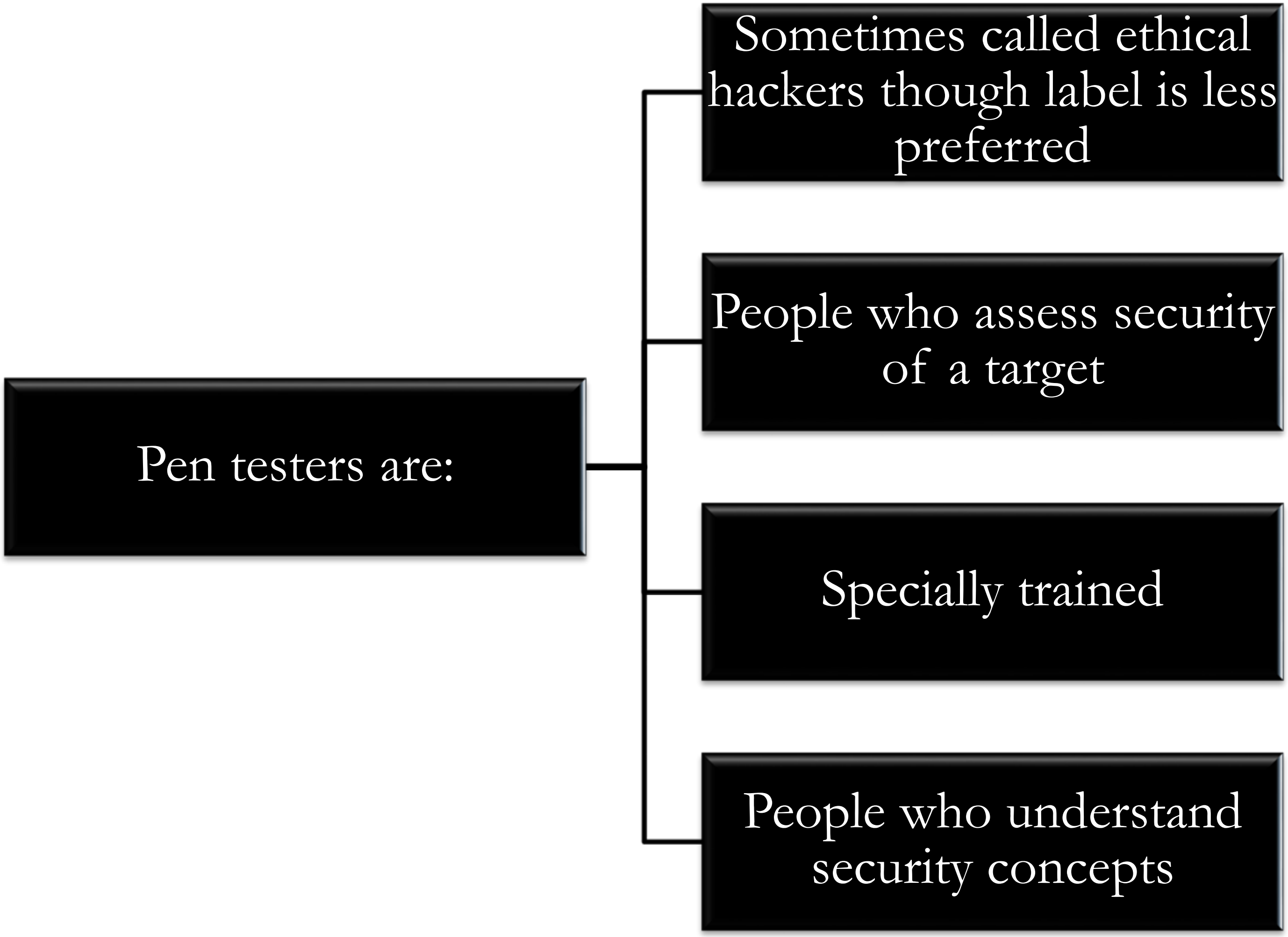
Introduction to Ethical Hacking

Chapter 1

Definition of a Penetration Tester



Pen testers are:

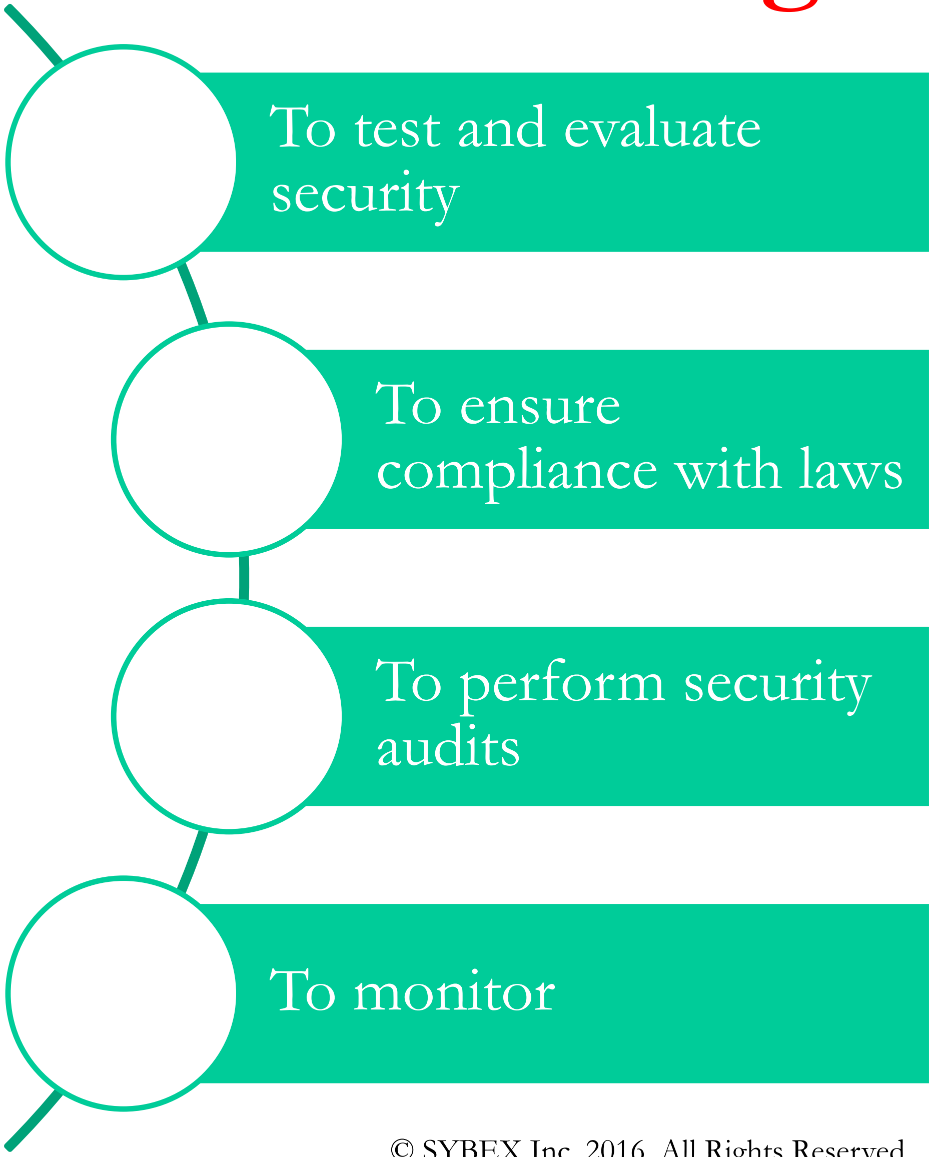
- Sometimes called ethical hackers though label is less preferred
- People who assess security of a target
- Specially trained
- People who understand security concepts

