WHY WINDOWS INTERNALS?

TO BETTER UNDERSTAND THE INTERNALS OF WINDOWS OPERATING SYSTEM

TO CREATE BETTER RED TEAM TOOLS AND EVASION TECHNIQUES

TO ENHANCE THE MALWARE ANALYSIS SKILLS

BETTER JOB OPPORTUNITIES

Job Descriptions !!

Security Researcher - Malware Analysis
Zscaler · Bengaluru, Karnataka, India

Apply ⬀   **Save**   ...

Qualifications
- 2 to 4 years of experience in security research
- Reverse engineering skills
- Experience with Malware analysis - Dynamic & Static, Tools like – IDA Pro, Ollydbg, Wireshark etc.
- Experience writing IDS/IPS, YARA signatures
- Understanding of windows internals and API calls.
- Strong understanding of web protocols

Senior Security Researcher
Sony India Software Centre · Bengaluru, Karnataka, Ind...

Apply ⬀   **Save**   ...

if we are happy with the performance.

Profile

The candidate needs to have the following profile / experience:
- Experience with reverse engineering tools and techniques,
  - Debuggers, decompilers, disassemblers, deobfuscators
  - Static and dynamic binary analysis, binary injection
  - Packet sniffers
- Solid knowledge and experience in ARM architecture exploitation
- Solid exploitation skills
- Experience in identifying vulnerabilities by source code analysis
- Good understanding of OS internals, security features and ways to bypassing them
- Good C/assembly development skills
- Good writing skills
- Fluent English

