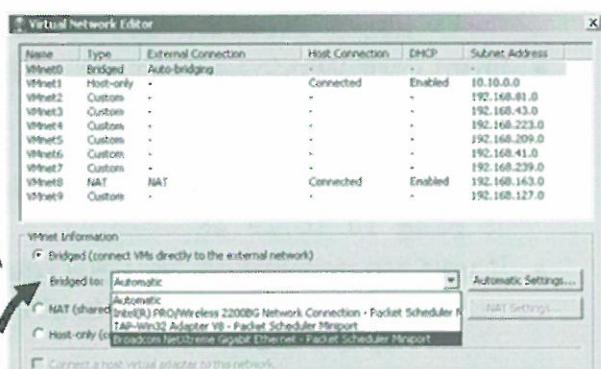
Possible Bug in VMware Networking

- In approximately 10% of systems, VMware bridges to the wrong interface
- To fix this, in VMware Workstation, go to Edit→Virtual Network Settings
- Then, select the Host Virtual Networking Tab
- In VMware Player 3.0, you will need to extract an executable by running the original VMware Player installer package:

```
C:\> VMware-player-[version].exe /e C:\extract
```

- In the “extract” directory, find a file called “network.cab”
- In the Windows File Explorer, open the network.cab file
- Take the vmnetcfg.exe file from it, and copy it to c:\Program Files\VMware\VMware Player\
- Run vmnetcfg.exe

Drop this one down to your physical interface



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

10

Sometimes, when using bridged networking, VMware will not be able to connect the network interface VMnet0 to your physical interface automatically. You may see errors in the guest machine associated with a disabled interface, or sometimes even IP address conflicts when there are no conflicts.

To fix this problem, in VMware Workstation, go to Edit→Virtual Network Settings. Then, select the middle tab, called Host Virtual Network Mapping. Select VMnet0. Then, under the “Bridged” portion of the screen, select the drop down box to choose your physical Ethernet adapter. You can even do this while the virtual machine is running. No reboot is necessary.

Click “Apply” and then “OK”. Then, try again to ping 10.10.10.45.

In VMware Player versions less than 3.0, you can do this same thing by running a program in C:\Program Files\VMware\VMware Player\vmnetcfg.exe. Run that program, and make the same change you see above.

If you are in VMware Player 3.0 or later, you need to extract the vmnetcfg.exe program from the VMware installation package. You can do that by running the following commands:

```
C:\> VMware-player-[version].exe /e C:\extract  
C:\> cd c:\extract  
C:\> explorer .
```

Now, find the file called network.cab, and double click on it. Here you will see a file called vmnetcfg.exe. Copy this file to C:\Program Files\VMware\VMware Player\

Then, run the vmnetcfg.exe file to reveal the GUI shown above. Select your local area connection physical adapter in the “Bridged to:” drop down menu, and click “Apply” and then “OK”.

Workshop Objectives

- To tie together everything we have learned
- To show the steps attackers use to compromise systems
- To get you into the mindset of an attacker so that, as an incident handler, you can anticipate their moves
- To gain hands-on experience with various attack tools
- To understand how the defenses work and why they are important
- To play capture the flag, and to have some fun

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

11

These are the reasons we are here today:

- To tie together everything we have learned throughout the previous five days.
- To show the steps attackers use to compromise systems.
- To get you into the mindset of an attacker so that, as an incident handler, you can anticipate their moves
- To gain hands-on experience with various attack tools.
- To understand how the defenses work and why they are important.
- To play capture the flag, and to have some fun.

No Permission to Attack

YET

- You do not (yet) have permission to attack my machines
 - No scanning (yet)
 - No attacking (yet)
 - No intrusion (yet)
- Sit tight for a little bit while we provide a brief overview of the workshop
- While we are discussing this, please get yourself networked
 - You want to ping 10.10.10.45 from all of your operating systems
- The only thing allowed right now is ICMP Echo Request messages, with NO UNUSUAL PAYLOAD, to 10.10.10.45, and their associated responses
- If you are networked and bored... sniff... you will see interesting stuff
 - Just don't send any packets except those pings mentioned above

Just hang on for a little while. If you are already networked, you can start copying tools from the CD to your hard drive.