What Is a Penetration Tester?

- Can be employed full-time by a company
- May work freelance as a contractor
- Uses the techniques of malicious hackers against a client
  - Tactics and tools of pen tester are the same as a hacker
  - Intent and permission differ

Why Use Penetration Testing?

Taking on the pen tester role and the associated skillset has become more important in today's world as organizations have had to take a more serious look at their security posture and how to improve it.



- To test and evaluate security
- To ensure compliance with laws
- To perform security audits
- To monitor

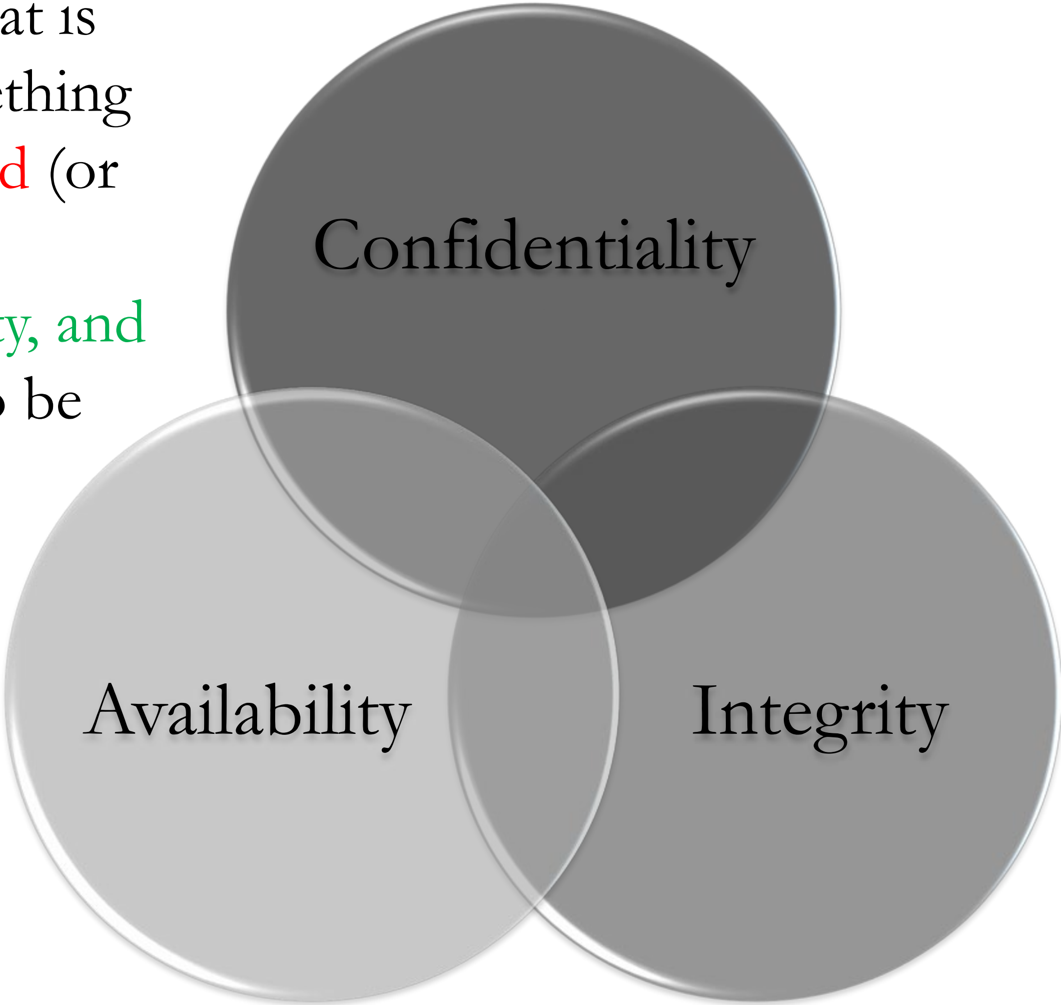
Origins of Penetration Testing

The term *hacker* is an old one that can trace its origin back about 50 years to technology enthusiasts of the 1960s. These individuals were not like the hackers of today; they were simply those who were curious and passionate about new technologies and spent time exploring the inner workings and limitations of early systems.

