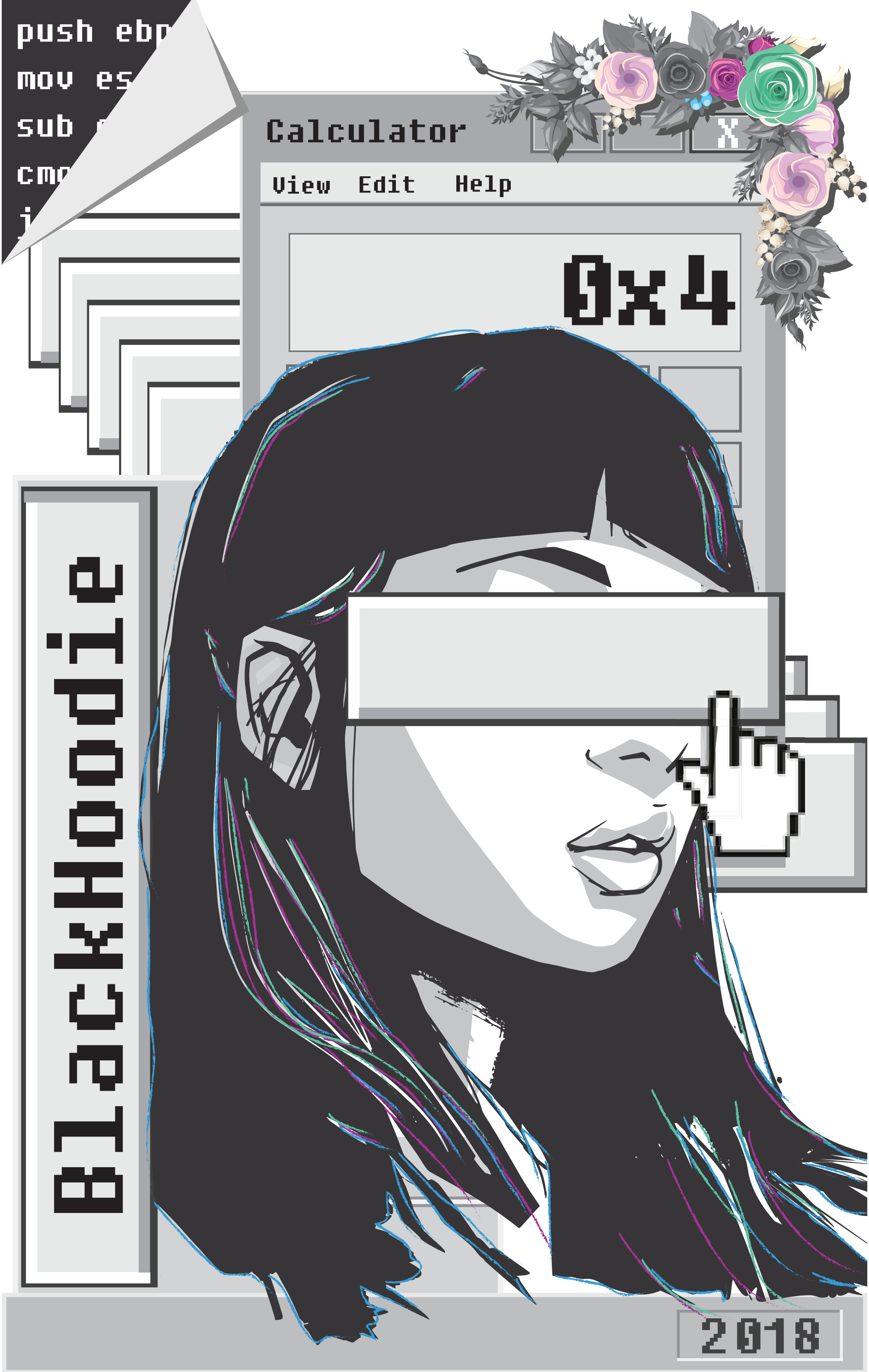

push ebp
mov es
sub
cmp
j
Calculator
View Edit Help
X
0x4
BlackHoodie
2018

Contents

Welcome

We roll again, Berlin November 16th-18th! 3 tracks of workshops, two introductory ones, one advanced; one track is me yelling my usual litany, the other two are entirely held by former attendees and will feature topics of their likings. That might or might not include Windows kernel, ARM, car hacking, yada yada, yes we now hack everything, did I mention that? Former BlackHoodies keep blowing my mind with their advances in not only RE but oh so many different areas. I keep on thinking we might in the end indeed change an industry. Speaking of which, you can be part of it. BlackHoodie #4 will again be free, women-only and super challenging. ALSO, we will again have a one day conference before the workshops, cause two days apparently are not enough!