If your tools are all ready to go, please be patient. You'll be able to launch your attacks within half an hour.

The only thing allowed right now is ICMP Echo Request messages, with NO UNUSUAL PAYLOAD, to 10.10.10.45, and their associated responses.

You are allowed to do passive sniffing, if you'd like. You will see some interesting packets coming occasionally from 10.10.10.X.

Class Structure

- Approximately a half hour of lecture
- Rest of the day for your attacks
- At 2:30 PM, at second break, we will show you the vulnerabilities we expected you to find
 - You may find others... that's cool
 - You will have at least one more hour to attack after we show you the expected vulnerabilities

You will have plenty of time to attack the systems. Please get yourself networked.

At 2:30 PM, at our afternoon break, we will show you a vulnerability map describing the state of the systems when we arrived this morning. We'll go over each vulnerability and explain how it can be exploited. You may find other vulnerabilities beyond what we show at 2:30 PM... that's cool, and we welcome you to comment on your findings in class at 2:30 PM. Please feel free to dazzle the class with information about your brazen exploits (while following the GROUND RULES!).

You will have at least one more hour to attack after we show you the expected vulnerabilities. That way, you'll have all the vulnerability information you need, and can attack with full knowledge of the target environment.

Keeping Track of Your Work

- Just as we incident handlers and security personnel benefit from organizing our notes...
- ...Good attackers are organized and maintain good notes
- Fill out the following pages with server IP address information based on your discoveries
- Continue to update these pages with additional information throughout the day

Take detailed notes. Remember, information gathered from one system might be useful in attacking other systems.

Your Machine Information

- Host Name: _____
- Host IP Addr: _____
- Host OS: _____
- Host Version: _____
- Services: _____
- Notes: _____

You will receive your IP address from a room monitor. To get an IP address, you will be required to show the room monitor your badge and your MAC address.

Team's Machines' Information

- Please work in teams of two, three, four, or five people

• Host Name: _____
• Host IP Addr: _____
• Host OS: _____
• Host Version: _____
• Services: _____
• Notes: _____

• Host Name: _____
• Host IP Addr: _____
• Host OS: _____
• Host Version: _____
• Services: _____
• Notes: _____

• Host Name: _____
• Host IP Addr: _____
• Host OS: _____
• Host Version: _____
• Services: _____
• Notes: _____

• Host Name: _____
• Host IP Addr: _____
• Host OS: _____
• Host Version: _____
• Services: _____
• Notes: _____

I strongly encourage you to work in a team of two, three, four, or five people. That's how many attackers work. Also, you will learn far more if you work with a team throughout the day. You'll get further, and perhaps make a new friend, although there are no guarantees. ☺

Target Information - 1

- Target Host Name: _____
- Target IP Addr: _____
- Target OS: _____
- Server Version: _____
- Ports/Services: _____
- Users/Passwords: _____
- Notes: _____

You will be filling these sheets out with the information you discover during your scans and attacks.

Target Information - 2

- Target Host Name: _____
- Target IP Addr: _____
- Target OS: _____
- Server Version: _____
- Ports/Services: _____
- Users/Passwords: _____
- Notes: _____

You will be filling these sheets out with the information you discover during your scans and attacks.

Target Information - 3

- Target Host Name: _____
- Target IP Addr: _____
- Target OS: _____
- Server Version: _____
- Ports/Services: _____
- Users/Passwords: _____
- Notes: _____

You will be filling these sheets out with the information you discover during your scans and attacks.

Target Information - 4

- Target Host Name: _____
- Target IP Addr: _____
- Target OS: _____
- Server Version: _____
- Ports/Services: _____
- Users/Passwords: _____
- Notes: _____

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

20

You will be filling these sheets out with the information you discover during your scans and attacks.

You may even find more servers on the 10.10.10.x network. Write notes about such servers below.