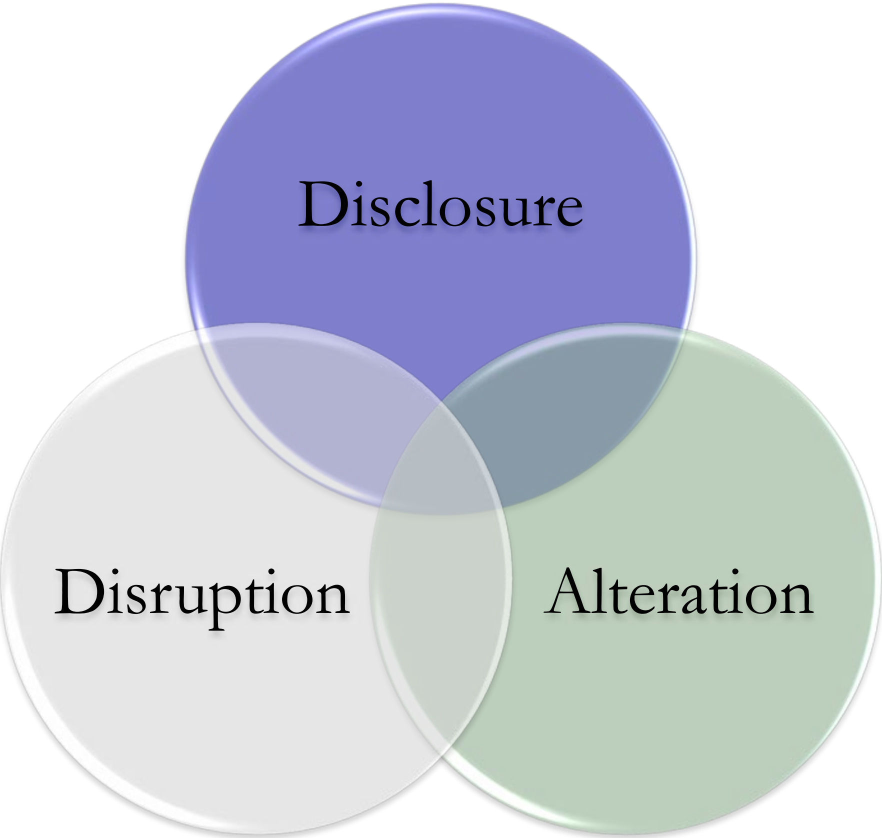
- Evolved from traditional hacking
- Arose from a need to proactively assess an organization's security
- Created in response to hacker activity
- Increasingly popular with rise in cybercrime

Goals of a Penetration Tester

In any organization that is security minded, something known as the CIA triad (or the core principles of confidentiality, integrity, and availability) is trying to be preserved.

