Penetration Testing

Penetration Testing

Penetration Testing

Remember - security testing is different from other kinds of testing in that you have an actual, thinking adversary.

Oftentimes, the best way to prevent these adversaries from compromising your systems is to have someone else attempt to compromise it first (and report back an assessment).

This is called "penetration testing".

Real-world example:
You are hired to try to gain access to a building to which you don't have permission.

What could you try?

"Users are a vulnerability that can never be patched."
-Georgia Weidman

"People are prone to taking mental shortcuts. They may know that they shouldn't give out certain information, but the fear of not being nice, the fear of appearing ignorant, the fear of a perceived authority figure - all these are triggers, which can be used by a social engineer to convince a person to override established security procedures."
-Kevin Mitnick

The weakest element is often the human element.

Lots of possible technical vulnerabilities, as well, which can be fixed.

Technical vulnerabilities can often be done much more quickly, however, and thus allow more chances of success.

Both technical and social skills are useful for penetration testing.

Penetration ("pen") testing and security research has become much more mainstream in recent years.

Bug bounties (https://www.facebook.com/BugBounty)
pwn2own
zero-day markets
Companies, e.g. Bulb Security, Offensive Security
State actors (e.g. Stuxnet, Equation Group)
Conferences (Black Hat, DefCon)

Times have changed! Security is big business.

Remember - security testing is different from other kinds of testing in that you have an actual, thinking adversary.

Oftentimes, the best way to prevent these adversaries from compromising your systems is to have someone else attempt to compromise it first (and report back an assessment).

This is called "penetration testing".

Real-world example:
You are hired to try to gain access to a building to which you don't have permission.

What could you try?

"Users are a vulnerability that can never be patched."
-Georgia Weidman

"People are prone to taking mental shortcuts. They may know that they shouldn't give out certain information, but the fear of not being nice, the fear of appearing ignorant, the fear of a perceived authority figure - all these are triggers, which can be used by a social engineer to convince a person to override established security procedures."
-Kevin Mitnick

The weakest element is often the human element.

Lots of possible technical vulnerabilities, as well, which can be fixed.

Technical vulnerabilities can often be done much more quickly, however, and thus allow more chances of success.

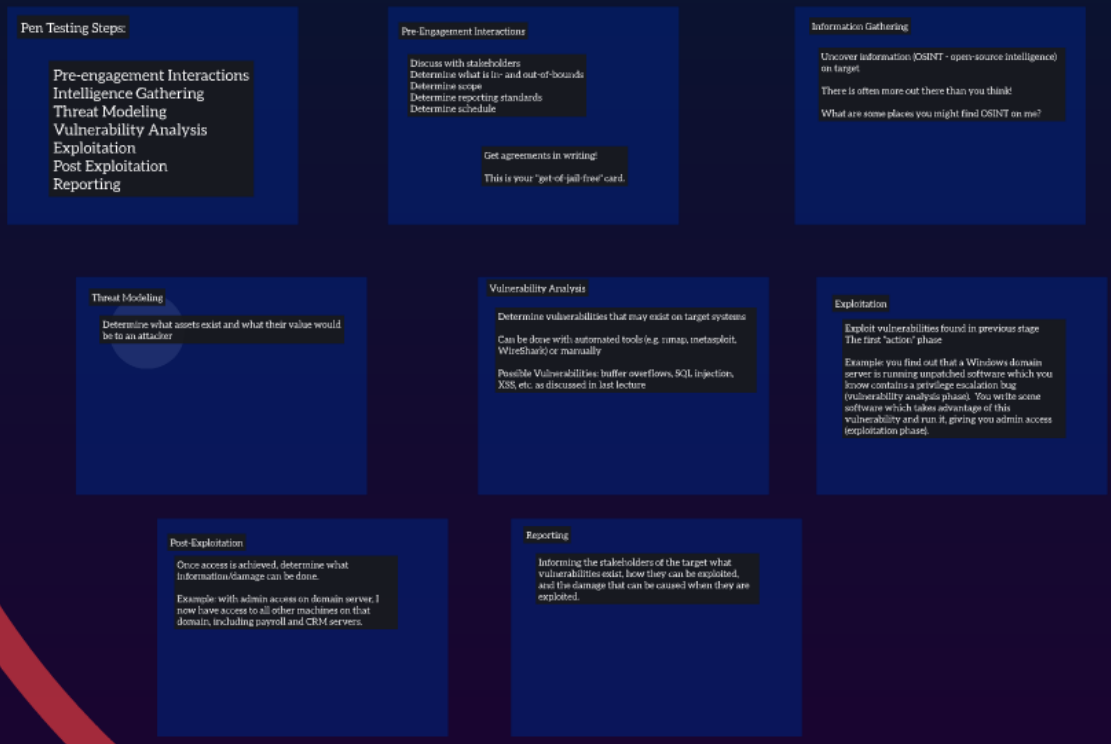
Both technical and social skills are useful for penetration testing.

