560.6
Penetration Test and Capture the Flag Workshop

SANS

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

SEC560.6 | Network Penetration Testing and Ethical Hacking

SANS

Penetration Testing Workshop

Welcome to SANS Security 560.6. Today, you conduct a penetration test of an example target enterprise. This section describes the challenge you will face and provides the Rules of Engagement and a description of how to conduct the day-long lab. This session focuses on the hands-on application of tools and techniques we've discuss throughout the class. Without further ado, let's begin.

Final Workshop Goals

- To apply what we've covered throughout the course, in a 1-day lab
- Hands-on, end-to-end penetration testing
- Instead of using tools one by one, you can use various tools together as components of your pen test
- The target enterprise is fictional:
  - But it models numerous vulnerabilities from real-world organizations
- ***If you are taking the course across the Internet via SANS vLive or SANS OnDemand, you will receive an e-mail with directions for getting networked using the VPN with your 560B credentials***
  - ***Please follow those directions so you that can ping 10.11.11.1***

The goal of the session today is to tie together concepts that we've covered throughout the entire 560 course, pulling them together in a full-day hands-on lab. You conduct a hands-on, end-to-end penetration test today.

Instead of using tools one-by-one, as you have for labs in the earlier components of the class, you now use the tools together to find and exploit vulnerabilities in a fictional target organization. Although the infrastructure is associated with a fictional company, we have tried to model real-world vulnerabilities, with lessons learned from actual, recently conducted penetration tests.

Note: if you are taking this course across the Internet via SANS vLive or SANS OnDemand, you will receive an e-mail from SANS NOC personnel with directions for accessing the target systems across the VPN. The VPN connection information used for 560.6 relies on a different configuration (560B certificates) than the one for the labs 560.2 to 560.5 (560A certificates). Follow those directions carefully, so you can get networked via VPN and ping 10.11.11.1. If you have any questions, please contact the SANS Support Staff at support@sans.org.

Organization of the Day

- Start with a lecture describing the scenario
- Your team then performs a penetration test of the target environment we have prepared for you
- At 2:30 p.m., we will conduct a final debriefing, revealing the secrets behind the challenge and various methods for successfully compromising the targets

This full-day session is organized into three phases. The first phase includes a short lecture that describes the goals for the day and lays out the scenario for the penetration test you will perform. This initial discussion lasts less than one-half an hour.

Then, you get to the largest part of the day: A penetration test of the target environment we have prepared for you. You are free to work through the breaks and lunch, but we do recommend taking a periodic break for a snack and to sort through your findings in the workshop so far.

At 2:30 p.m. we'll re-convene the class in lecture style, in which we'll do a final debriefing, where all secrets of the target environment will be revealed. We'll talk about the vulnerabilities present in the target systems and methods for conquering them.

Teams

- Work in a team of three and five people
- Make sure all team members record their discoveries, and have regular meetings to exchange ideas
  - We recommend that you get together each hour to brief each other and share ideas
  - A short (5 minutes) debriefing meeting every hour can help your progress

For today's session, you should work in a team of between three and five people. Do not work in teams larger than five people because it is too easy to lose sight of what's happening across a project in teams that grow too large, and you might miss important lessons from the day.

Make sure each person on your team records their progress and discoveries, in writing! Specifically, they should write down discovered vulnerabilities, account names, passwords, systems conquered, and so on.

We also strongly recommend that you have an hourly debriefing meeting with your team to discuss your findings so far, share information about what you've done and learned, and to plan the next hour's activities.

The RFP

- The 560 Global Conglomerate Corporation requires a penetration test
  - What do they do? They conglomerate, of course
  - They refer to themselves as "560GC" for short
  - While conducting their conglomeration business, they gather sensitive Personally Identifiable Information (PII)
  - 560GC needs to determine whether and how an attacker could get access to this information across the Internet
- Their domain name is 560gc.tgt
  - Fictional Top Level Domain (.tgt)

Next, look at the scenario you will be analyzing throughout this session. You have received a penetration testing project from an enterprise called "560 Global Conglomerate," called "560GC" for short. This organization issued an RFP that provides a high-level view of its infrastructure, the type of penetration test it requires, and an overview of the Rules of Engagement.

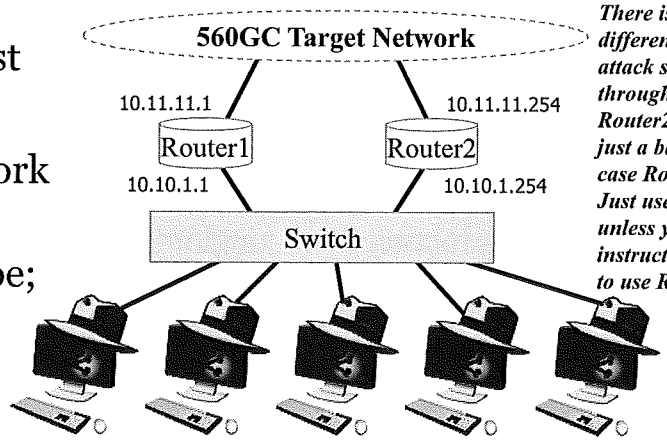
The 560 Global Conglomerate company is in the business of conglomeration. It is among the best conglomerators in the world.

In the process of conglomerating, 560GC gathers sensitive Personally Identifiable Information (PII) about its customers, including credit card numbers and other sensitive information. The RFP explains that 560GC needs to know whether this PII can be accessed by an attacker who targets its systems across the Internet.