Threat Research Security Researcher
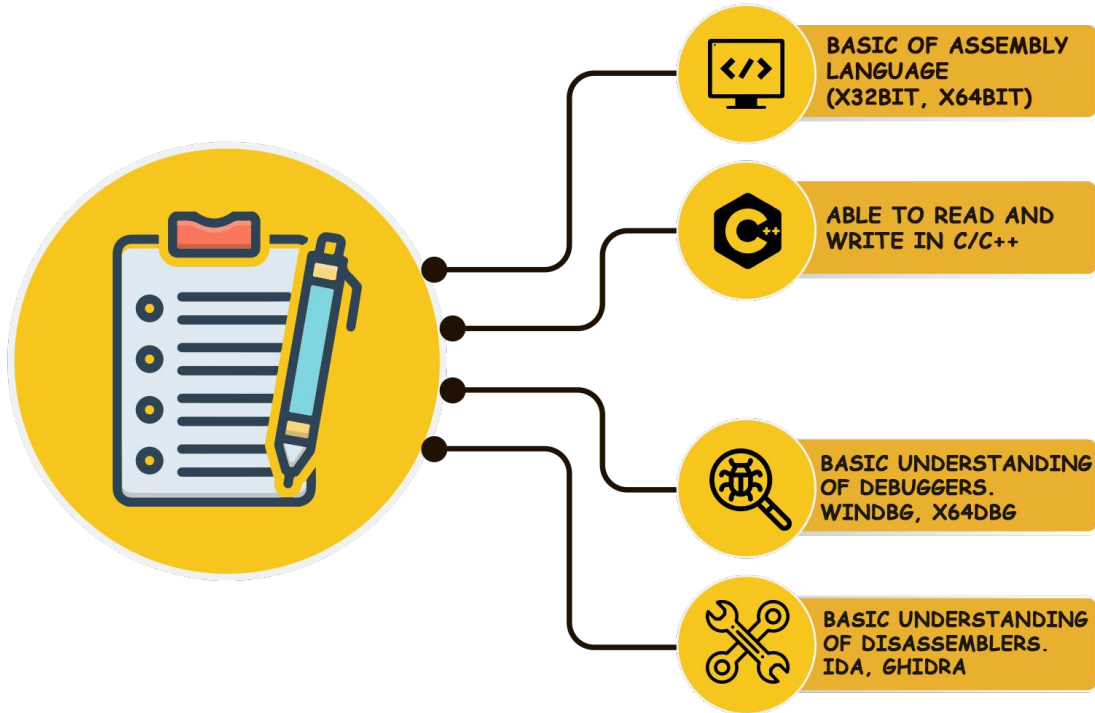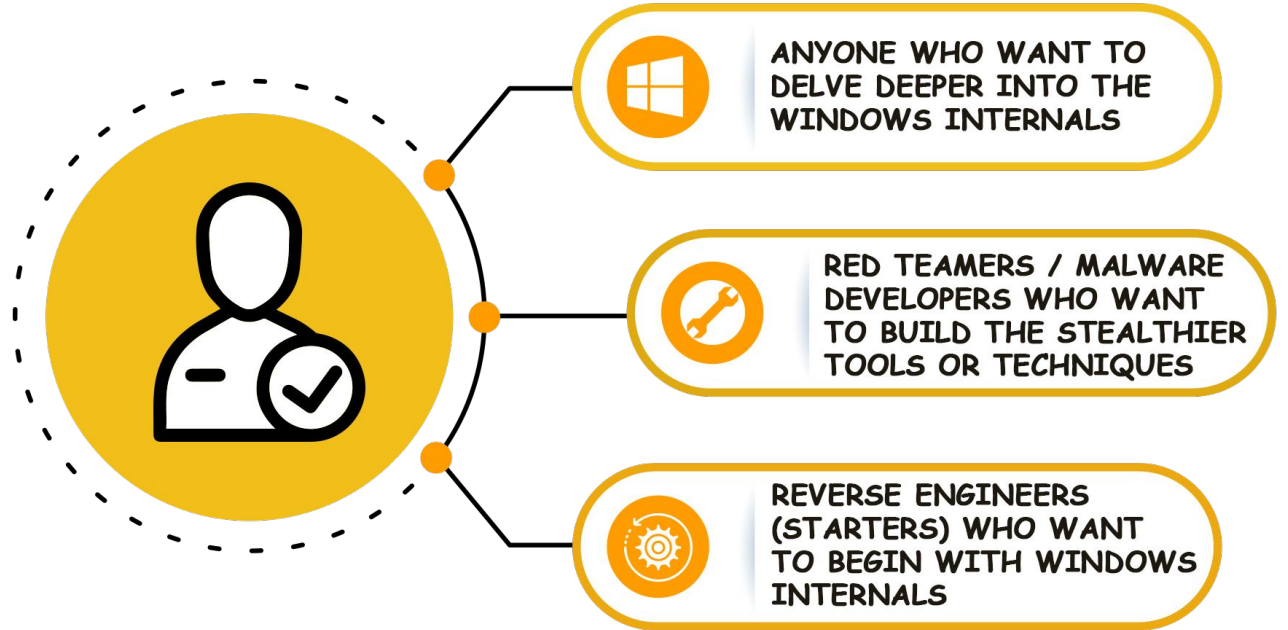Trellix · Bengaluru, Karnataka, India (On-site)

Apply ⬀   **Save**   ...

- Ideally you must have experience in a Security or Malware Researcher role.
- You should have experience in Python, C/C++, or other similar programming languages.
- You should understand PE file format.
- You should have knowledge of Windows OS internals - memory, threads, processes, API, etc.
- You should have proficiency in debugger usage (OllyDbg, IDA pro).
- You should have knowledge of Networking protocols and experience with network traffic analysis tools (Wireshark, Fiddler).
- You should have experience in reverse engineering.
- You should have experience of various malware analysis tools.
- You should have excellent problem-solving skills, fast learner, self-motivated to take initiatives with focus on achieving results in timely manner.
- You should have proven ability to translate insights into business recommendations.
- Degree Level Computing Qualification or equivalent with 3+ years demonstrated experience.
- Ability to positively adapt to changes and multitasking in a fast-moving industry.