Penetration ("pen") testing and security research has become much more mainstream in recent years.

Bug bounties (https://www.facebook.com/BugBounty)
pwn2own
zero-day markets
Companies, e.g. Bulb Security, Offensive Security
State actors (e.g. Stuxnet, Equation Group)
Conferences (Black Hat, DefCon)

Times have changed! Security is big business.

The Penetration Testing Framework



Pen Testing Steps:

Pre-engagement Interactions
Intelligence Gathering
Threat Modeling
Vulnerability Analysis
Exploitation
Post Exploitation
Reporting

Pre-Engagement Interactions

Discuss with stakeholders
Determine what is in- and out-of-bounds
Determine scope
Determine reporting standards
Determine schedule

Get agreements in writing!

This is your "get-of-jail-free" card.

Information Gathering

Uncover information (OSINT - open-source intelligence) on target

There is often more out there than you think!

What are some places you might find OSINT on me?

Threat Modeling

Determine what assets exist and what their value would be to an attacker

Vulnerability Analysis

Determine vulnerabilities that may exist on target systems

Can be done with automated tools (e.g. nmap, metasploit, WireShark) or manually

Possible Vulnerabilities: buffer overflows, SQL injection, XSS, etc. as discussed in last lecture

Exploitation

Exploit vulnerabilities found in previous stage
The first "action" phase

Example: you find out that a Windows domain server is running unpatched software which you know contains a privilege escalation bug (vulnerability analysis phase). You write some software which takes advantage of this vulnerability and run it, giving you admin access (exploitation phase).

Post-Exploitation

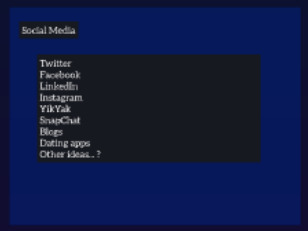
Once access is achieved, determine what information/damage can be done.

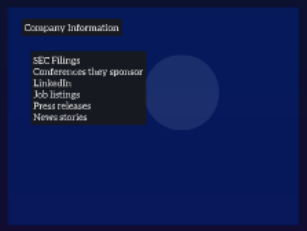
Example: with admin access on domain server, I now have access to all other machines on that domain, including payroll and CRM servers.

Reporting

Informing the stakeholders of the target what vulnerabilities exist, how they can be exploited, and the damage that can be caused when they are exploited.

Information Gathering





Social Media

Twitter
Facebook
LinkedIn
Instagram
YikYak
SnapChat
Blogs
Dating apps
Other ideas... ?

Company Information

SEC Filings
Conferences they sponsor
LinkedIn
Job listings
Press releases
News stories

Knowledge is power.
-Francis Bacon

The more you can learn in this phase, the easier subsequent phases become.

Threat Modeling

Based on information obtained in previous phase, determine goals based on business/ target value.

- Employee records
- Customer records
- Trade secrets
- User accounts
- Policy information
- Financial data

Remember the InfoSec triad!

Are you trying to influence:

- Confidentiality
- Integrity
- Availability

Will differ depending on goal!