The RFP specifies that the test is conducted on a black-box basis. That is, you will not be provided with a detailed diagram showing you the target systems, their addresses, and the infrastructure on which they reside. You should know, however, that their domain name is 560gc.tgt, which relies on a fictional top-level domain suffix of .tgt created for some SANS classes.

Project Scope

- Network services and web application penetration test
- No social engineering
- Everything on target network 10.11.11.2-253 is in scope
- The routers are *not* in scope; do not attack them
  - Router external interfaces are 10.10.1.1 and 10.10.1.254
  - Router internal interfaces are 10.11.11.1 and 10.11.11.254



There is no difference in the attack surface through Router1 or Router2. Router2 is just a backup in case Router1 fails. Just use Router1 unless your instructor tells you to use Router2.

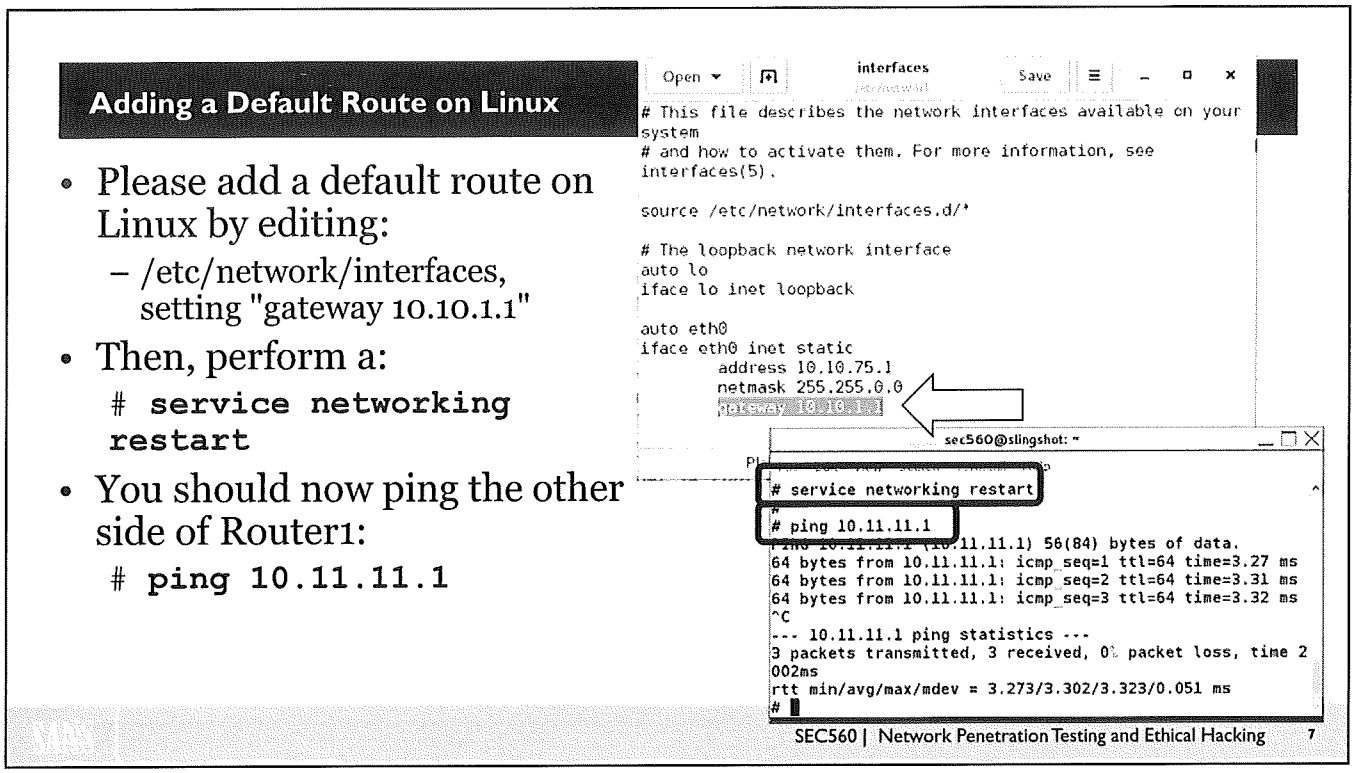
The RFP explains that you will be conducting a network services and web application penetration test. Social engineering is not within the scope of the project and should not be attempted.

The target network range for 560GC machines is 10.11.11.2-253. You can reach these machines by sending packets through one of two routers. One router is at 10.10.1.1, and the other is at 10.10.1.254. You can configure your systems to use either of these as your default route. On Linux, to set a default route, you can run this command:

```
# route add default gw [RouterIPaddr]
```

The routers, which have external IP addresses of 10.10.1.1 and 10.10.1.254 and internal IP addresses of 10.11.11.1 and 10.11.11.254, are NOT in the scope of the project. Do not attack the routers. Just let them route. You can send attack packets *through* them, but do not attack the routers themselves.

There is no difference in the attack surface through Router1 or Router2. Router2 is just a backup in case Router1 fails. Just use Router1 unless your instructor tells you to use Router2.