Or, Create a Spreadsheet

- Another valuable way to sort what you find today is to create a spreadsheet (either in software or even on paper)

Target IP Addr	Target name	Target OS	Listening Ports	Known Vulns	Admin Accts / Passwds	Other Accts / Passwds	Misc Notes

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

21

Another format that is especially useful when doing penetration exercises is a spreadsheet of all findings so far, recording each cell in the spreadsheet as you discover new information. You may want to do this for your work today, either in a software spreadsheet or even on paper.

Most Important Tools to Use Today

- Very Important:

- Nmap – port scanning and OS Fingerprinting (Linux)
- Nessus – vulnerability scanning (Linux)
- Netcat – backdoors and file transfer (Windows and Linux)
- Enum – determining users & groups, and password guessing (Windows)
- John the Ripper – password cracking (Linux and Windows)
- Fgdump – remote SAM password hash dumper (Windows)
- Metasploit – exploiting vulnerable targets (Linux and Windows)

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

22

You should attempt to use all of the Very Important tools (on your own or on a partner's machine). The others are nice to use, but are not essential.

A Note About Tools...

- Everything you need to win the game is included in this environment
- Look around on your DVD... you might find some useful items on there
- Ask for hints if required

You can win the capture the flag game with everything you have in this environment. Look around on the course DVD for interesting tools and features. Feel free to ask for hints about given tools.

Legal Lawyer Stuff

- Always get permission before attacking systems, even on your own network
- Only use them to test your own systems
- Unauthorized access BAD, protecting your network GOOD
- When the instructor says so, you will have permission to attack only 10.10.10.X (Not yet...)

I am not a lawyer and I do not play one on TV. However, I just want to make sure everyone realizes that the exploits and programs that we are going to cover today could get you into trouble if you use them improperly. We are covering them so that you can learn to protect your network and respond to attacks. In no way, shape, or form are we giving you a license to hunt. The tools should only be used to test your own network and only after you get the proper permission.

You do not have permission to attack yet. When I say so, you will be able to attack 10.10.10.X, subject to our ground rules.

Speaking of ground rules, let's discuss them in detail next.

Extremely Important Ground Rules (1)

- VIOLATE THESE GROUND RULES, AND YOU'LL BE DISMISSED FROM CLASS IMMEDIATELY
- Attack only the machines on network 10.10.10.X
- DO NOT EVER launch a Denial of Service attack on any system in this workshop
 - You will not be demonstrating any real technical knowledge, and will destroy the learning environment
- Also, DO NOT ARP-cache-poison our servers, as this will likely result in a Denial of Service attack
- Do not install Rootkits on my machines; you may cause unexpected problems

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

25

WAKE UP! This is important stuff for the rest of the day.

Attack only the target machines, which are all located on 10.10.10.x.

Denial of service attacks are strictly forbidden!

No ARP cache poisoning! That could turn into a Denial of Service Attack, if you aren't careful. Frankly, I don't want to risk it, and neither should you.

For Rootkits, you can install them on your own machine to experiment. However, do not install them on the class target servers (10.10.10.x). Replacing system executables or modifying the kernel can easily result in destroying the OS, which would damage the learning environment.

Please do follow these rules. They really aren't that onerous. They are mandatory!

Ground Rules (2) – Dealing with the Targets

- Do not connect our network to the outside world
- The workshop is for learning, not showing off or taking systems down
- Once you gain access to a machine, please do not close the security hole!!!
 - Others still need to learn after you get in
- Do not change the passwords on my machines
 - If you need other passwords, create other accounts
- Once you gain access, don't trash a machine
 - You can display messages on the screen to show the class your skills...
 - ...DO NOT display anything objectionable or obscene!

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

26

Please follow the ground rules. Not following the ground rules could result in dismissal from class.

Connections to the outside world (SANS' networks, hotel networks, or the Internet) are strictly forbidden.

Don't trash a machine, or fix a hole. If you do that, you'll destroy the learning environment, with its carefully placed security vulnerabilities, each designed to teach a specific lesson.

Ground Rules (3) – Play Nicely with Others

- Identify one or more partners to work with
 - You will get more done and learn more with partners
 - The attackers work together... so should you!
- Do not attack your fellow students
- Some people will move faster than others; that's OK
- On occasion, I will need to reboot a target box... some exploits break services requiring a reboot

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

27

Please follow the ground rules. Not following the ground rules could result in dismissal from class.