WHY WOMEN ONLY

Because a girl-to-girl conversation is so much more fruitful than a full classroom with only one or two women hiding in the corners. I've done so many things in my life where I was the only girl among X other participants, and I promise I've been hiding in the corners more than once.

For the gents it might not be that obvious, but it is not easy for young females who haven't yet found their place in life to walk into a class room, a university lecture, an office or a conference room full of men. Who, generally speaking, very often very well seem to know their place.

I've had girls in my classes before, hiding and holding back although I am so certain they would have been capable to be so much better than what their final results showed. So yeah this will be women only, for every female should feel welcomed and encouraged to do her best and get the most out of it.

WHY MORE WOMEN IN LOW-LEVEL TECHNICAL JOBS IN GENERAL

- It's difficult. Mastering something difficult makes you happy. I want all of you to be happy.
- It pays well. While money makes you also happy, what's more important, it gives you courage and independence.
- It keeps you busy. Lots of open job positions globally, even better, believe it or not it is addictive and you might even find yourself a new hobby.

HARDFACTS

- There won't be slides, there will be you, and your debugger, only.
- Online preparation assignments, 4 of them, over the course of two months prior to the workshop
- No fees, no strings attached, all you have to do is get there

WHY ARE WE DOING THIS

The concept of women-only has no intention of pulling up walls or feeling exclusive, we don't need special help, don't need to be prefered by anything or anyone. I repeat, none of us could give less f*** about being granted a single thing based on our gender.

Blackhoodie is about creating space in an industry that's by definition offensive and very competitive, it is a special invitation for talents who wouldn't otherwise find the courage to start hacking on their own. It is a place, where attendees feel encouraged to grow skills without pressure, where they can be themselves without having to compete.

And, it works. BlackHoodie alumnis have gone far beyond all expectations since the workshop series started. They now hack minesweeper into showing where the damn flags are, give talks at international conferences on how to reconstruct C++ class hierarchies with SMT solvers, or how to gain code execution from XSS abusing the Electron framework, they hold workshops on car hacking, on ARM shellcode writing, on Windows kernel shim abuse.

They serve on conference review boards, including BlackHat our industry’s prime venue, and are listed on the prestigious Forbes 30under30 list. I kid you not, most of the BlackHoodie attendees haven’t stuck their noses into security research before they joined the bootcamp.

Why so successful you wonder? There are plenty of women out there who are ready to kill, but aren’t sure where to begin. BlackHoodie offers an easy start with a complex topic, packaged up with a courage boost and a neat network of contacts in the industry. This package, paired with the incomparable drive of a chronically underestimated minority, gives the ladies superpowers.

- Mari0n
🐦pinkflawd

Tips

- The weekend is going to be surprisingly exhausting. Make sure to keep yourself hydrated and sleep enough!

- Also, eat enough during the breaks. The workshops go on for 3-4 hours and it is not certain if there will be a break.

- Bring you own device with admin rights and charger as you want to get the most from this weekend.

- Join our IRC channel in freenode - #blackhoodie. Ask someone of the STAFF for the password.

- Have fun! Don't worry if you can't get everything in the first run. Ask, use the breaks to get to know new people and join us for the evening program, if you can!

Challenge

We have a challenge and you can win swag!

- ...for the first one to solve it
- ...for the best write-up of the solution

Go to https://tiny.cc/bh18-chall, password is : R0ck1ng4sh3!!

Send the flag before SUNDAY MIDDAY to: barbie@blackhoodie.re when you are done!

Calculator
X
View
Edit
Help
0x4
Talks
BlackHoodie
2018

Android_Emuroot: Abusing Google Play Emulator Debugging to RE Non-Cooperative Apps as Root

Short Talk

by anais

Rooting detection mechanisms implemented by Android applications can be a pitfall for reverse-engineers who want to study these applications. This presentation aims at sharing an interesting way based on Google Play emulator debugging to get a rooted shell not trivially detectable by the applications allowing to go further in reverse-engineering (RE).

Arming malware with GANs

Short Talk

by Maria Rigaki

This talk is about an application of Generative Adversarial Networks (GANs) in network security. More specifically, it is about our experiments in using GANs to modify malware C&C traffic so that it mimics normal network traffic in order for the malware to remain undetected while at the same time it continues to be effective.

Beating a Heavily Obfuscated App

Regular Talk

by Laura Tich and Evelyn Kilel

Obfuscation makes the source code unavailable which triggers the need to reverse engineer binaries as well as examine other file types in order to understand how they work and analyze their weak points. Reverse engineering an android application gives an understanding of how the application really works in the background and how it interacts with the actual device. This knowledge would assist in the process of discovery vulnerabilities that exist in the code and are not obvious. Additionally, some vulnerabilities are more visible in binary code than in source, so reverse engineering will find them first.