To get your system ready to engage in the workshop, make sure you set a default route in Linux to send all your packets through the router at 10.10.1.1. You need to edit /etc/network/interfaces, setting gateway 10.10.1.1 for eth0:

```
# gedit /etc/network/interfaces
```

At the end of the eth0 block, add a line that says:

```
gateway 10.10.1.1
```

Save the file and exit gedit. Now, restart your network interface:

```
# service networking restart
```

Finally, you should ping the far side of Router1, which will indicate that your routing is working:

```
# ping 10.11.11.1
```

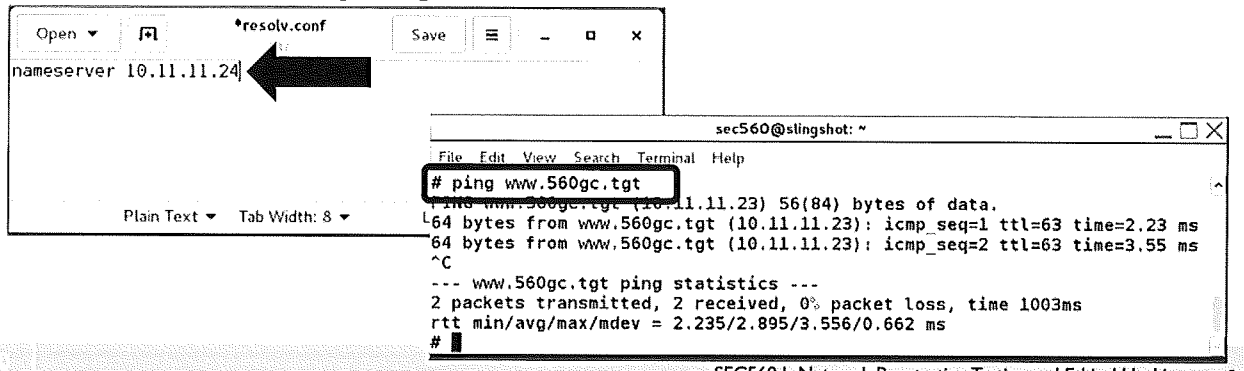
If you cannot ping it successfully, double-check your routing configuration inside of the /etc/network/interfaces file.

Configuring DNS on Linux

- To resolve names within Linux:
  - Edit /etc/resolv.conf, adding a line that says:

    nameserver 10.11.11.24
- Test that it is working by pinging www.560gc.tgt:

  # ping www.560gc.tgt



Now, configure your Linux machine to resolve names using DNS.

Edit the file /etc/resolv.conf:

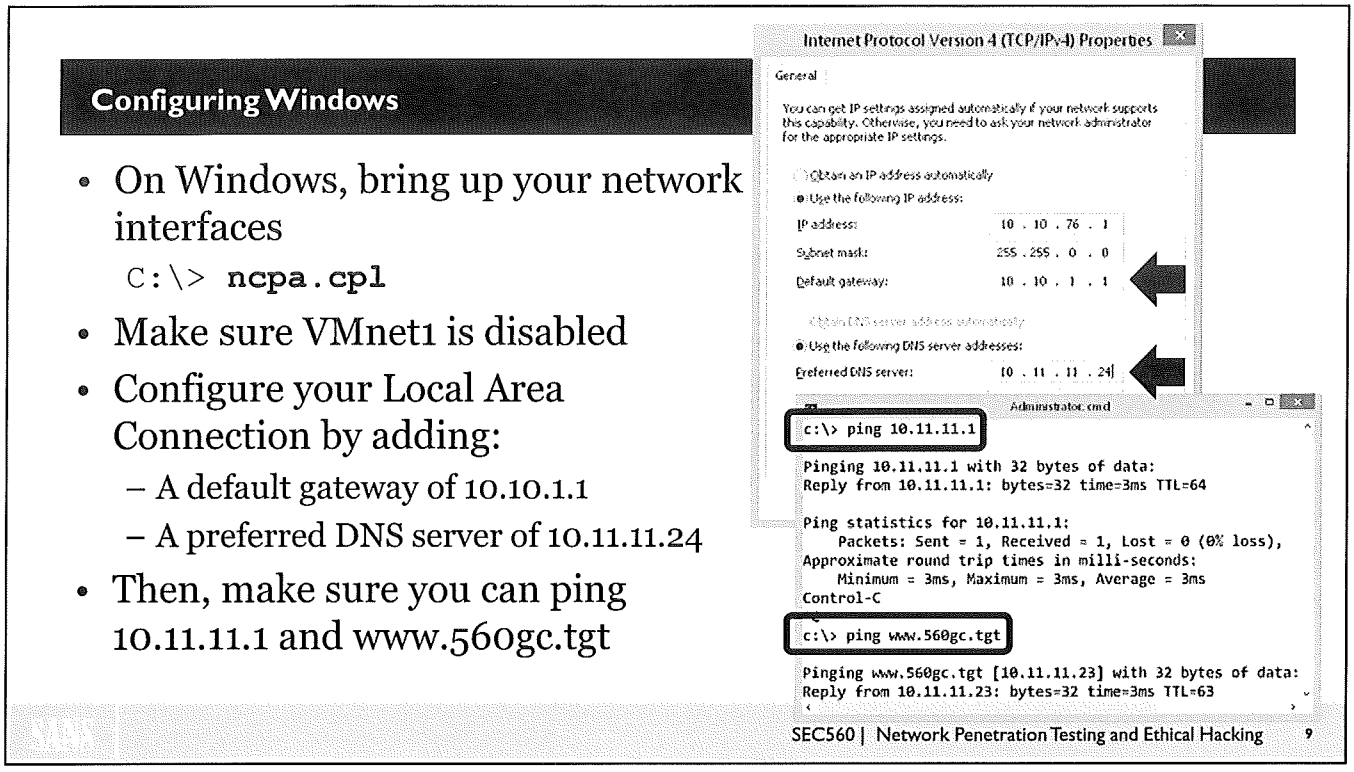
```
# gedit /etc/resolv.conf
```

Insert a line in that file that says:

```
nameserver 10.11.11.24
```

Save that file. Then, to test your DNS configuration, please try to ping www.560gc.tgt. If it pings successfully, you've resolved the name and your Linux system is configured properly for the network:

```
# ping www.560gc.tgt
```