Work with a partner, and, above all, do not get frustrated! Ask for help, if you need it.

Ground Rules (4) – Using Extra Tools

- Use any tool you have (for commercial tools, you must have a legal license!)
- If you need another type of tool or exploit, please feel free to download it (legally) from the Internet
 - Leave the room to do so... no wireless
- DO NOT run any attack tools on the terminal room network!
 - Hacking the terminal room or through the terminal room = automatic dismissal!

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

28

Please follow the ground rules. Not following the ground rules could result in dismissal from class, especially the rule about not attacking the terminal room!

Do not pirate software! That violates SANS' rules, and is ethically wrong.

If you need another tool, feel free to download it from the Internet, provided that you have a legal license.

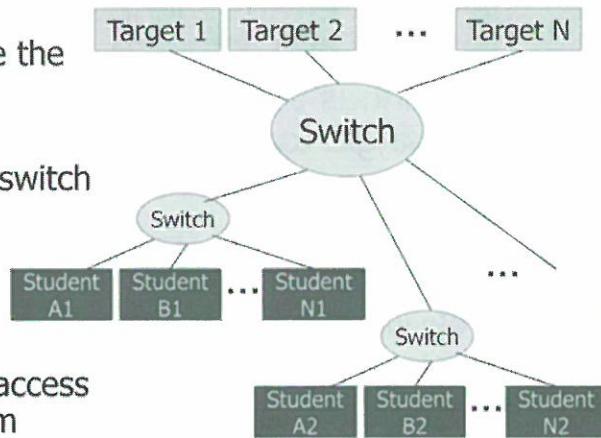
Final Ground Rules - (5)

- Many of the Linux tools depend on a very particular environment, impacted by both hardware and software
- Try various tools, but DO NOT get bogged down on a single tool
 - Move on to another tool
- It is the students' responsibility to get the tools compiled and running
 - We will give pointers to help you
- The five best tools to learn are Nmap, Enum, Nessus, Metasploit, John the Ripper, and Netcat

Feel free to use any tools for which you have a legal license, but remember not to get stuck for more than 30 minutes on a single tool. Move on if it doesn't work, or try to have another team member run that tool. You can make great progress in the capture the flag game, if you are very clever, using only Nmap, Enum, Nessus, Metasploit, John the Ripper, and Netcat. However, other tools can help you to win even faster. You can refer to the Linux mini-workshop in the back of book 504.1 for additional tips on Linux.

Network Layout

- IP addresses assigned when you came in
- Each person should use the assigned address
- Switch at each table
- Switch is connected to switch in front of the room
- No routers or firewalls
- No direct connection to the Internet
- No wireless – wireless access is forbidden in this room



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

30

If you use wireless LAN cards, there is a chance that you will inadvertently bridge the whole class to the Internet. The class would then, potentially, leak attack packets on to the public Internet. We must avoid this, so wireless LAN cards are forbidden.

Key Steps to Exploiting a System

1. Reconnaissance
2. Scanning
3. Exploiting Systems
 - Gaining Access
4. Keeping Access – Backdoors and Trojans
5. Covering the Tracks

Mostly
Simulated

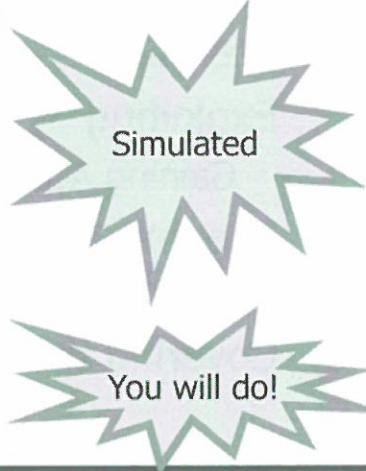
You will
do these!

As we have discussed throughout this session, these are the steps an attacker would use to conquer a system. These items are what you need to understand and protect against. We will actually try out each of these steps.

Here's the scenario: we're performing a penetration test of a target organization by running through these phases. Your goal is to break into as many target systems on the 10.10.10.X network as possible, with the highest privileges you can achieve.