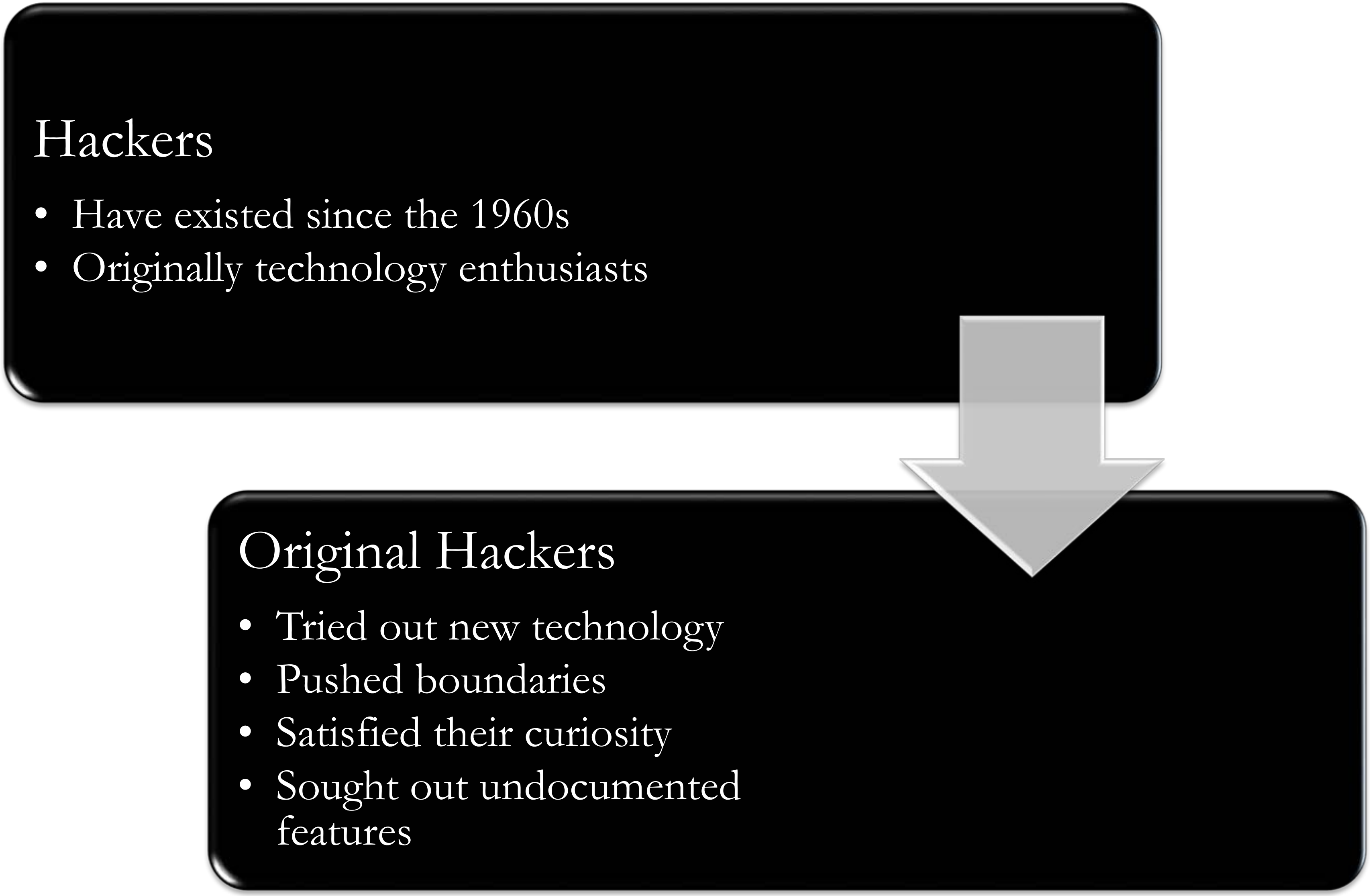


Goals of a Penetration Tester



Testers work to find holes in the client's environment that would disrupt the CIA triad and the way it functions. Another way of looking at this is through the use of something called the *anti-CIA triad*.

Overview of Pen Testing



Hackers

- Have existed since the 1960s
- Originally technology enthusiasts

Original Hackers

- Tried out new technology
- Pushed boundaries
- Satisfied their curiosity
- Sought out undocumented features

Evolution of Internet

Hackers became more prolific and more dangerous not too long after the availability of the Internet to the general public.

Introduction of the Internet expanded possibilities and range

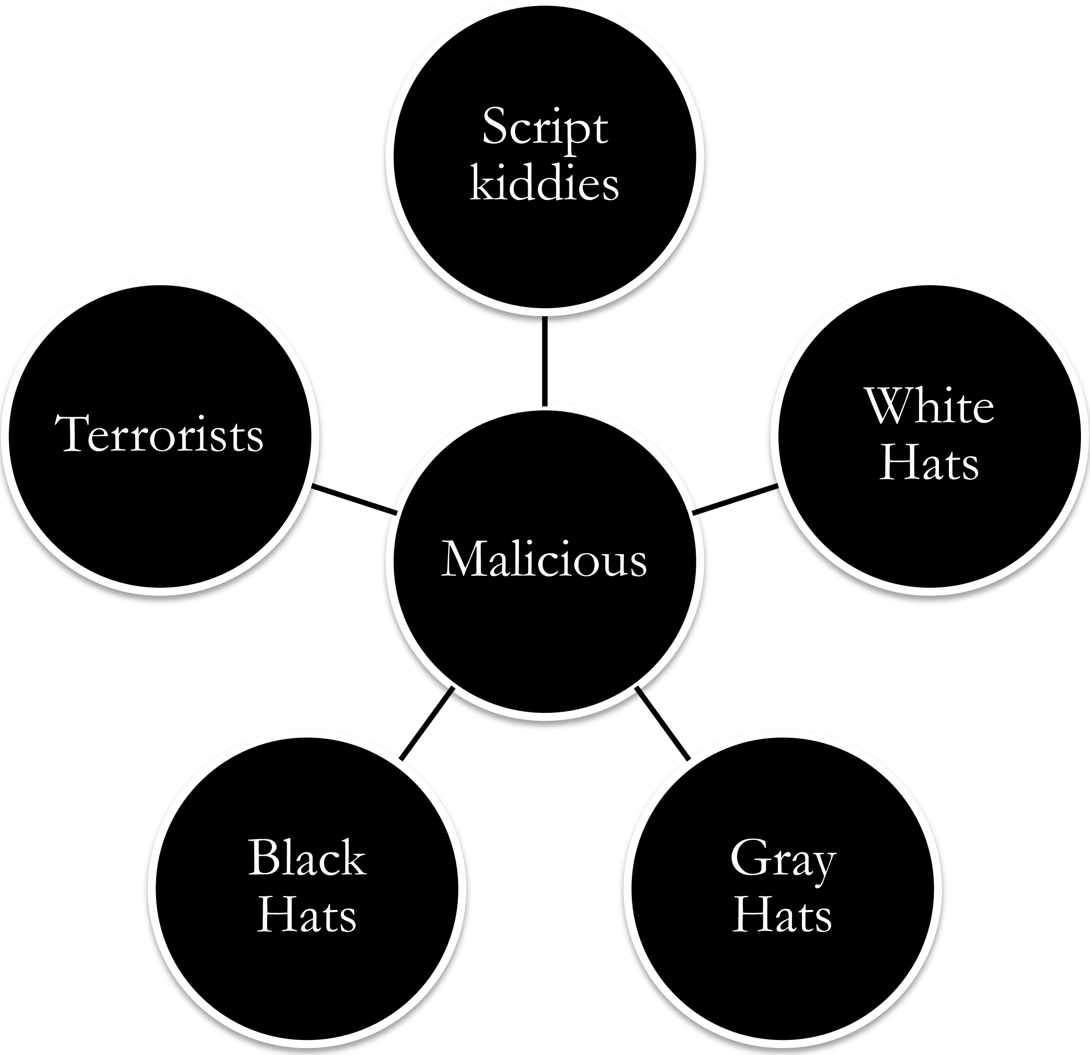
First attacks were mostly mischievous and benign

Later attacks became malicious

Newer attacks include financial fraud, piracy, credit card theft

Opponents

In the “real world,” hackers tend to be broken down into different categories to differentiate their skills and intent. These are the different types of hackers you can expect to encounter in the real world.



Examples of Cybercrimes

Over the past two decades crimes associated with hacking have evolved tremendously. These are some broad categories of cybercrime.

- Identity theft
- Theft of service
- Fraud
- Embezzlement
- Writing malware
- Cyberstalking

Target: Apple iCloud

In August 2014, a massive data breach against Apple's iCloud was responsible for the public disclosure of hundreds of celebrity pictures in various intimate moments. This breach has so far resulted in lawsuits by many of those who had their pictures stolen as well as a lot of negative publicity for Apple.