Next, configure Windows with a default route of 10.10.1.1 and a DNS server of 10.11.11.24. Start by launching ncpa.cpl to get to your network interfaces:

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

Make sure VMnet1 is disabled by right-clicking it and selecting Disabled.

Then, double-click your Local Area Network Connection (or your Ethernet connection). Click Properties. Scroll down to Internet Protocol Version 4 (TCP/IPv4) and double-click that.

Keep your IP address set to 10.10.76.X, the same address you've used throughout the class.

Set your Default gateway to: 10.10.1.1
Set your Preferred DNS server to: 10.11.11.24

Click OK and then click OK again.

Now, ping 10.11.11.1. If you get a ping response, your routing is working in Windows.

```
C:\> ping 10.11.11.1
```

Then, ping www.560gc.tgt. If you get a response, your DNS resolution is working in Windows as well.

```
C:\> ping www.560gc.tgt
```

Additional Notes on 560GC Infrastructure

- 560GC operates a DNS server at 10.11.11.24
- This server is in scope and can provide you with useful information to get started
  - When the lab begins, try a zone transfer
- There may be additional targets not included in the zone file
  - Ping sweeps can help you identify them

560GC operates a DNS server located at 10.11.11.24. This server is a valid target, included in the scope of the project. When the lab begins, you should attempt a DNS zone transfer from this system, looking for hosts in the 560gc.tgt domain.

Note that it is possible that there will be target machines that do not have DNS records. Some will; others may not. Thus, your zone transfer will provide you a set of useful targets, but additional ping sweeping may find other targets as well.

Rules of Engagement

- No denial of service attacks
- No "dangerous" attacks
  - Don't risk bringing down our machines!
  - No performance-hogging attacks; this is a production environment
    - Don't do a full search of file system:
      - Don't run `find /` or `dir /s c:\`
  - When you gain access to a machine, don't delete items or plant false flags
- You need to help keep the infrastructure running
- Attack only the target infrastructure
  - You are not allowed to attack other testers

The Rules of Engagement set forth by 560GC prohibit all denial of service attacks. This lab represents a penetration test of a production environment, and you should avoid any activities that could break the target environment. Don't risk bringing down 560GC's machines. Do not conduct any denial of service attacks or other dangerous attacks that could bring services or systems down.

Also, try to avoid obviously performance-hogging activities, such as a comprehensive search of the file system, which would bog down a given machine. Everything you need to find in the target environments is located either at the top of the directory structure (c:\ on Windows and / on Linux) or in a user's home directory (`C:\Documents and Settings\[UserName]\` on Windows and `/home/[UserName]` on Linux). Do not run a **`find /`** or **`dir /s c:\`** command because that will slow the machine to a crawl.

Also, do not attack your fellow testers. Only machines on 10.11.11.2-253 are valid targets.

Additional Rules of Engagement

- You should not harden the target machines
  - That might break our production services
- You shouldn't weaken the targets either
  - Each is running a firewall
  - If you need to open a port through the firewall, that's okay
  - But don't disable the firewall entirely
- You are allowed to create new accounts on targets
  - Don't change the passwords of existing accounts, though
- You are allowed to install software on the targets, provided it doesn't break existing applications and services or require a reboot

We have some additional Rules of Engagement. Because this represents a production environment, do not harden the machines when you get access to them. Do not reconfigure them; do not activate a firewall; and do not patch them. The applications used by 560GC depend on some specific configurations and could break if you start hardening machines.

Likewise, do not weaken the targets either. Each target machine runs a firewall. You are allowed to poke holes through the firewall, opening ports on a one-by-one basis, but do not disable the firewall.

The Rules of Engagement do enable you to create accounts on the target machines, but do not change the password of any existing accounts.

And, finally, you are allowed to install software on the target machines, provided that the software you install does not interfere with any other functions on the systems. The software you install should also not require a reboot.

Monitoring Services

- We will monitor services throughout the day
  - Some systems will come down periodically for maintenance, which happens during real penetration tests, too
  - We will announce systems going down to let you know that they will be offline temporarily
- If you notice a service go down, let the system administrator know
  - The course instructor
- We will attempt to resume service as quickly as possible

As the workshop proceeds, we will monitor the services on the machines to verify that they function properly. Some services and systems will go down periodically for maintenance by the system administrator. Keep that in mind. This mimics real-world behavior of actual penetration tests. We will announce that it is undergoing maintenance so that you don't continue to attack a machine that is not available. (Such announcements are a luxury we usually don't have in a real-world penetration test, but we will do them here for this lab.)

If you do notice a system go down, let the system administrator (that is, the course instructor) know, so he can get it back into production. We will endeavor to get machines back in service as quickly as possible.

If a machine you are working to attack does go offline, start working on another target. Don't wait for the system to come back. Instead, move on.