Step 1: Overview of Reconnaissance

- Acquire Domain Name
- Open Source
- Whois lookup
- ARIN lookup
- DNS Interrogation



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

32

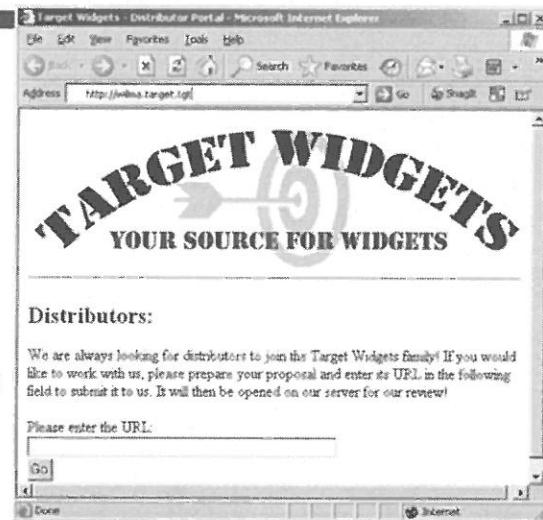
Step 1 is casing the joint. Because we have no Internet connection, most of this phase will be simulated.

We'll walk through the steps performed during normal recon, telling you the results you would have gotten in a real penetration attempt.

However, you'll be performing the last element of recon, DNS Interrogation, on your own against one of our servers.

Acquire Domain Name

- No connection to the Internet (we want to control the environment), so we will simulate the next steps
- Let's pick a target organization
- How about an organization named "SANS 504 Target Company" with domain name "target.tgt"?
- They are the owner of Target Widgets, producer of the finest Widgets in the world
- Analyze their web sites and think about the business service that each offers



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

33

In order to get started, we need to pick a target organization. Just for reference purposes only, let's pick a sample organization named "SANS 504 Target Company". This company owns a company called "Target Widgets", which produces some of the finest widgets in the world.

When you analyze their websites, try to think about what each one is doing from a business perspective. That'll help you sort out your planned attack.

Whois Search

- Look up target.tgt at www.internic.net
- Reveals nameserver names
- Shows last update
- Also reveals the registrar

The screenshot shows a web browser window with the URL http://reports.internic.net/cgi/whois?whois_nc=target.tgt&type=domain. The page title is "InterNIC". The search results for "target.tgt" show the following information:

```

Whois Server Version 1.3

Domain Name: TARGET.TGT
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: FRED.TARGET.TGT
Name Server: FRED.TARGET.TGT
Status: ACTIVE
  
```

Computer and Network Hacker Exploits - ©2012 All Rights Reserved 34

Here is the result we get when we perform a whois lookup of our target site (target.tgt) using www.internic.net. Remember, this is a completely hypothetical search; there is no real “SANS 504 Target Company” in the outside world. This InterNIC record is simulated.

Note the very relevant information here: the target DNS server name is fred.target.tgt, and this domain was registered with www.networksolutions.com. Next, we'll interrogate this network solutions whois server for more details.

Whois – Detailed Search (1)

TARGET.TGT

Registrant:

Johnson, Bob "Nugget"
(BN160) bob@target.tgt
555 Main St.
City, State Zip
222-555-1212

Technical Contact:

Falken, Professor
(FF1243)
333 State St.
City, State Zip
444-555-6541 (FAX) 444-
555-6551

Billing Contact:

Smith, Susan (ZQ1458)
susan@target.tgt
666 Acorn Ave.
City, State Zip
777-555-1212

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

35

Here is some additional useful information associated with our target domain. Note those interesting names, addresses, and phone numbers.

Whois – Detailed Search (2)

```
Record expires on 22-Jun-2013.  
Record created on 22-Jun-2001.  
Database last updated on 22-Mar-2012  
15:58:44 EST.
```

```
Domain servers in listed order:
```

```
FRED.TARGET.TGT      10.10.10.45
```

```
*** Connection closed
```

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

36

Finally, at the end of the detailed record, we get the IP address of the DNS server for our target organization. We'll use this value shortly to attempt a zone transfer.