PREREQUISITE

BASIC OF ASSEMBLY LANGUAGE (X32BIT, X64BIT)

ABLE TO READ AND WRITE IN C/C++

BASIC UNDERSTANDING OF DEBUGGERS. WINDBG, X64DBG

BASIC UNDERSTANDING OF DISASSEMBLERS. IDA, GHIDRA

WHO ARE THE CANDIDATES

ANYONE WHO WANT TO DELVE DEEPER INTO THE WINDOWS INTERNALS

RED TEAMERS / MALWARE DEVELOPERS WHO WANT TO BUILD THE STEALTHIER TOOLS OR TECHNIQUES

REVERSE ENGINEERS (STARTERS) WHO WANT TO BEGIN WITH WINDOWS INTERNALS

What Not To expect

USER/KERNEL EXPLOIT DEVELOPMENT

DRIVER/ROOTKIT DEVELOPMENT

WINDOWS MEMORY MANAGEMENT

Windows Internals For Red Team
[Beginner Edition]

CYBER SECURITY ESSENTIALS

Introduction to Windows Internals
Start Debugging in Kernel Land
Explore the codes in Kernel Land
Learn Various Kernel Data Structures

Stealth Malware Development Skills

Premium Study Material

Get Custom VM for debugging & internals

Get your hands dirty with latest attack techniques

Is 20 hours enough?

The first 20 hours -- how to learn anything | Josh Kaufman | TEDxCSU
33M views • 9 years ago

TEDx Talks

Josh Kaufman is the author of the #1 international bestseller, 'The Personal MBA: Master the Art of Business', as well as the ...

Subtitles

Introduction | The 10000 hour rule | The learning curve | Research | Method | Deconstruct |...   12 chapters

19:27

Is 20 hours enough?

The first 20 hours -- how to learn anything | Josh Kaufman | TEDxCSU

33M views • 9 years ago

TEDx Talks

Josh Kaufman is the author of the #1 international bestseller, 'The Personal MBA: Master the Art of Business', as well as the ...

Subtitles

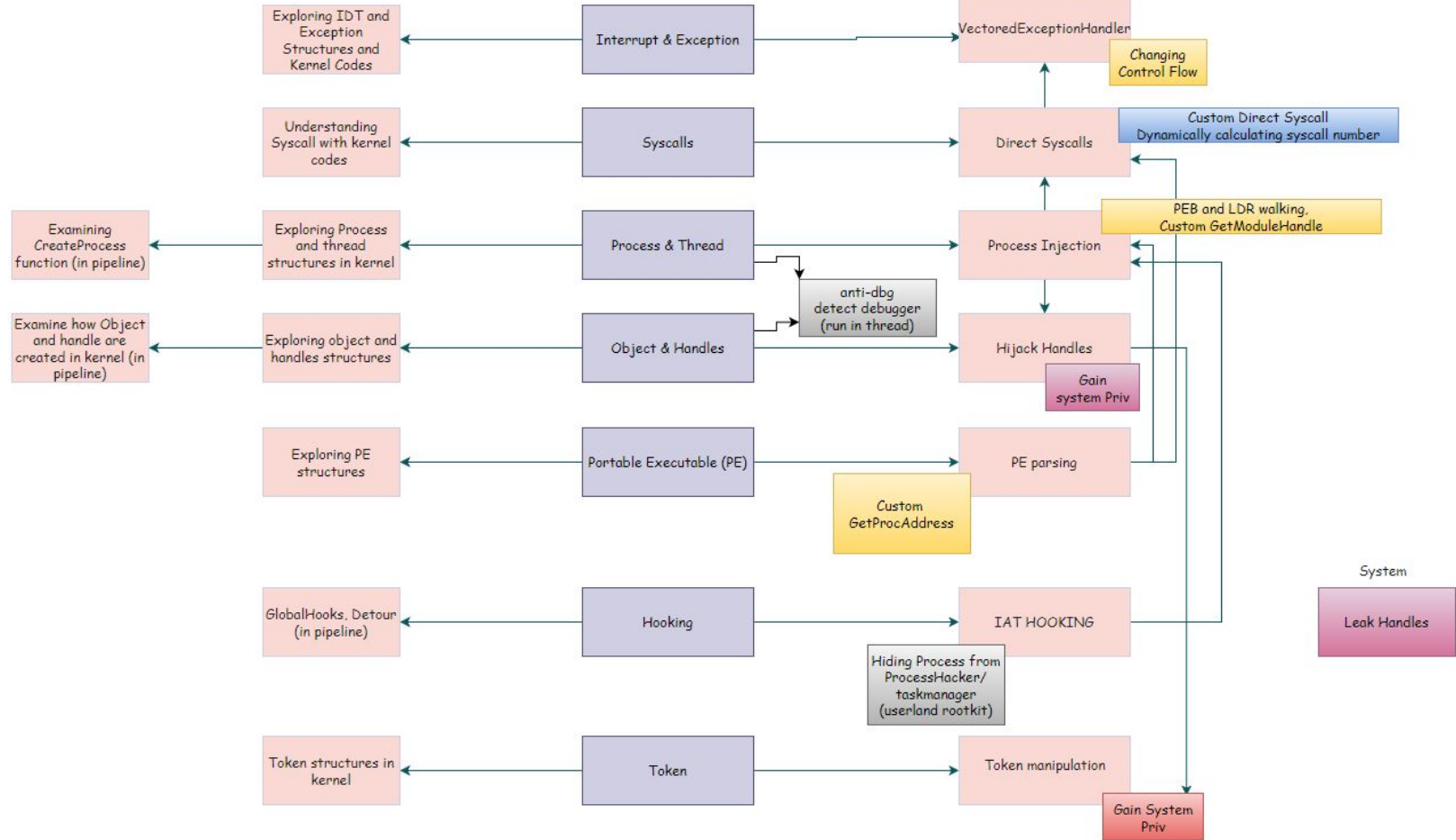Introduction | The 10000 hour rule | The learning curve | Research | Method | Deconstruct |... 12 chapters