Capture the Flag Goal

- Compromising 560GC's sensitive Personally Identifiable Information is your goal
- It is stored on the accounting server in a file called pii.csv, ***at the top of the directory structure***
- The file is encrypted using Gnu Privacy Guard
  - Multiple layers of encryption
- Encrypted, in this order, by users Kim, Lara, Sam, John, each for himself or herself
  - First encrypted by Kim, then by Lara, and so on.
- The "flags" in this challenge are the GnuPG private keys of these four users
- IMPORTANT NOTE: On Windows machines, GnuPG directories have the hidden attribute
  - Therefore, to see them in a cmd.exe shell, you have to run "dir /a" to show all files without regard to the attributes

Now, let's talk about the overarching goal for the Capture the Flag challenge that 560GC has issued for you in its RFP.

As mentioned earlier, the Personally Identifiable Information (PII) about its customers is the most sensitive item that 560GC has on its infrastructure. This PII information is stored on an accounting server, in a file called pii.csv. This file is at the top of the directory structure on the server(s) where it resides, in / on a Linux machine or c:\ on a Windows system.

Your goal is to get a copy of the clear-text pii.csv file. However, this file has been encrypted, using the Gnu Privacy Guard (GnuPG) encryption program. It has actually been encrypted by four different users. Kim encrypted it first, encrypting the file for herself using her own public key. Then, Lara encrypted it for herself, using her public key. Sam went next, using his public key. Finally, John encrypted it.

You need to get the file pii.csv and decrypt it, using the private keys of each user, following the reverse order in which the encryption was applied. To decrypt the file, therefore, you need to compromise the target machines to retrieve the GnuPG keyrings of each of those four users.

In essence, the flags for this Capture the Flag challenge are the GnuPG keyrings of these four users.

Note that on Windows, GnuPG directories have the hidden attribute set. Thus, from within cmd.exe, you should run dir /a to see all directories and files, with any attribute (hidden or otherwise) set.

Capture the Flag Approach

- You need to retrieve the encrypted pii.csv file
- You also need to retrieve the GnuPG keyrings of each of the four users
  - Stored under users' home directories in files called pubring.gpg and secring.gpg
  - Get both of those files for each of the four users
- Use GnuPG (on the course USB for both Windows and in the Slingshot Linux image) to decrypt the pii.csv file
  - Don't wait until you get all four sets of keys to start decrypting
  - When you get the appropriate keys, apply the first round of decryption:
    - That way, you can make sure keys are not corrupted and that you understand the decryption operations
- You win when you show the instructor the clear-text contents of the pii.csv file and explain how you got it to the instructor

Crucial!

For this scenario, you need to compromise the accounting server to get a copy of the pii.csv file. You also need to get the GnuPG keyrings of each of those four users. These keyrings hold the public and secret keys of each user. They are stored in the users' home directories in files called pubring.gpg and secring.gpg. The first stores the public key(s) of each user, whereas the latter stores the secret keys. Get a copy of *both* the pubring and secring for each user. You need both the public and secret key rings to perform your task today.

GnuPG is on the course USB, with an install package for Windows and a pre-installed copy on the SANS Slingshot Linux VMware image for the course.

You win the challenge when you show the instructor the clear-text contents of the pii.csv file and successfully explain to the instructor how you retrieved the encrypted file and the GnuPG keys to decrypt it.

GnuPG Installation

- You can run GnuPG on either Linux or Windows
  - GnuPG is installed on the Linux image provided in the class
  - Or install it on Windows by running the gnupg-w32cli-[version].exe from the Windows directory on the USB:
    - Choose all defaults by pressing Next
- After it is installed, run the gpg binary once with no parameters to automatically create the directory and files GnuPG will use
  - On Windows, invoke c:\Program Files (x86)\GNU\GnuPG\gpg.exe
  - Press CTRL-C when prompted to "Go ahead and type your message"
- You will not have to generate your own keys
  - Instead, you use keys that you grab from 560GC's target machines

You can run GnuPG on either Linux or Windows. On Linux, you can simply invoke it at the command line by typing **gpg**. On Windows, you can install it by running the gnupg-w32cli-[version].exe file from the course USB in the Windows directory. Double-click that .exe, and simply click Next on all the install screens to select defaults.

On Windows, you can invoke the gpg.exe program by changing directories to c:\Program Files (x86)\GNU\GnuPG and then running gpg.exe. After you install GnuPG on Windows, invoke it once so that it creates the appropriate directories for your current user. When it prompts you to "Go ahead and type your message...", just press CTRL-C. You have now prepared GnuPG.

You will not have to generate your own GnuPG keys for this lab. You will use the keys from other users that you retrieve during the session.

Stealing GnuPG Keyrings

- Windows 2008, 2012, Vista, 7, and 8 machines, GnuPG keys are stored in:

```
C:\Users\[UserName]\AppData\Roaming\gnupg\pubring.gpg
C:\Users\[UserName]\AppData\Roaming\gnupg\secring.gpg
```

- On Windows XP and 2003 machines, GnuPG keys are stored in:

```
C:\Documents and Settings\[UserName]\Application Data\gnupg\pubring.gpg
C:\Documents and Settings\[UserName]\Application Data\gnupg\secring.gpg
```

- On Linux targets, they are stored in:

```
/home/[UserName]/.gnupg/pubring.gpg
/home/[UserName]/.gnupg/secring.gpg
```

- On the target machines, grab these files for users John, Sam, Lara, and Kim

To steal GnuPG keys from the target systems during the session, you must compromise the target machines with the appropriate privileges. Then, on Windows targets, you need to grab the pubring.gpg and secring.gpg files from `C:\Documents and Settings\[UserName]\Application Data\gnupg\` or `C:\Users\[UserName]\AppData\Roaming\gnupg`. On a Linux target, the files are stored in `/home/[UserName]/.gnupg`.

