APP100

Introduction to Penetration Testing and Applied Security

LEARNING OBJECTIVES

At the completion of this lecture, students should be able to:

- LO1: Summarize web and network penetration testing frameworks
- LO2: Describe the methodology behind penetration testing
- LO3: Define exploitation in the context of vulnerability


WELCOME TO APP100!
Expectations
Methodology
Frameworks
Vulnerability Scanning
Tool Utilization
Tool Creation
System and Application Exploitation

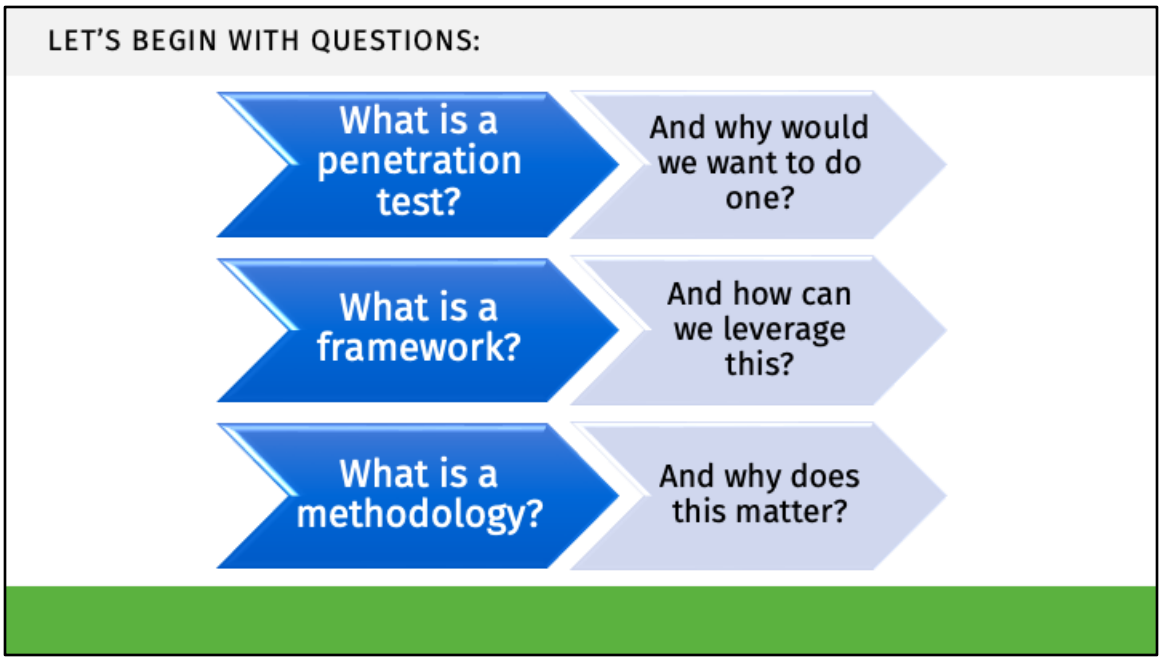
APPROACH

Build off of what we already have learned...

- Python
- Crypto
- Linux and networking foundations

APPLY what we already know

- Take things a few steps further
- Focus on offensive security
- Understand other ways to protect an organization


LET'S BEGIN WITH QUESTIONS:
What is a penetration test?
And why would we want to do one?
What is a framework?
And how can we leverage this?
What is a methodology?
And why does this matter?

PENETRATION TESTING

Penetration testing is the process of manually (and it is a significant manual effort) exploiting vulnerabilities in a controlled manner to identify and quantify business risk

Taking the action of exploiting a vulnerability to identify true risk to the system, users, business, PII, etc.

- We don't know the "true" risk if we just run a scan

Exploitation is the validation of a vulnerability and the measurement of how bad the vulnerability actually is

SO HOW DO WE PERFORM A PENETRATION TEST?

Penetration testing should be done in a controlled, reproducible, and professional manner

Frameworks help keep us on track and be thorough

Let's talk about a couple

Frameworks

METHODOLOGIES AND FRAMEWORKS

This page was last edited on 14 January 2017, at 15:30.

This page was last edited on 16 August 2014, at 20:14.

This page was last edited on 30 April 2012, at 06:04.

Penetration Testing Execution Standard (PTES)

- Complete and dated at the same time – covers lots of ground
- Great reference point and lots of useful information, but we can do better

METHODOLOGIES AND FRAMEWORKS

OSSTM – 213 pages

Long read… it is any good?

Let's keep in mind and recap what a methodology looks like and what a test consists of:

Define	• what are we doing and why?
Scope	• what are we testing?
Rule of Engagement	• testing times, points of contact, what's allowed, etc.
Planning	• how should we approach the test and environment
Execution	• what do we do/how do we engage the target
Reporting	• the one lasting piece of all your hard work

METHODOLOGIES AND FRAMEWORKS

There are more frameworks

Some are more specific to the type of test

For example, the OWASP Web Security Testing Guide (WSTG) - 475 pages

REALITIES

We can't just read documents and be successful

- There is academia and there is practical/hands on; two different things

Exploring the frameworks helps

Looking at the details of a pen test will also help

But first, why would a company want to have a pen test done?