Remember that the target organization's DNS server is 10.10.10.45. That's hugely useful information.

Status

- Now we have a domain name (target.tgt) and the authoritative name server (fred.target.tgt at 10.10.10.45)
- Next, we need to find out some IP addresses to start mapping the network
- Let's try a zone transfer...

It's important to take inventory. What have we gotten so far? A target organization's name, a domain name, and a DNS server! Not bad for a few minutes' work.

Your Turn – Part II

- Now that we have covered a simulated reconnaissance phase, it will soon be your turn to use the tools
- When the instructor gives you permission to attack, you will start from this slide
- You may want to bookmark this page so you can easily come back

You may want to dog-ear or bookmark this page, as it is the place where you will return after the lecture component of this class.

DNS Interrogation – Zone Transfer

- To perform a zone transfer, we can use nslookup in Windows or dig in Linux

- Windows:

```
C:\> nslookup  
> server 10.10.10.45  
> ls -d target.tgt
```

- Linux:

```
# dig @10.10.10.45 target.tgt -t AXFR
```

- Goal is to harvest target IP addresses

Try to harvest domain names using nslookup in Windows or dig in Linux.

If zone transfers are blocked on these machines, we can skip this step and move on directly to scanning the 10.10.10.1-255 target network.

Status

- Now we have some more IP addresses valid for a given domain
- We want to find out the range of addresses
- Go to ARIN... hypothetically...
 - Submit query... answer comes back:
 - Target.tgt has been assigned 10.10.10.1-255
- We know a handful of systems and addresses from DNS, but there may be other addresses in use on the network

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

40

After a zone transfer of target.tgt or ping sweep of 10.10.10.1-255, you should have a series of IP addresses that you are ready to attack.

Key Steps to Exploiting a System

1. Reconnaissance
2. **Scanning**
3. Exploiting Systems
 - Gaining Access
4. Keeping Access –
Backdoors and Trojans
5. Covering the Tracks

Next, we move to scanning, whereby we'll try to find openings in the target machines.

Step 2: Overview of Scanning

- Ping Sweeping (Nmap)
- Port Scanning (Nmap)
- OS Fingerprinting (Nmap)
- Vulnerability Scanning (Nessus)
- Null Sessions (Windows)



Here are some of the elements of the scanning phase. You should try each of these to get maximum information about your target network.

Server Discovery - Exercise

- Using Nmap, try to fill out information about the target servers
- Use the templates on slides 16 to 20 of this book
- Draw a diagram of the network, based on the discovery phase (the diagram will be simple!)
- Include the following:
 - Topology layout
 - IP addresses
 - Open ports, with services and versions if possible
 - Operating system type

You could use Nmap to get detailed information about the topology, IP addresses, and openings on the target network.

Enum Against Windows

- Don't forget to run Enum against all discovered Windows machines
 - Enum with various flags will be useful:

```
C:\> enum -U [target_IP_addr]  
C:\> enum -G [target_IP_addr]  
C:\> enum -D -u [user] -f [password.lst] [target_IP]
```

Don't leave this section without trying the enum command against your Windows targets. It can turn up a good deal of useful information.

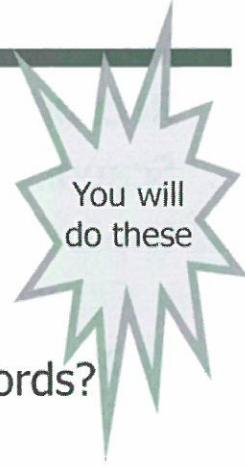
Key Steps to Exploiting a System

1. Reconnaissance
2. Scanning
3.  Exploiting Systems
 - Gaining Access
4. Keeping Access –
Backdoors and Trojans
5. Covering the Tracks

Now that scanning is complete, you can attempt to gain access.

Step 3: Gaining Access

- Run exploits
- Depends on what was discovered during Phase 2
- Common Windows exploits?
- Metasploit exploitation
- Easily guessed or cracked passwords?
- Buffer overflow vulnerabilities?
- Weak trust relationships?
- Others?



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

46

Your actions in Step 3 will depend heavily on what you found during your scanning step. The slide contains a few hints of the items you may discover.