REMEMBER TO GET BOTH THE PUBRING AND SECRING FILES! You need both.

You need both keyrings for users John, Sam, Lara, and Kim.

Using Stolen GnuPG Keyrings

- To use a stolen keyring, copy *both* the pubring.gpg and secring.gpg to your gnupg (Windows) or .gnupg (Linux) folder replacing any of the files with these names that are there already
- Note: This overwrites your entire key ring with the provided key ring files, so make sure you back up any files you replace if you have important keys in them

To use stolen GnuPG keyrings, you should copy both the pubring.gpg and secring.gpg files into your gnupg (Windows) or .gnupg (Linux) directories *on your own machine*, replacing any keyrings that are already there. Note that you should create a backup of the keys that are already there if you use them for any production purposes.

By simply copying in the appropriate user's pubring.gpg and secring.gpg files, you will not have to import or export keys. Just move these files into the appropriate location, and then decrypt the pii.csv file for the given user. Remember, you must decrypt the file in the inverse order from which encryption was applied. This is a Last-In, First-Out (LIFO) operation. First, use the keys of the last user who encrypted the file. Then, swap out the keyring files for the second-to-last user, and decrypt the file. Then, swap out the keyring files again, and so on, until you get the original file.

Verifying the Keys

- To verify keys, on the command line type:

```
gpg --list-keys
gpg --list-secret-keys
```

- You should see the key with the correct username listed in the output of both of these commands
- Note: Although the Linux installation includes the gpg executable in your path, the Windows installation does not
  - You need to navigate to the folder containing gpg.exe to run these commands:

```
C:\> cd C:\Program Files (x86)\GNU\GnuPG
```


After you move the keyring files into the appropriate directory *on your own machine*, you can verify that the keys for the given user are present and ready to use by running these commands on either Windows or Linux:

```
gpg --list-keys
gpg --list-secret-keys
```

The first command lists public keys, whereas the second lists secret keys. If you see both the public and secret key for the given user (such as John, Sam, Lara, and Kim), you are ready to go.

Note that the Linux install includes the gpg binary in your default path, so you can invoke gpg by just running gpg. On Windows, it is not in your path, so you must navigate to c:\Program Files (x86)\GNU\GnuPG. Then, you can run gpg.exe because your current working directory (.) is in your path in Windows.

Decrypting a File Using GnuPG

- To decrypt a file, on the command line type:
  `gpg -d -o <OutputFileName> <EncryptedFileName>`
- If the correct key is located in the keyring, GnuPG should automatically find the proper key to decrypt the file
- You need to know the user's passphrase to open the secret key
  - You should figure that out during the session... it won't be too hard
  - Remember: Users manually synchronize their passwords

After the appropriate keyrings are in place on your machine, you can decrypt a file on the command line by running this command:

```
gpg -d -o <OutputFileName> <EncryptedFileName>
```

If the correct key is present on the keyrings, GnuPG will find it. It then prompts you for the user's passphrase so that it can unlock and use the secret key. You must type in the user's GnuPG passphrase. You determine the passphrase for the given user from other aspects of the environment. Remember, users manually synchronize their passwords. With the right keyrings and the proper passphrase for that user, you should decrypt the file.

Winning the Challenge

- You must show the clear-text pii.csv file to the instructor
- Not everyone gets all four sets of keyrings:
  - Some get one
  - Some get two
  - Some get three
  - Some get them all
- Even retrieving one set of keys shows you have mastered really useful pen test techniques
- If we reach 2:00 p.m. and you don't have one yet, let the instructor know, who will provide some guidance

Again, to win the challenge, you must show the instructor the clear-text pii.csv file.

Note that not everyone in the class will get every one of the four sets of keyrings. Some of you will get the keyrings for one user. Others will get two. Some will get three. And, some will get all four.

Even if you get only one set of keyrings, however, you have accomplished something. You have compromised a target machine and made progress in the penetration test. You have one or more findings worthy of including in a report in a real-world penetration test.

If we reach 2:00 p.m. and you still do not have any of the target users' keyrings, let the instructor know. The instructor can provide some guidance so that you get at least one set of keyrings for one target user.

To Win, You Must Track Your Work

- As part of this penetration test, you must record how you got into each system and how you got root or admin privileges on the box
  - No written report necessary, but maintain notes!
  - Consider the spreadsheet format that we discussed in 560.1
    - Included on the course USB in the Target_Inventory.csv file in the Cheat_Sheets directory
- To win the challenge, you must show the pii.csv file to the instructor and explain how you compromised each target

Target IP Addr	Target Name	Target OS	How Discovered	Listening Ports	Known Vulns	Admin Accts / Passwds	Other Accts / Passwds	Misc Notes

To win the challenge, you must track your work. Upon winning, the instructor will ask you how you got into each machine and how you conquered root, admin, or SYSTEM on them. To answer these questions, you need to document your work. After you get access to a box, record the method that you used IN WRITING! When you get superuser privileges on a box, record how you did so. You may want to use the spreadsheet format that we discussed in 560.1, which is available on the course USB in the Cheat_Sheets directory in a file called Target_Inventory.csv.