In this session, we will look at reverse engineering in penetration testing using a Frida especially for heavily obfuscated mobile applications that have complex obfuscation: Use of Magisk to check if root detection is enabled and all methods including renaming binaries (Magisk creates random names to any modules including hiding specific apps) proving very hard to decompile the applications. Enter DBI using Frida.re, dump the memory using Fridump and parse the readable strings to a file. As a Dynamic Binary Instrumentation (DBI) tool, Frida can enumerate the loaded modules and the classes on the application. Search through the file using normal keywords to find the obfuscation method/library that works.

We will also analyze all levels from a systems view down to individual functions which include how the app interacts with its processing and networking environment, the trust boundaries between components, and relevant lines of code. The process can uncover malware hidden in a seemingly legitimate application. We will do a step by step process of retrieving the APK file from google play store or the device itself to patching.

Bushwhacking Your Way Around a Bootloader

Regular Talk

by .bx

This talk will cover the methods and tools I developed to ”reverse engineer” the open source Das U-Boot bootloader, and how they can be applied more generally to as a dynamic analysis technique to correlate interesting events with control flow and ultimately a location in the binary/source code.
Even when you have access to some binary’s source code, it can still be challenging to understand said software. In this talk, I will discuss the techniques and I tools I developed in order to understand and navigate the pile of code that is the open-source Das U-Boot bootloader. The tools I developed do not rely on proprietary software and instead make use of free and powerful debugging tools such as Capstone, Unicorn, and the GDB Python plugin API. My approach strives to highlight the temporal and mechanical connections that exist between higher-level behaviors and regions of the code base/binary by instrumenting, tracing, and analyzing all memory writes with respect to the software’s current execution path. This technique allows us to develop and test our understanding of the relationships between code and objects (data structures and/or regions of memory). I will demonstrate how these tools and techniques can be used in practice by discussing how they were used to identify and distinguish between different phases of U-Boot execution (including distinct phases of initialization and relocation). This talk aims to be both accessible to software folk who merely want to learn more about bootloaders as well as interesting to those with bootloader and/or reverse-engineering experience.

Down the Drain: A Look into Pinball's Embedded Systems

Short Talk

by Anna Neal

I've been digging to into the pinball update file for fun. I had to create a little python tool to unpack the file. Then used strings to find out about the processor type and OS and find the files that were most interesting. I'm now learning radare2 to try and reverse through the binary a bit. This is not a finished project and I don't know where it will lead me but thought I should stick out my neck and try something scary.

Enter the Matrix (Ransomware)

Lightning Talk

by Luca Nagy

The Matrix ransomware family introduced some new techniques for obfuscating internal structures and embedded data. In this presentation, I'll walk attendees though my investigation of the Matrix ransomware family and a reverse engineering of its main components.

Fun with C++

Lightning Talk

by Carly

C++ has a lot of features. Sometimes what you think you are doing and what is actually happening are two different things. We are going to look at some C++ anti-patterns and how you can abuse them.

Hidden in Plain Sight

Regular Talk

by Essy

This talk will take a look at some living-off-the-land techniques and fileless persistence methods in Windows. Tools that are already installed on a system provide a good opportunity to hide in plain sight and Windows gives us various options to 'legitimately' play around. The overall goal is to point to interesting fields worth taking a closer look at later on.

JaSt: Fully Syntactic Detection of Malicious (Obfuscated) JavaScript

Regular Talk

by Aurore Fass

In this talk, we present JaSt, a low-overhead solution that combines the extraction of features from the abstract syntax tree with a random forest classifier to detect malicious JavaScript instances. Even though the analysis is entirely static, it yields a high detection accuracy of almost 99.5% and has a low false-negative rate of 0.54%.

Linux Security APIs and the Chromium Sandbox

Regular Talk

by Patricia Aas

The Linux Security and Isolation APIs have become the basis of some of the most useful features server-side, providing the isolation required for efficient containers. However, these APIs also form the basis of the Chromium Sandbox on Linux, and we will study them in that context in this talk.

Linux Servers Under Siege: a Real Case Forensic Analysis of a Cryptocurrency Miner Attack

Regular Talk

by Veronica Valeros

Everything started with an email alert to a network administrator hinting that something was not right in one of the organization’s Linux servers. What followed is two months of digital forensic analysis where we followed the trail of breadcrumbs left behind by the attackers, only to find that what we found was just the last of a series of attacks that have started almost a year before.