- **Hackers broke into Apple's cloud-based storage service.**
- **Several celebrities had their photos stolen and posted online.**
- **This breach resulted in numerous ongoing lawsuits.**

Target 2014

In 2014 Target Corp became a victim of a large-scale cybercrime. This breach was responsible for the disclosure of an estimated 56 million different credit card accounts.

The breach resulted in loss of customer data.

56 million records were compromised during the incident.

The breach resulted in major lawsuits.

There was a decrease in business.

JP Morgan 2014

83 million accounts compromised

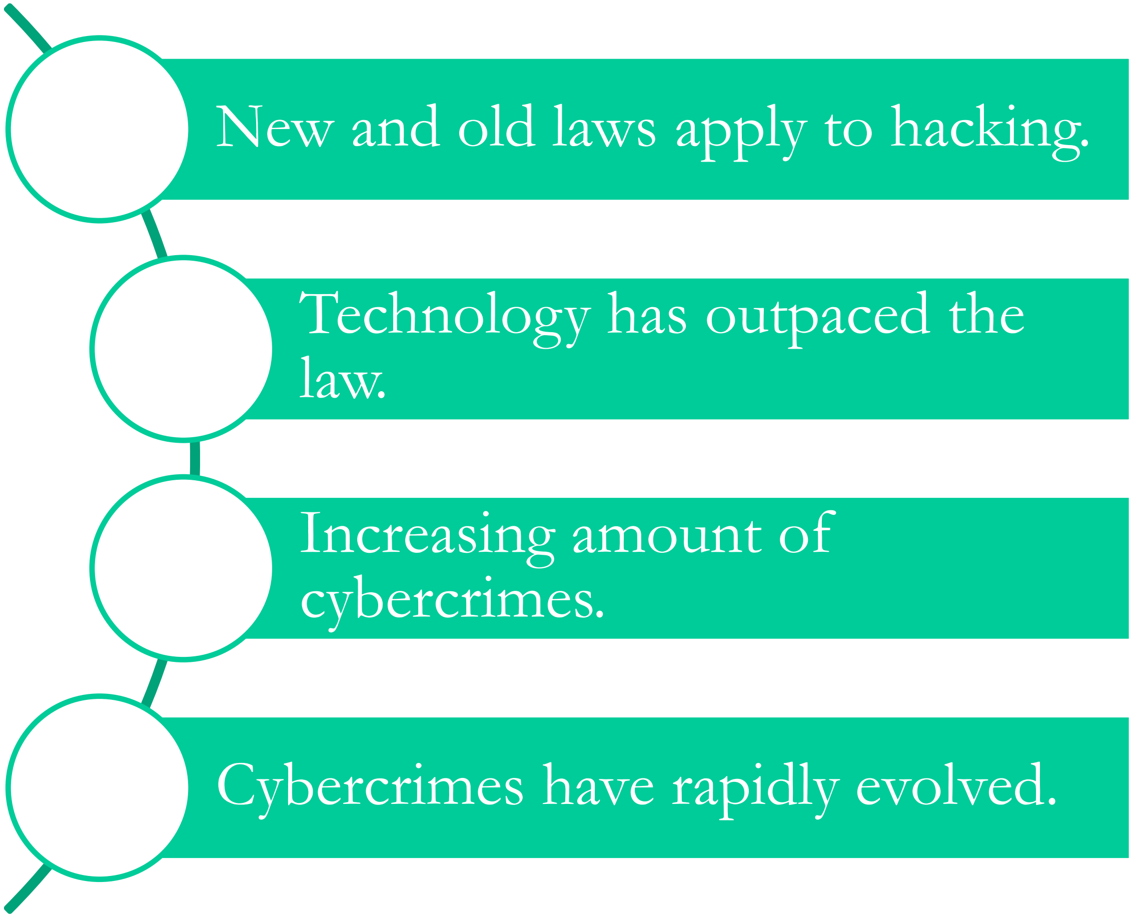
Being actively investigated by SEC in the United States

Generated numerous lawsuits

Loss of customers

In October 2014 JP Morgan revealed to the U.S. Securities and Exchange Commission (SEC) that 83 million accounts were compromised. The breach is being actively investigated by the U.S. Secret Service. Early information points to the breach being the result of attackers discovering vulnerabilities in software on JP Morgan’s own computer systems.

Hacking and the Law



New and old laws apply to hacking.

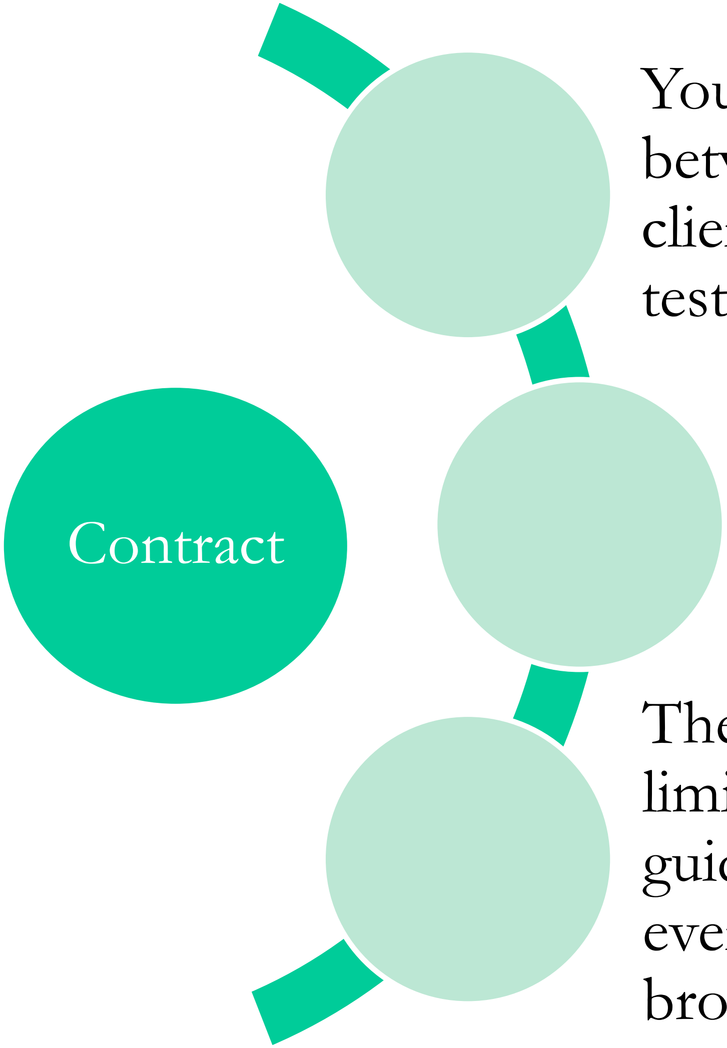
Technology has outpaced the law.