You need to maintain good notes, but you do not need to write a final report for this lab.

Any Questions?

- If you have any questions, now is the time to ask them
- Ask questions for clarification
- The instructor may not answer all your questions directly because figuring out some of the answers is what this lab is all about
  - When you ask for help, your instructor will provide tips to help you move forward in the challenge

We are almost ready to begin the lab. If there are any questions, now is the time to ask them. You can ask the instructor for clarification on any of the points in the lab.

The instructor will answer questions so that you can engage in the lab and work on the challenge. But, keep in mind that the instructor reserves the right not to answer some questions about how to compromise certain machines or win the challenge because you are supposed to figure out those issues by playing the challenge itself. Thus, some questions may not be answered by the instructor because you are supposed to work out or discover their answers.

Where to Start?

- DNS zone transfer
- Ping sweep
- Port scan
- OS fingerprint
- Vuln scan
- Password guessing
- Exploitation
- Pivoting

If you have no idea of where to start in the lab, consider the process we've discussed throughout this course. This slide offers some ideas, sorted in chronological order, of the steps you may want to apply. We won't go into these steps in detail here because we covered them throughout the rest of the course. But this list should help trigger memories and give you a high-level idea of how to approach this challenge.

After Class ... Where to Go Next

- Many downloadable environments are available for you to practice and develop your skills
  - Metasploitable 2: https://community.rapid7.com/docs/DOC-1875
  - Damn Vulnerable Linux: http://en.sourceforge.jp/projects/sfnet_virtualhacking/downloads/os/dvl/DVL_1.5_Infectious_Disease.iso/
  - Damn Vulnerable Web App: http://www.dvwa.co.uk/
  - Foundstone's Hacme applications (Hacmetravel, hacmebank, hacmeshipping, hacmecasino, and hacmebooks): http://www.mcafee.com/us/downloads/free-tools/index.aspx
  - OWASP's WebGoat: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
  - Irongeek's Mutillidae: http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10
- New ones are released on a regular basis
- Additional lists of target systems and CtF environments are at:
  - http://rootsec.blogspot.com/2011/02/pentest-lab-vulnerable-servers.html
  - http://www.amanhardikar.com/mindmaps/Practice.html

After you finish class, you may want to consider downloading one of the numerous simulation environments listed on this slide. Each of these tools provides free vulnerable systems or applications that you can download, install, and practice your skills against. New projects with similar goals are created on a frequent basis and provide an excellent resource for verifying and further building your skills.

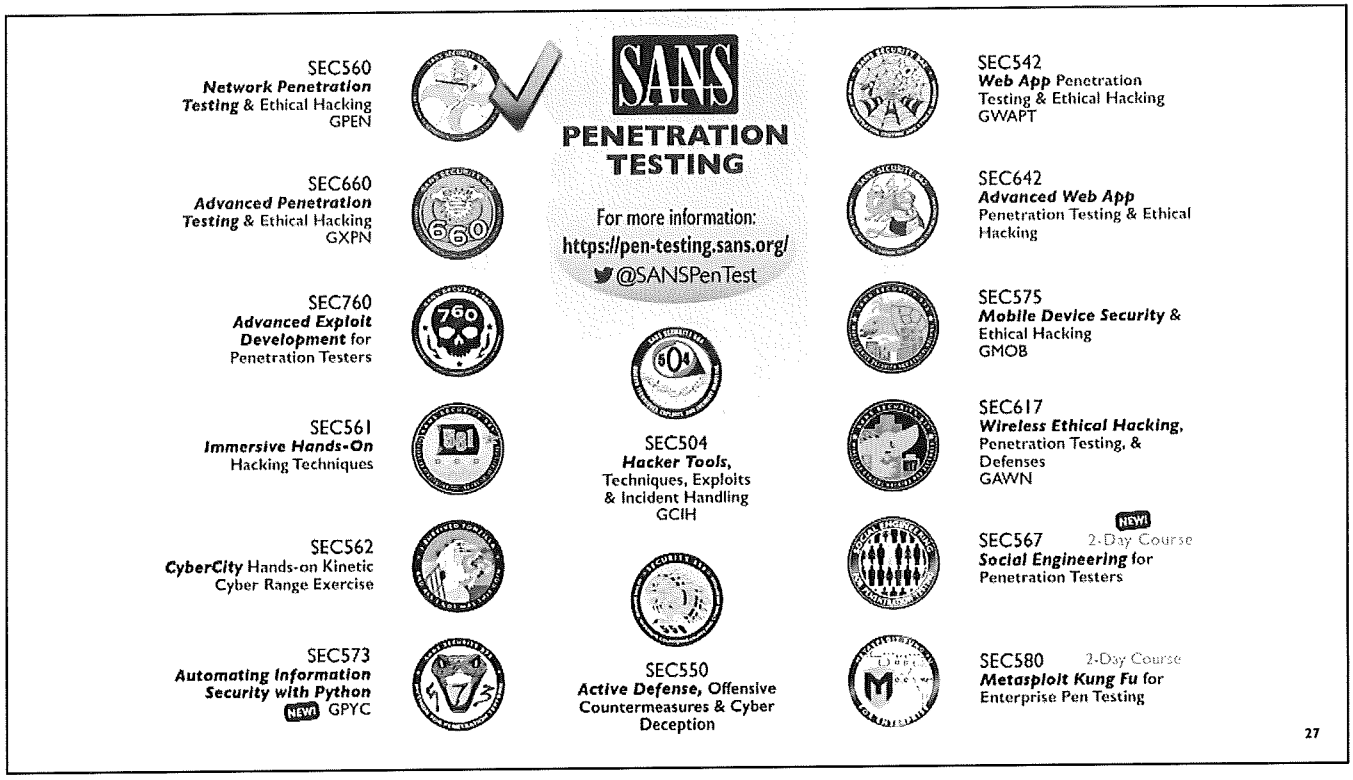
You Now Have Permission to Begin

- You now have permission to begin the attack against target network 10.11.11.2-253 in this room
- Follow the Rules of Engagement
- If and when you win, notify the instructor
- The first winners will receive a fine prize

You now have permission to begin attacking targets in the 10.11.11.2-253 range in this room.