19:27

ⓘ Fact:

It's impossible to cover everything about windows internals in 20 hours of video course

Internals

Userland Attack Techniques Challenges

Internals		Userland Attack Techniques
Exploring IDT and Exception Structures and Kernel Codes	← Interrupt & Exception	VectoredExceptionHandler
		Changing Control Flow
Understanding Syscall with kernel codes	← Syscalls →	Direct Syscalls
		Custom Direct Syscall Dynamically calculating syscall number
Examining CreateProcess function (in pipeline)	← Exploring Process and thread structures in kernel ← Process & Thread →	Process Injection
		PEB and LDR walking, Custom GetModuleHandle
	anti-dbg detect debugger (run in thread)	
Examine how Object and handle are created in kernel (in pipeline)	← Exploring object and handles structures ← Object & Handles	Hijack Handles
		Gain system Priv
Exploring PE structures	← Portable Executable (PE) →	PE parsing
	Custom GetProcAddress	
GlobalHooks, Detour (in pipeline)	← Hooking →	IAT HOOKING
	Hiding Process from ProcessHacker/ taskmanager (userland rootkit)	
Token structures in kernel	← Token →	Token manipulation
		Gain System Priv

System

Leak Handles

How To Get Certified?

COMPLETE ALL THE TASKS.

TAKE AN EXAMINATION.
> 12 HOURS FOR TASK
> 8 HOURS TO GENERATE REPORT

YOUR REPORT WILL BE MANUALLY ASSESSED

IF YOU PASS THE TEST, YOU'LL BE CERTIFIED

CYBERWARFARE LABS
THIS IS TO CERTIFY THAT

Has successfully completed the exam requirements and is recognized as a
Certified Windows Internals
Red Team Operator

Date:
ID:

Where To Go?

1 EXAMINE THE INTERNALS IN MORE DETAIL

2 TOOLS & MALWARE DEVELOPMENT

3 MALWARE ANALYSIS

4 KERNEL EXPLOIT DEVELOPMENT

5 ROOTKIT DEVELOPMENT

We Are Giving away 1 Seat of CWI-RTO

*Note: The Giveaway winner will be announced only after attending the CWI-RTO Launch Webinar.

THANK YOU

Do you have any questions?
info@cyberwarfare.live