BUSINESS DRIVERS BEHIND PENETRATION TESTING

- New product/service coming online
- Regulatory/mandatory per industry (PCI for example)
  - (This is a primary driver in many cases)
- Clients/Customers asking for due diligence
- Desire to strengthen security posture
- Realize that the security team is a cost center
- We need to make sure we are efficient
  - This will be a recurring theme

Preparation

SCOPING A TEST

Sometimes the scope is dictated

- We need to test this network and that's it

Sometimes the scope is debated

- We think these servers are in scope and these workstations are not in scope

Sometimes the scope is gray

- We need to test this mobile app, but does that include the data recovery site?

Sometimes the scope is for you to define

- Based on our expertise, what should be in scope?

Sometimes the scope needs to be discussed

- We know we need to test the website, but should phishing be included?

SCOPING A TEST COMES DOWN TO A FEW THINGS

What SHOULD be tested based on what it stores, processes, transmits, supports and/or where it resides on the network

What does the auditor SAY has to be tested?

How sensitive is the system and how important is it?

Does the system/app/API/device/etc. have access to PCI data or support the cardholder environment? (for example)

If service “A” is compromised, can its exposure impact service “B”?

Serious questions that take a significant amount of knowledge to be able to confidently answer in some cases

Network diagrams can tremendously help with scoping

RULES OF ENGAGEMENT

The points of contact and permission letter

Testing timeframes (when to start, end, testing time windows)

Source of penetration testing (your IP(s))

Is it Black, White, or Grey box testing?

Will the SOC/security personnel be notified of testing?

Will we be blocked by IPS/WAF or added to the allow list?

What do we do with compromised data?

Will we be onsite? Frequency of briefings...

PLANNING

What do we know about the target organization?

- Scope of assets
- Internal vs external vs mobile vs physical vs web application vs IoT device
- Do we have a copy of the application?
- Do we have an application test account?
- Do we need to go onsite?
- Do we need to send out a device to facilitate testing?
- Per rules of engagement, are we going to send spear phishing emails?
  - SMTP server configured? Allow list configuration? Template/theme(s)?
- Does the company have guards on duty, employees with badges, etc.

EXECUTION

We have permission

We have defined scope and the starting date

We planned out the engagement and are ready to start

Now what?

Reporting

REPORTING

- Reporting is of critical importance
  - The one lasting thing the company keeps, and you must show for your efforts
- Starts with active note taking
- Several ways to tackle this portion of the test
  - Take notes along the way
  - Onenote
  - Mindmapping
  - Dradis
  - Notepad type options – or create the report as you test!

REPORTING

There are several pieces to a great report

- Executive summary
- Scope
- Methodology
- Risk rankings
- Findings
- Evidence
- Recommendations
- Steps to reproduce
- Conclusion

EXECUTIVE SUMMARY

The CISO/CEO/CSO don't have time or desire to read a 50+ page report

Make the executive summary easy to understand

Include pictures/charts/graphs if possible

Get the point across clearly

Make it BRIEF

SCOPE

What did we test?

Include it in the scope section

- IP addresses
- Mobile applications
- Web applications
- Devices, domains, people; everything you tested

When did the test start and end?

- Include this information in the report as well

Who performed the testing?

- Name of personnel/certificates – how do we know they are experts?

SCOPE IS ACTUALLY REALLY IMPORTANT

What is tested and not tested has significant impact

- On audits
- On security
- On cost/time
- On remediation efforts

Segmentation/isolation helps reduce scope

Boundary system/those containing PII are typically in-scope

- What about "supporting systems"?
- Where do you draw the line on what is "in-scope"?

What do you do if there is a disagreement on what is in-scope?

REPORTING - METHODOLOGY

Yes: You actually include your methodology right in the report

Gives the auditor/client a sense of what you did, how you approached the test, your level of thoroughness, etc.

NOT a copy/paste of PTES!

- This is the clearly communicated, concise series of steps that we took during the test

Should be reproducible

Should be based on industry standard

RISK RANKINGS

We need to contextualize the finding

How do we define risk?

- CVSS?
- RAV?
- Some custom tool?

Is there a qualitative output?

- For example, if the CVSS score is 4.3, but we exploited it and got root...

FINDINGS/EVIDENCE

What did we find during the test?

How did we find it?

What evidence do we have to prove what we found?

How did we assign the risk rating to the finding?

Clients *will* let us know if they don't agree with a risk rating

- How can we support our rating? Is it a fair assessment?

This makes up the bulk of the report ~ 85%

RECOMMENDATIONS

We are the experts, so act like it

We found a flaw and exploited the flaw; how can we fix the flaw?

There is where expertise come into play

Sometimes it's straightforward:

> "We exploited CVE XXXX-XXX, the recommendation is to patch the flaw"

Other times it's less so:

> "The compromised Windows XP machine runs the $100MM line of business and we can't update it without breaking it – what do you recommend?"

STEPS TO REPRODUCE

How did we do what we did?

What tool did we use?

How was the tool configured?

What was the command-line syntax we used?

How can they reproduce it themselves to confirm its really a flaw?

Once they fix the issue, they want to be able to test the fix...

Only include details the client/company can use

CONCLUSION

How good/bad was it?

Compare to others in the industry

Did the company pass or fail?

Where should they start on fixing the identified flaws?

Make ourselves available to answer questions and retest

POST TESTING

- Remove shells
- Remove accounts
- Remove listeners
- Delete sensitive information
- Secure and deliver report in encrypted manner

Stay abreast of the latest information to be ready for the next penetration test – things move/change quickly