Remember to follow the Rules of Engagement.

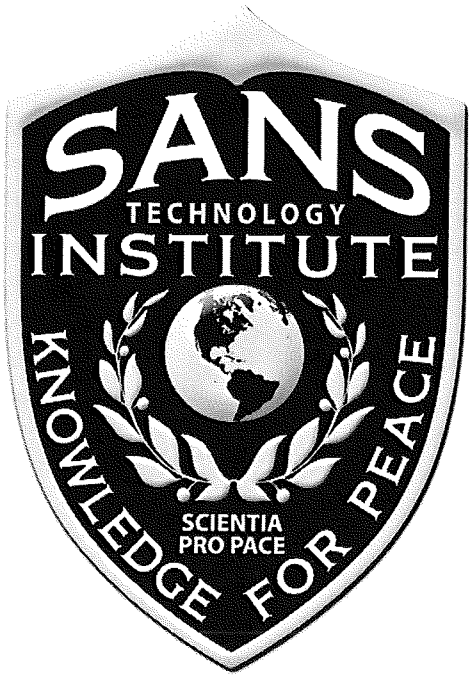
If and when you win the challenge, notify the instructor. The first winners will receive a prize for their efforts.



Now that you've nearly completed the 560 course, you may want to further develop your skills with other in-depth courses in the SANS Penetration Testing Curriculum. Each of these courses was created with a focus on giving you the skills you can apply directly in doing your job as an information security professional. Each of these 6-day courses is available at live conferences, OnSites, across the Internet via SANS vLive, and in the SANS OnDemand system:

- **SANS Security 504: Hacker Techniques, Exploits, and Incident Handling**: This session, one of SANS' most popular courses, focuses on how to respond to computer attacks using a detailed incident response methodology.
- **SANS Security 542: Web App Pen Testing and Ethical Hacking:** If you are interested in focusing on web application penetration testing, this course delivers the skills you need to thoroughly analyze web apps.
- **SANS Security 550: Active Defense, Offensive Countermeasures, and Cyber Deception** provides practical advice on applying an offensive mindset while defending our environment in a safe and effective fashion.
- **SANS Security 561: Intense Hands-On Skill Development for Penetration Testers:** This course is 80%+ hands-on, helping you build serious pen test skills quickly.
- **SANS Security 562: CyberCity Hands-On Kinetic Cyber Range:** This course is also 80%+ hands-on, with missions in the SANS CyberCity kinetic range, which features a miniature city with a real power grid and other components.
- **SANS Security 573: Automating Information Security with Python:** This offering helps security professionals master the Python programming language, and it shows attendees how to build custom tools and tweak existing tools to add more functionality.
- **SANS Security 575: Mobile Device Security and Ethical Hacking:** This course provides the in-depth knowledge that organizations need to design, deploy, operate, and assess their mobile environments, including smartphones and tablets.
- **SANS Security 617: Wireless Ethical Hacking, Pen Testing, and Defenses:** This fantastic course provides in-depth information about attacking and defending wireless LANs, Bluetooth devices, Zigbee, and more.
- **SANS Security 642: Advanced Web App Pen Testing and Ethical Hacking:** This course builds on SANS Security 542, providing advanced, hands-on skills in web application analysis and penetration testing.
- **SANS Security 660: Advanced Penetration Testing, Exploits, and Ethical Hacking:** This exciting and advanced course helps penetration testers take their skills to the next level, and it covers topics such as NAC bypass, route injection, domain compromise, and exploit development to dodge modern OS defenses such as DEP and ASLR.
- **SANS Security 760: Advanced Exploit Development for Penetration Testers:** This is our deepest technical offering, with Windows kernel manipulation, patch diffing, and many other deep attacks and exploits.

In addition, SANS offers two 2-day course related to penetration testing skills in demand today—SANS Security 580, focused on the amazing Metasploit tool, and SANS Security 567, focused on Social Engineering for Pen Testers.



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**

COURSE RESOURCES AND CONTACT INFORMATION

AUTHOR CONTACT
Name: Ed Skoudis
Email: ed@counterhack.com

SANS INSTITUTE
8120 Woodmont Ave., Suite 310
Bethesda, MD 20814
301.654.SANS(7267)

PEN TESTING RESOURCES
pen-testing.sans.org
Twitter: @SANSPenTest

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

This page intentionally left blank.

This page intentionally left blank.

Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."
Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs
sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards

Search SANSInstitute

SANS Free Resources
sans.org/security-resources

- E-Newsletters
  NewsBites: Bi-weekly digest of top news
  OUCH!: Monthly security awareness newsletter
  @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

tute
ont Avenue | Suite 310
20814
(7267)