Specific Exploits

- Using the information we discovered regarding ports and services, research known vulnerabilities
- Similarly, use the results of Nessus to determine exploit for a given vulnerability
- Look through Metasploit's capabilities to see how you can leverage them

Use the information from your scanning phase to determine what kind of exploits you should try. What did we cover in class that might be of use here? We specifically chose exercises in class to help you in this step. If you are having trouble here and get bogged down, by all means, please ask the instructor and/or proctors for help.

Compromising Additional Machines

- Once one machine is compromised, attackers can use it as a jumping off point for other attacks
 - Exploit Windows SMB sessions between target machines
 - Net use, at, etc.
 - Crack passwords, and look for systems where users have set up identical passwords on multiple machines

Remember, sometimes the easiest way in is through a full frontal assault on a machine. For other systems, the easiest way in is to use information you've plundered from other boxes, exploiting trust relationships or shared accounts/passwords on the boxes.

Key Steps to Exploiting a System

1. Reconnaissance
2. Scanning
3. Exploiting Systems
 - Gaining Access
- 4. Keeping Access –
Backdoors and Trojans**
5. Covering the Tracks

Once you gain a sufficient level of access, you may want to keep that access. You can do that by using backdoors (such as Netcat or VNC). Remember... NO ROOTKITS OR KERNEL-LEVEL ROOTKITS SHOULD BE INSTALLED ON THE TARGET SYSTEMS!

Step 4: Keeping Access

- Planting Netcat backdoor
- Use Metasploit shell or Meterpreter payloads
- Deploying VNC
- Others?
- DO NOT put Rootkits on my machines; too risky



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

50

Feel free to deploy application-layer Trojan Horse backdoors, like Netcat or VNC. Or, use Metasploit to exploit a target, gaining remote shell or Meterpreter access of it.

Key Steps to Exploiting a System

1. Reconnaissance
2. Scanning
3. Exploiting Systems
 - Gaining Access
4. Keeping Access –
Backdoors and Trojans
5. Covering the Tracks

Finally, we will experiment with different techniques for covering tracks, especially file hiding and covert channels.

Step 5: Covering the Tracks

- Creating hidden files on Linux
 - Directories named " "
- Creating hidden files on Windows
 - Alternate data streams
- Don't forget about shell history files!
 - Could be useful for you to see what others are attempting
 - You might want to cover your tracks by deleting your own shell histories on my machines



Computer and Network Hacker Exploits - ©2012 All Rights Reserved

52

Once you've broken in, feel free to experiment with the hiding techniques we discussed in class.

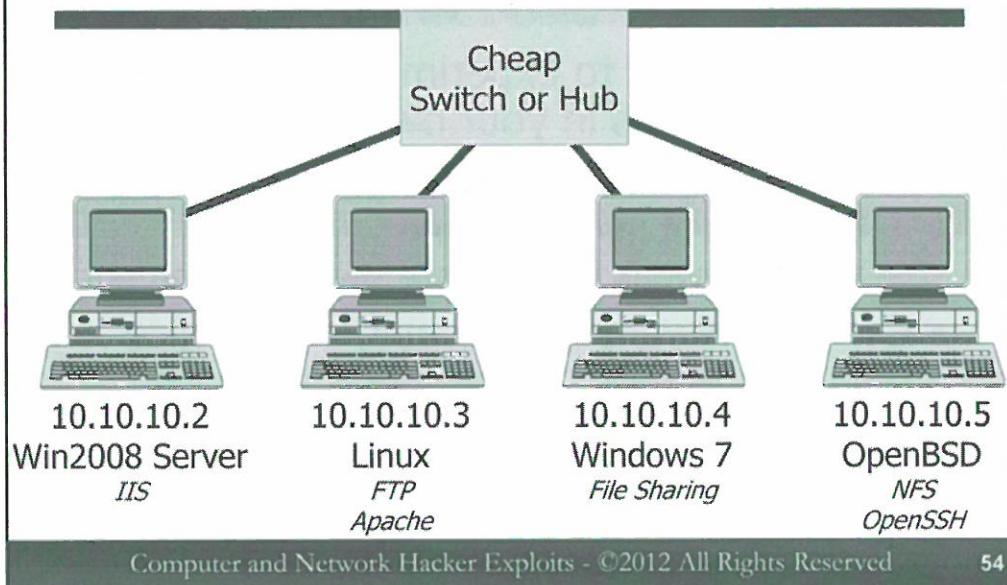
In particular, hide your tracks on Linux and Windows by concealing files.

