

Forum:[Hack Forums](#)

Thread: [Getting Started with Penetration Testing: Which Programming Language to Learn and How](#)

haumeaquaoar - August 18, 2024, 10:53 am

I want to learn penetration testing in depth. Which programming language should I start with and how deep should I learn it?

Bastille - August 18, 2024, 11:01 am

You don't use programming for pentesting, you use network and system knowledge.

Start with networking, Windows, Linux, learn how a server works, how IP addresses are structured, what is TCP/IP, and so on.

Read this : <https://hackforums.net/showthread.php?tid=6263412>

Programming in hacking or security is mostly used for :

- programming tools (like hacker tools)
- programming malware
- malware analysis / reverse engineering

EDIT : Just to clarify, I received few disagreements regarding the fact that I've said that you don't use programming for pentesting. When I say programming I speak about low level languages that are used to make programs such as Java, C or ASM, which are not often used by pentesters. Instead, they use a lot scripting languages such as Python, Perl, Bash, PowerShell, and it's also useful to be aware of developing languages such as JavaScript, SQL, PHP, ... if you're interested in web pentesting. That's how I've learned, maybe I'm not using the right terms, not fluent in english.

ttbr0 - August 18, 2024, 11:23 am

(Aug 18, 2024 11:01 AM)Bastille Wrote: [\[CITE\]](#) You don't use programming for pentesting, you use network and system knowledge.

i dont agree with this. lack of programming will severely limit your potential. you will need it to read and modify existing tools or write your own ones to enhance your tool kit or writing payloads to test an attack. learning programming may also help you put into perspective how things may work under the hood and that can give you hints on how you may approach the target. the benefits of programming are far too good to ignore. you can probably scrape by "pentesting" without programming but you will likely be bottom tier.

source - August 18, 2024, 11:56 am

(Aug 18, 2024 11:01 AM)Bastille Wrote: [\[CITE\]](#) You don't use programming for pentesting, you use network and system knowledge.

Start with networking, Windows, Linux, learn how a server works, how IP addresses are structured, what is TCP/IP, and so on.

Read this : <https://hackforums.net/showthread.php?tid=6263412>

Programming in hacking or security is mostly used for :

- programming tools (like hacker tools)
- programming malware

- malware analysis / reverse engineering

I'd like to disagree on this, most successful penetration testers know how to write programs in python, etc, they also need to know how webapps work before even attempting to break into them.

I do agree with the end use needed to learn the basics ie; osi model, mitre threat model, owasp top 10, etc

Learn php, python, javascript, html, sql before just blatantly running automation tools

Bastille - August 18, 2024, 12:20 pm

(Aug 18, 2024 11:23 AM)ttbr0 Wrote: [\[CITE\]](#) i dont agree with this. lack of programming will severely limit your potential. you will need it to read and modify existing tools or write your own ones to enhance your tool kit or writing payloads to test an attack. learning programming may also help you put into perspective how things may work under the hood and that can give you hints on how you may approach the target. the benefits of programming are far too good to ignore. you can probably scrape by "pentesting" without programming but you will likely be bottom tier.

Based on the definition provided by ChatGPT :

Pentesting, short for penetration testing, is a simulated cyberattack on a computer system, network, or web application to evaluate its security.

During pentetration testing exercises you use existing tools, but you don't modify or create them, or at least in a profesionnal environment it's done by dedicated teams that develop internal tools.

From what I've learnt, the term programming includes low level languages such as C, Java, Assembly which include memory management and stuff. In case pentesters have to create tools they'll usually go with scripting languages such as PowerShell, Bash, or other versatile languages such as Python, Ruby, Perl.

I don't think that learning programming such as C is useful for pentesting, however, as I mentioned it can be useful for malware analysis, malware development, or to create programs used during pentesting like Cobalt Strike (Java), Nessus (C and C++), Burp (Java).

(Aug 18, 2024 11:56 AM)source Wrote: [\[CITE\]](#) I'd like to disagree on this, most successful penetration testers know how to write programs in python, etc, they also need to know how webapps work before even attempting to break into them.