Increasing amount of cybercrimes.

Cybercrimes have rapidly evolved.

Addressing Legal Issues

You will need to always ensure that the utmost care and concern is exercised at all times to ensure that the proper procedures are observed to avoid legal issues.

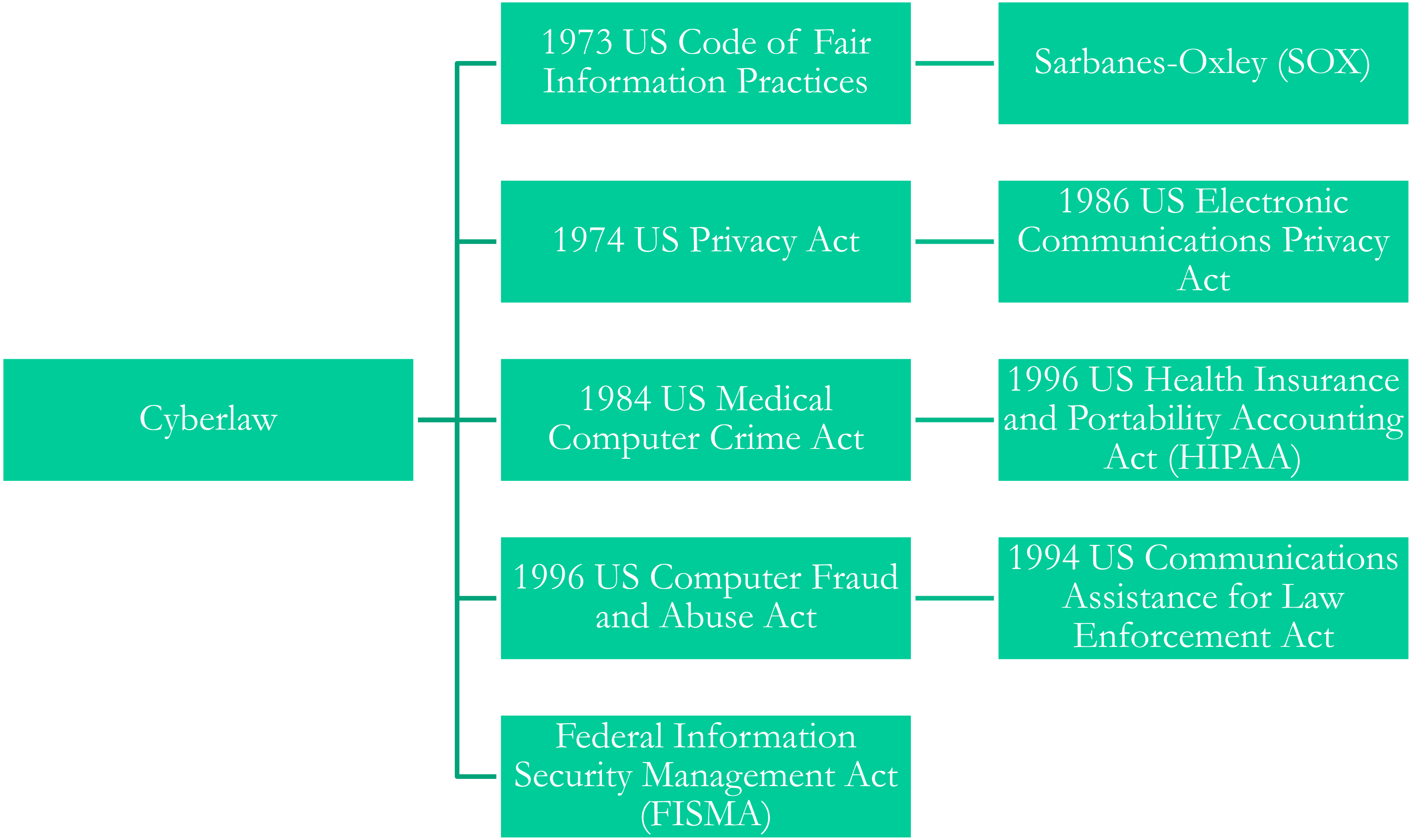


You need trust between the client and pen tester.

The client needs to have confidence rules will be followed.

The client needs limits and guidelines in the event they are broken.

Sample Laws



Cyberlaw

1973 US Code of Fair Information Practices

Sarbanes-Oxley (SOX)

1974 US Privacy Act

1986 US Electronic Communications Privacy Act

1984 US Medical Computer Crime Act

1996 US Health Insurance and Portability Accounting Act (HIPAA)

1996 US Computer Fraud and Abuse Act

1994 US Communications Assistance for Law Enforcement Act

Federal Information Security Management Act (FISMA)