We now have goals and a baseline of knowledge of the target system.

Time to find vulnerabilities to exploit.

Based on information obtained in previous phase, determine goals based on business/ target value.

Employee records
Customer records
Trade secrets
User accounts
Policy information
Financial data

Remember the InfoSec triad!

Are you trying to influence:

Confidentiality
Integrity
Availability

Will differ depending on goal!

We now have goals and a baseline of knowledge of the target system.

Time to find vulnerabilities to exploit.

Vulnerability Analysis

Determine what vulnerabilities exist

nmap
- version scan
- port scan

There are entire books written on network scanning with nmap.

Automated vulnerability scanner
- nessus
- ZAP
- metasploit scanner modules

Capture traffic (if possible)
- WireShark

Can use ARP/DNS cache poisoning to avoid raising red flags

Manual analysis (the human brain is powerful!)

"Hmm.. there might be a SQL injection possible here!"
"This database error page indicates that they're running an old version of MySQL!"
"Hey, I found the code for their website on Github!"
"Looks like somebody checked in an AWS key into the repo..."

Determine what vulnerabilities exist

nmap
- version scan
- port scan

There are entire books written on network scanning with nmap.

Automated vulnerability scanner

- nessus
- ZAP
- metasploit scanner modules

Capture traffic (if possible)
WireShark

Can use ARP/DNS cache poisoning to avoid raising red flags

Manual analysis (the human brain is powerful!)

"Hmm.. there might be a SQL injection possible here!"
"This database error page indicates that they're running an old version of MySQL!"
"Hey, I found the code for their website on Github!"
"Looks like somebody checked in an AWS key into the repo..."

Exploitation

Determine ways to exploit vulnerabilities

1. Pre-existing scripts ('script kiddies')
2. Write your own
3. Exploit manually

ACCESS GRANTED

Determine ways to exploit vulnerabilities

1. Pre-existing scripts ("script kiddies")
2. Write your own
3. Exploit manually

ACCESS GRANTED

Post-Exploitation

What's more impressive to a non-technical client?

a. I got root shell on your dev server using a well-known privilege escalation vulnerability.

b. Here are the names and addresses of all your customers last month, along with what they ordered.

Determine what is at risk based on the vulnerabilities you have discovered.

Remember making goals during the threat analysis phase?

Now is the time to see if you can reach those goals post-exploitation.

Other possibilities:
- Keylogging
- Adding additional software/malware
- Capturing user information
- Lateral movement (hop to other networked machines)
- Pivot to other networks (use this as a base of attack)

Remember -
- The goal is not exploitation for exploitation's sake.
- The goal is to determine what business value would be lost if an actual adversary was able to do the things that you have done.

What's more impressive to a non-technical client?

a. I got root shell on your dev server using a well-known privilege escalation vulnerability.

b. Here are the names and addresses of all your customers last month, along with what they ordered.

Determine what is at risk based on the vulnerabilities you have discovered.

Remember making goals during the threat analysis phase?

Now is the time to see if you can reach those goals post-exploitation.

Other possibilities:

- Keylogging
- Adding additional software/malware
- Capturing user information
- Lateral movement (hop to other networked machines)
- Pivot to other networks (use this as a base of attack)

Remember -

The goal is not exploitation for exploitation's sake.

The goal is to determine what business value would be lost if an actual adversary was able to do the things that you have done.

Reporting

Remember to keep copious notes!

When writing up the reports, having more information is always better.

However, you will most likely have to condense down what you wrote. Communication is a vital skill, in software testing and in life.

Keep the audience in mind.

Technical and non-technical stakeholders care about different things(we will talk about this more in the Stakeholders lecture).

Remember to keep copious notes!

When writing up the reports, having more information is always better.

However, you will most likely have to condense down what you wrote. Communication is a vital skill, in software testing and in life.

Keep the audience in mind.

Technical and non-technical stakeholders care about different things (we will talk about this more in the Stakeholders lecture).

Penetration Testing