I do agree with the end use needed to learn the basics ie; osi model, mitre threat model, owasp top 10, etc

Learn php, python, javascript, html, sql before just blatantly running automation tools

Maybe I'm using the wrong term but for me programming includes low level languages which are, not limited to this but, capable of memory management such as Java, C, ASM. Instead, I would of course recommend, what I call, scripting with Python, Perl, JavaScript, PowerShell, Bash, etc ...

source - August 18, 2024, 12:33 pm

(Aug 18, 2024 12:20 PM)Bastille Wrote: [\[CITE\]](#) Based on the definition provided by ChatGPT :

Pentesting, short for penetration testing, is a simulated cyberattack on a computer system, network, or web application to evaluate its security.

During pentetration testing exercises you use existing tools, but you don't modify or create them, or at least in a profesionnal environment it's done by dedicated teams that develop internal tools.

From what I've learnt, the term programming includes low level languages such as C, Java, Assembly which include memory management and stuff. In case pentesters have to create tools they'll usually go with scripting languages such as PowerShell, Bash, or other versatile languages

such as Python, Ruby, Perl.

I don't think that learning programming such as C is useful for pentesting, however, as I mentioned it can be useful for malware analysis, malware development, or to create programs used during pentesting like Cobalt Strike (Java), Nessus (C and C++), Burp (Java).

Maybe I'm using the wrong term but for me programming includes low level languages which are, not limited to this but, capable of memory management such as Java, C, ASM. Instead, I would of course recommend, what I call, scripting with Python, Perl, JavaScript, PowerShell, Bash, etc ...

I was curious on your use case of the word programming, i questioned myself as well after posting, thanks for clearing up.

BlackSoulZN5006 - August 18, 2024, 4:14 pm

The offensive C#, .NET, and Offensive C++ and Rust.

PlasticWifi - August 18, 2024, 4:46 pm

I need you to pay attention.

Learn and understand Python first. This will be your main weapon.

I would then say javascript but by this point you'd have figured it out yourself.

Bash/Shell Scripting if ur on linux

Learn and understand CMD / Powershell on windows.

if you want to tinker with existing programs like kali.. learn bash and how to operate on linux

If you like Metasploit.. learn the programming language Ruby.

understand .NET assembly*

This will take years, this isn't a joke. It's a serious skill. Goodluck

ttbr0 - August 18, 2024, 9:36 pm

(Aug 18, 2024 12:20 PM)Bastille Wrote: [\[CITE\]](#) Based on the definition provided by ChatGPT :

Pentesting, short for penetration testing, is a simulated cyberattack on a computer system, network, or web application to evaluate its security.

During pentetration testing exercises you use existing tools, but you don't modify or create them, or at least in a profesional environment it's done by dedicated teams that develop internal tools.

From what I've learnt, the term programming includes low level languages such as C, Java, Assembly which include memory management and stuff. In case pentesters have to create tools they'll usually go with scripting languages such as PowerShell, Bash, or other versatile languages such as Python, Ruby, Perl.

I don't think that learning programming such as C is useful for pentesting, however, as I mentioned it can be useful for malware analysis, malware development, or to create programs used during pentesting like Cobalt Strike (Java), Nessus (C and C++), Burp (Java).

Maybe I'm using the wrong term but for me programming includes low level languages which are, not limited to this but, capable of memory management such as Java, C, ASM. Instead, I would of

course recommend, what I call, scripting with Python, Perl, JavaScript, PowerShell, Bash, etc ... programming is general development of programs while scripting is a subset of that. the official python, perl and ruby websites say they are a programming languages and most people will agree that bash and powershell are the same. i dont think it makes any sense to categorize languages with "memory management and stuff" ability - i assume you mean manual management here. i could counter argue saying that java doesnt really have memory management unlike scripting languages since they all have an automatic gc under the hood. but that is beyond the scope of the thread.

i would highly recommend golang over python.

SovietBastard - August 19, 2024, 7:23 am

(Aug 18, 2024 11:01 AM)Bastille Wrote: [\[CITE\]](#) You don't use programming for pentesting, you use network and system knowledge.

Start with networking, Windows, Linux, learn how a server works, how IP addresses are structured, what is TCIP/IP, and so on.