Points to Remember

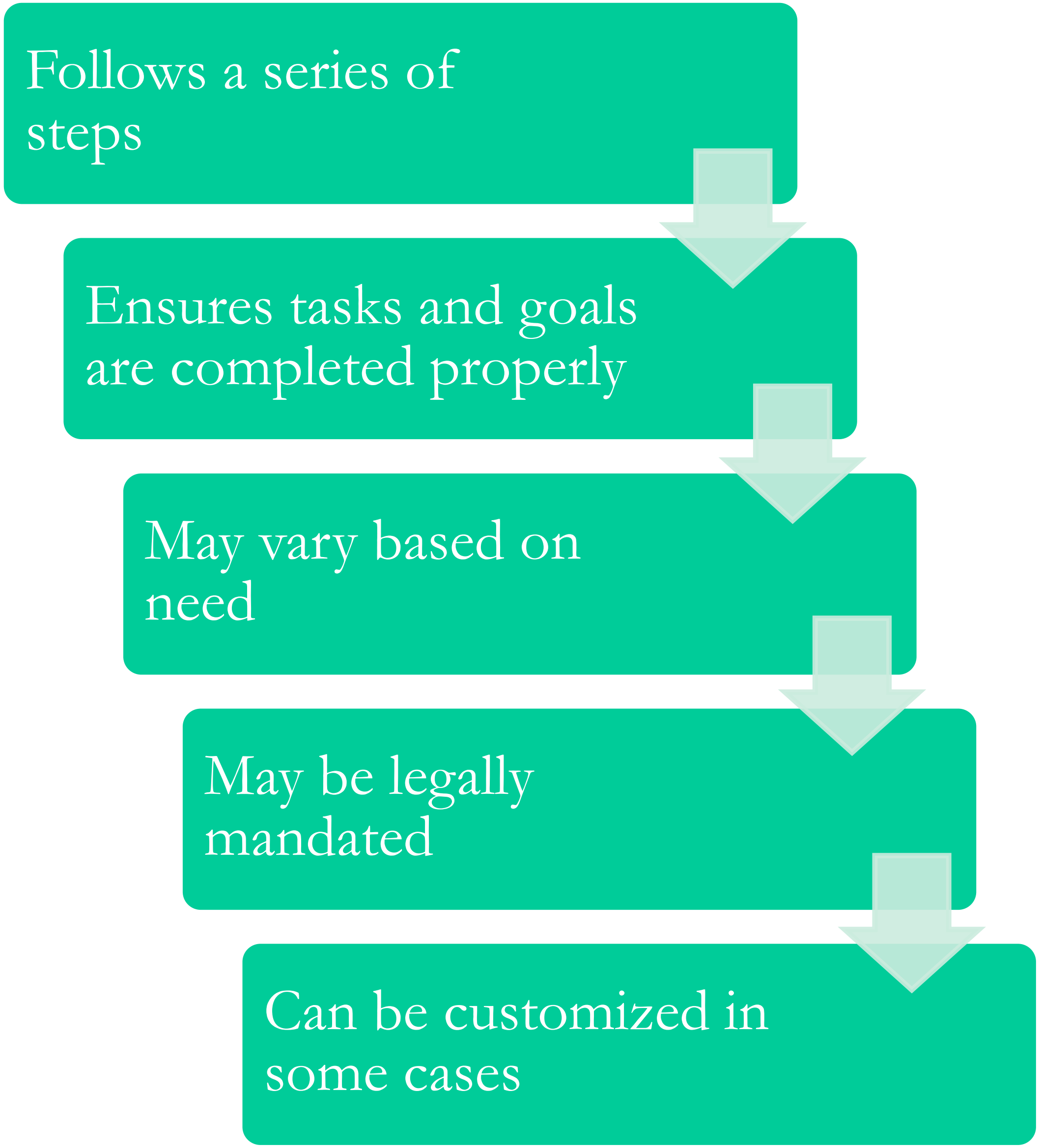
Remember as a pen tester that the law will impact your actions and can result in prison time and/or fines if you do things without permission.

Do not attempt to become an "armchair" lawyer. Rather, understand that the law has an impact on what you do. Seek legal assistance if you don't fully understand the implications.

- **The law will impact and guide many penetration tests.**
- **Seek legal assistance from a lawyer; don't try to interpret the law yourself.**

Pen Testing Process

Once a pen tester is in possession of the necessary permissions to conduct their activities, the actual testing can take place. There are a myriad of ways to proceed with testing at this point, and each is valid in its own way.



Follows a series of steps

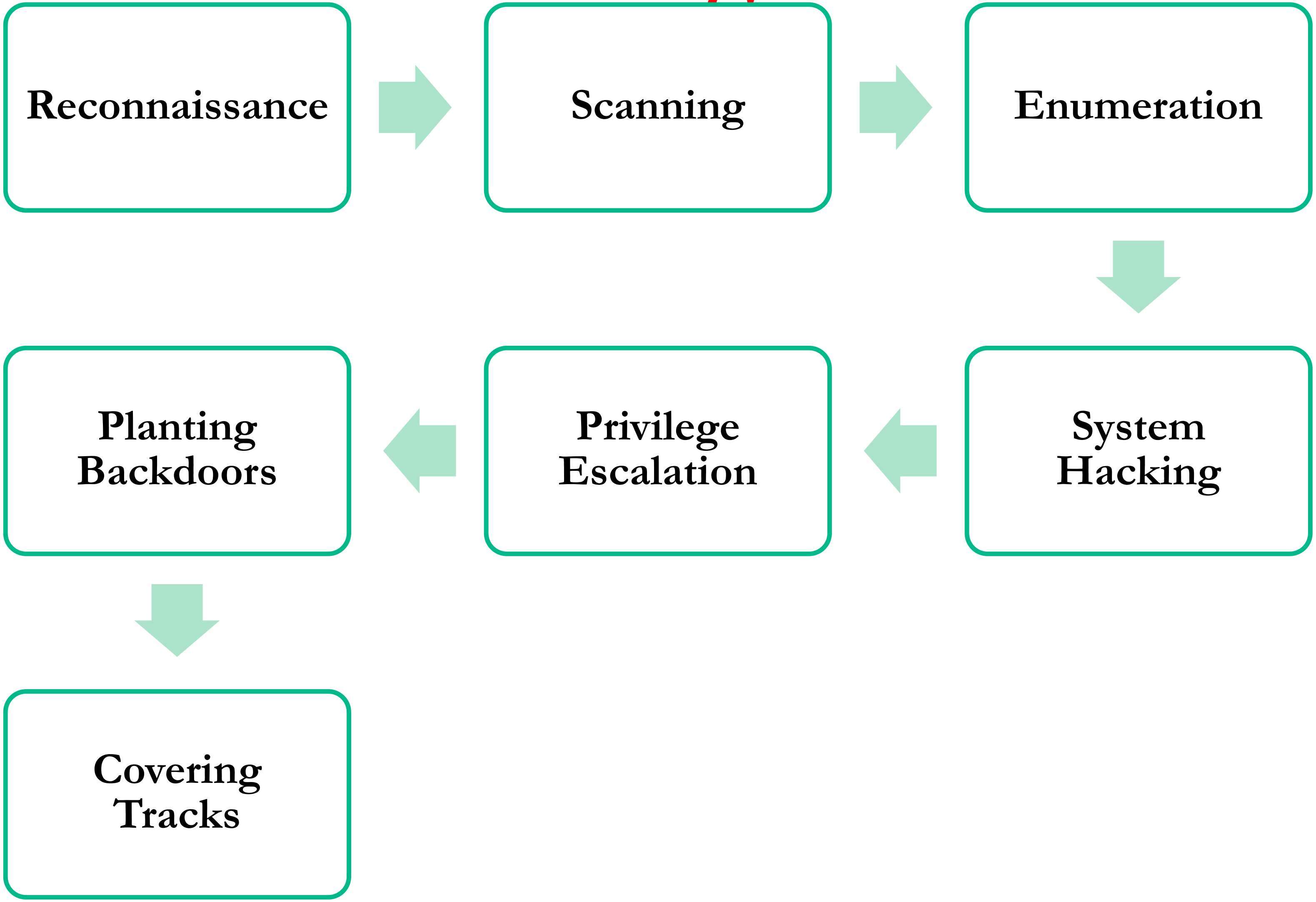
Ensures tasks and goals are completed properly