Building a Lab at Home

- You may want to experiment with these and other tools in your own environments
- Here is a recommended architecture
 - I use this at my own home
 - You can tweak it to fit your own environment
- Or, get VMware or VirtualPC with a nice laptop, and carry the whole thing with you!

I frequently get asked about how to set up a network for this kind of analysis at home. The next slide shows you an architecture you could use for experimentation.

Recommended Test Lab Environment



You can vary operating systems, adding OpenBSD, Solaris x86, and other machines as needed.

You can also activate or install other services. The services listed above are just examples of what you might want to run on your test machines.

VMware can help make this type of laboratory more portable by running multiple virtual machines on a single physical box.

Capture the Flag Contest

- We'll be playing a game of capture the flag
- There are four regular flags and one bonus flag
 - flag1.txt, flag2.txt, flag3.txt, flag4.txt
 - ...and bonusflag.txt
 - All flags located in the top of the directory structure (inside c:\ on Windows and / in Linux)
- Each flag provides you information about a "Phrase that pays"
- Break in to my machines, look at the flags, and determine the phrase that pays

We'll be playing a game of capture the flag. I've got four flags on my machines, plus one bonus flag. You get to hack in and read the flags to determine the phrase that pays. The first one to determine the phrase that pays will win!

Capture the Flag Rules

- The first person to whisper the phrase to me wins the game
- You are not allowed to change any flags
- You are not allowed to delete any flags
- You are not allowed to plant false flags
- Read them, analyze them, and determine the phrase that pays
- Break these rules, and you will lose the game (and get kicked out of class)!

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

56

You must follow these rules to win the game. Violating these rules makes you ineligible to win.

The first person to whisper the phrase to me wins the game. Just come up to the front of the room, and tell me the phrase, or show it to me on your screen.

It's crucial to note that you are not allowed to change any flags, you are not allowed to delete any flags, and you are not allowed to plant false flags! If everyone follows these rules, we'll have a great game. If you violate the rules, you will be dismissed from class.

Are You Ready?

- Remember our process:
 1. Reconnaissance
 2. Scanning
 3. Exploiting Systems
 4. Keeping Access – Backdoors and Trojans
 5. Covering the Tracks
- Are there any questions on the ground rules or the Capture the Flag game?
- ASK NOW!!

Remember, follow these steps and the guidelines covered in this book. Are you ready?

Conclusions

- You must understand how exploits work in general
- With permission, take what you have learned and test your own network
- If you do not test it, attackers will

As we've said all week, it's important to understand the attacker's activities, so we can anticipate their moves and respond to them effectively. With the appropriate permission, take what you've learned here and apply it to your own environment.

LET THE GAMES BEGIN!!

You Now Have Permission

- You now have permission to attack my systems on the 10.10.10.x network in this room
- Anything on the 10.10.10.x network in this room is a valid target...
- ...just follow the ground rules!
- Ask the instructor or a proctor for help & hints
 - We're happy to give you hints, but won't tell you exactly how to succeed
- Social engineering of the system administrator is also acceptable, but it better be good! ☺
 - E-mail, help desk calls... no physical attacks, please

Computer and Network Hacker Exploits - ©2012 All Rights Reserved

59

Ok, let us begin.

Remember, ask the instructor and/or proctor for help if you get stuck. We are here to give you hints. Also, I'll act as the system administrator for the target machines. My job involves keeping them up in light of the many attacks we'll see today. Every now and then, the instructor may have to reboot a box... we'll work hard to keep that to a minimum, but it will occur.

Also, keep in mind that social engineering of the system administrator is also acceptable, but it better be good. Come see me if you think you have a clever social engineering exploit attempt.