Malware Dissection 101 : TinyNuke

Short Talk

by Nha-Khanh Nguyen

What is a banking trojan ? How does it work ? Let's dissect a TinyNuke sample to find it out.

Last year, a massive malware campaign have been spotted targeting French and American banks. This banking trojan called TinyNuke or NukeBot targets American and French bank customers in order to steal credentials by keylogging. The presentation will cover a quick analysis of TinyNuke to understand how it works. So we will talk about basic malware analysis method including lab setup, macro word deobfuscation, basic anti-debugg bypass, dynamic analysis and finding IoCs. The goal of this presentation is to show that nowadays malwares are not always as tricky as we might think. Some are still basic and easy to dissect for beginners.

"May I See Your Credentials, Please?"

Regular Talk

by Dana Baril

Credential theft is an important part of the attacker playbook when attempting lateral movement. This process mostly involves dumping credentials saved locally on the machine. In many cases these passwords can be retrieve from the Windows Credential Manager, allowing attackers an easy path into the organization. This was evident in major attacks such as the NotPetya ransomware, and high-profile tools like Mimikatz. In this talk, we explain how to detect credential theft out of the Windows Credential Manager using Windows Defender Advanced Threat Protection (WDATP). This involves modifying the Windows operating system to send telemetry to the WDATP cloud which was extended with new detection rules.

Calculator
View
Edit
Help
0x4
BlackHoodie
Workshops
2018

Introduction to x86 RE

Track 1 [Beginners]

by Mari0n

Prerequisites

- Computer science background in a sense you understand programming logic, how a processor works and how an operating system works.
- A Notebook capable of running at least one virtual machine.
- A virtual machine, preferred Win7 32-bit.
- Guts :) (It is going to be a lot to learn in a very short time).

No need to have dealt with x86 before.

Description

In this track you will be introduced to the basics of malware analysis (static and dynamic) and reversing techniques.

Attendees will have to complete 4 homework assignments before the actual bootcamp in November.

Introduction to Hack All the Things

Track 2 [Beginners / Intermediate]

by Various

Prerequisites

- Basically similar as for track 1, computer science background in a sense you understand programming logic, how operating systems tick, what the essential parts of a web application are, basics of cryptography, how networks work, etc.
- Security affinity assumed.
- Don't fret if you don't come with ALL requirements, knowing a little bit of something is tots fine. ;)

No need to have dealt with x86 before.

Description

This includes introductory workshops on a broad range of topics which could treat crypto, web security, an intro to binary exploitation, network forensics, hardware security, telco security and so on.

Workshops

- A Beginner's Guide to Android Malware Analysis by Kristina Balaam
- Capture the Flag: An Introduction to Binary Exploitation by Katharina Männle
- ARM Exploitation 101 by Azeria

Reversing All the Things

Track 3 [Intermediate / Advanced]

by Various

Prerequisites

- Firm understanding of operating systems and computer architecture concepts.
- Exposure to x86 and x64 assembly and C language is assumed.
- Familiarity with debugging and reversing frameworks.
- Grasp of the TCP/IP protocols.
- Familiarity with VMware/VirtualBox and be able to import and configure virtual machines.
- Technical requirements for the specific workshops will be communicated in advance.

No need to have dealt with x86 before.

Description

This track includes workshops that we don't think beginners will find entertaining, since they require some understanding of topics listed above already. Typically former attendees bring mentioned requirements already. Workshops might tackle Windows kernel, ARM exploitation, one or another little hacking challenge. (TBC.)

Workshops

- Cryptography for Non-Cryptographers by Marion Videau
- Introduction to Return Oriented Programming by chiliz
- Introduction to Windows Kernel: Let's Keylog All the Things by Gwaby

The Blackhoodie brand, abstracts and graphics belong to
Marion Marschalek and their original owners.

This booklet is a non-profit project made for distribution at the Blackhoodie Bootcamp 2018.

Our intent is to help other women enjoy reverse engineering as well as other fields in information security and computer science to the fullest. We hope you all have an unforgettable experience. Thank you for coming.

WRITING
Thaís 🐦barbieauglend

LAYOUT & GRAPHICS
Essy 🐦casheeew

CHALLENGE CONCEPTION
Nha-Khanh 🐦N1aKan

CONTENT
Blackhoodie Team
🐦Blackhoodie_RE

TEAM BLACKHOODIE

Marion 🐦pinkflawd
Bhavna 🐦bsoman3
Gaby 🐦pwissenlit
Emma 🐦_kylma
Maria 🐦Fox0x01
Ninon 🐦__noutoff__
Priya 🐦priyachalakkal
Thaís 🐦barbieauglend

SPECIAL THANKS
here 🐦here
hack.lu 🐦hack_lu
Every attendee of
Blackhoodie #4