May vary based on need

May be legally mandated

Can be customized in some cases

Pen Testing Process



Reconnaissance

Scanning

Enumeration

System Hacking

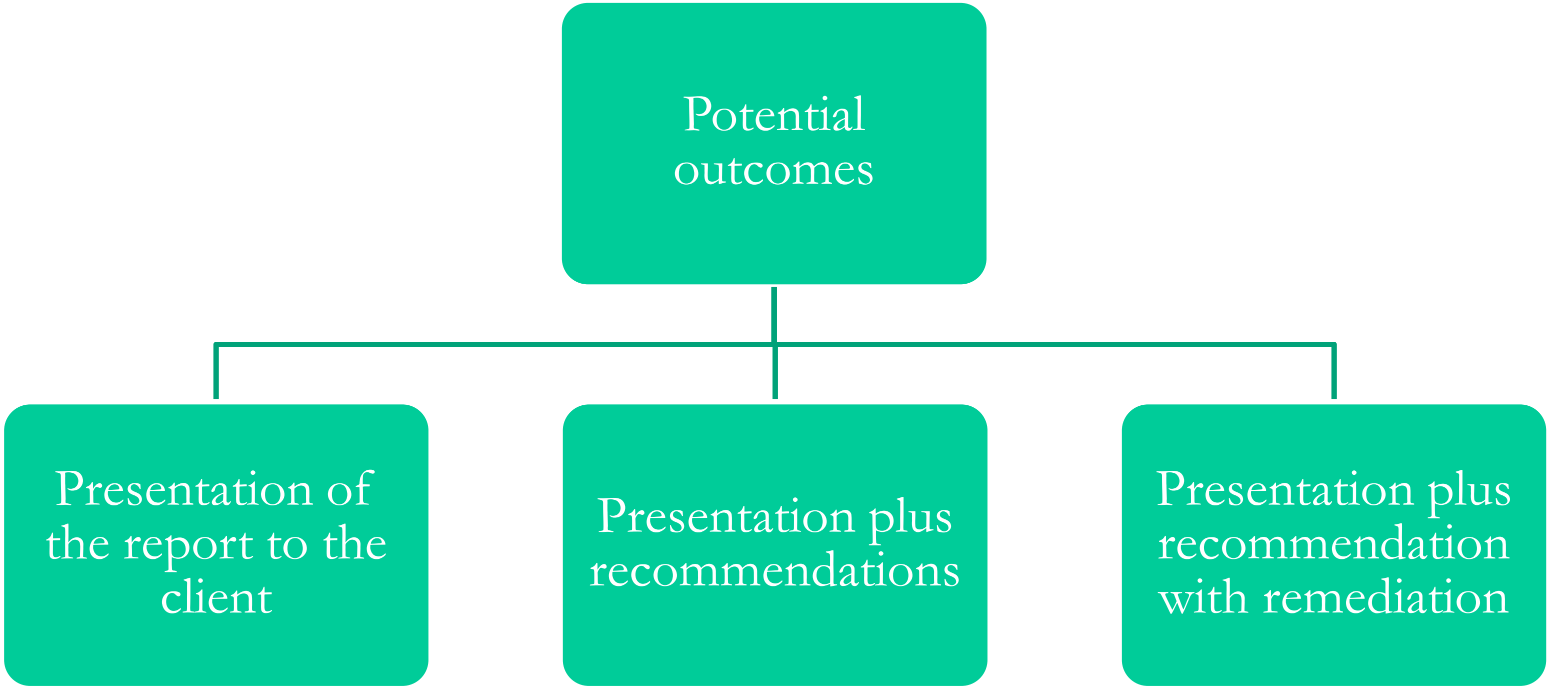
Privilege Escalation

Planting Backdoors

Covering Tracks

Conclusion of the Test

Once this is complete, the tester should be prepared to present a detailed report of their findings. Presenting the report to the client may be the last task the tester has or there may be additional steps.



Potential outcomes

Presentation of the report to the client

Presentation plus recommendations

Presentation plus recommendation with remediation