Read this : <https://hackforums.net/showthread.php?tid=6263412>

Programming in hacking or security is mostly used for :

- programming tools (like hacker tools)
- programming malware
- malware analysis / reverse engineering

im sorry man, but i need to disagree on this one...

(Aug 18, 2024 09:36 PM)ttbr0 Wrote: [\[CITE\]](#) programming is general development of programs while scripting is a subset of that. the official python, perl and ruby websites say they are a programming languages and most people will agree that bash and powershell are the same. i dont think it makes any sense to categorize languages with "memory management and stuff" ability - i assume you mean manual management here. i could counter argue saying that java doesnt really have memory management unlike scripting languages since they all have an automatic gc under the hood. but that is beyond the scope of the thread.

i would highly recommend golang over python.why is that you prefer golang?

(Aug 18, 2024 04:14 PM)BlackSoulZN5006 Wrote: [\[CITE\]](#) The offensive C#, .NET, and Offensive C++ and Rust.

kind of true, c++ will just substitute the first 2 and last one

Bastille - August 19, 2024, 8:21 am

(Aug 18, 2024 09:36 PM)ttbr0 Wrote: [\[CITE\]](#) programming is general development of programs while scripting is a subset of that. the official python, perl and ruby websites say they are a programming languages and most people will agree that bash and powershell are the same. i dont think it makes any sense to categorize languages with "memory management and stuff" ability - i assume you mean manual management here. i could counter argue saying that java doesnt really have memory management unlike scripting languages since they all have an automatic gc under the hood. but that is beyond the scope of the thread.

i would highly recommend golang over python.

Yeah when I said "memory management" I meant languages you have to manually manage the addressing, or I should have say languages that are closer to the hardware maybe ?

(Aug 19, 2024 07:23 AM)SovietBastard Wrote: [\[CITE\]](#) im sorry man, but i need to disagree on this

one...

I edited my post as few people had the same feedback :

EDIT : Just to clarify, I received few disagreements regarding the fact that I've said that you don't use programming for pentesting. When I say programming I speak about low level languages that are used to make programs such as Java, C or ASM, which are not often used by pentesters. Instead, they use a lot scripting languages such as Python, Perl, Bash, PowerShell, and it's also useful to be aware of developing languages such as JavaScript, SQL, PHP, ... if you're interested in web pentesting. That's how I've learned, maybe I'm not using the right terms, not fluent in english.

SovietBastard - August 19, 2024, 8:24 am

(Aug 19, 2024 08:21 AM)Bastille Wrote: [\[CITE\]](#) Yeah when I said "memory management" I meant languages you have to manually manage the addressing, or I should have say languages that are closer to the hardware maybe ?

I edited my post as few people had the same feedback :

EDIT : Just to clarify, I received few disagreements regarding the fact that I've said that you don't use programming for pentesting. When I say programming I speak about low level languages that are used to make programs such as Java, C or ASM, which are not often used by pentesters. Instead, they use a lot scripting languages such as Python, Perl, Bash, PowerShell, and it's also useful to be aware of developing languages such as JavaScript, SQL, PHP, ... if you're interested in web pentesting. That's how I've learned, maybe I'm not using the right terms, not fluent in english.
you received few disagreements bcz what u said is kind of wrong i guess :), but i do also understand your point, correct me if im wrong, but do you code at all?

haumeaquaoar - August 19, 2024, 12:30 pm

I decided to learn either Go or C++ after doing some research. Which one do you think I can learn more easily and quickly?

BlackSoulZN5006 - August 19, 2024, 2:03 pm

Both GO and C++ can be learned faster I say C++ can be learned faster and its much more traditional language and has offensive capabilities as well. All you need is an IDE like Code::Blocks.

brenleehelm - August 19, 2024, 8:01 pm

I found that some unnecessary data was sent back to the server when the software was working. Have you noticed?

hierNULLphant - August 23, 2024, 3:48 pm

Learn enough of a language to be able to read it and generally tell what it can do. Maybe learn python for automation reasons. Also it depends on what you're attacking, JS will probably prove useful if you're into web hacking, low level languages are always good to know too.