Black Hat 2018 tools list

Red C0de Follow
Aug 14, 2018 · 2 min read

2018 Black Hat Conference

2018 Black Hat Conference

Android, iOS and mobile hackers

Vulnerable iOS app: Swift version

https://github.com/prateek147/DVIA-v2

Code evaluation

OWASP dependency check

https://github.com/jeremylong/DependencyCheck

Cougar scan

Https://github.com/pumasecurity/puma-scan

encryption

DeepViolet: SSL / TLS scanning API and tools

https://github.com/spoofzu/DeepViolet

Data forensics and incident response

Beginner to expert

Https://github.com/bro/bro

CyBot: Open Source Threat Intelligence Chatbot

https://github.com/CylanceSPEAR/CyBot

LogonTracer

https://github.com/JPCERTCC/LogonTracer

Rastrea2r (reload!): Collect and hunt IOC with Gusto and Style
https://github.com/rastrea2r/rastrea2r

RedHunt OS (VM): Virtual machine for adversary emulation and threat search
https://github.com/redhuntlabs/RedHunt-OS

Exploitation and ethical hacking
AVET: AntiVirus Evasion Tool

Https://github.com/govolution/avet

DSP: Docker Security Playground
https://github.com/giper45/DockerSecurityPlayground

hideNsneak: Attack Confusion Framework
https://github.com/rmikehodges/hideNsneak

Merlin
https://github.com/Ne0nd0g/merlin

RouterSploit
https://github.com/threat9/routersploit

Hardware / Embedded
ChipWhisperer
https://github.com/newaetech/chipwhisperer

JTAGulator: Uncover the Achilles heel of hardware security
https://github.com/grandideastudio/jtagulator

Micro-Renovator: Bring the processor firmware into the code
https://github.com/syncsrc/MicroRenovator

TumbleRF: RF Blur becomes easy
https://github.com/riverloopsec/tumblerf

Walrus: Make the most of your card cloning device
https://github.com/TeamWalrus/Walrus

IoT
Scalable Dynamic Analysis Framework for IoT Devices
https://github.com/sycurelab/DECAF

BLE CTF project
https://github.com/hackgnar/ble_ctf

WHID Syringe and WHID Elite: Next Generation HID Aggressive Device
https://github.com/whid-injector/WHID

Malware Defense
Provides advanced deep learning analysis platform for every security researcher
https://github.com/intel/Resilient-ML-Research-Platform

EKTotal
https://github.com/nao-sec/ektotal

Firmware Audit: Platform Firmware Security Automation for Blue Teams and DFIR
https://github.com/PreOS-Security/fwaudit

MaliceIO
https://github.com/maliceio/malice

Goal—see MacOS Security Tools
https://github.com/objective-see

Malware offensive
BloodHound 1.5
https://github.com/BloodHoundAD/BloodHound

Cyber attack
armory
https://github.com/depthsecurity/armory

Chiron: An advanced IPv6 security assessment and penetration testing framework
https://github.com/aatlasis/Chiron

DELTA: SDN Security Assessment Framework
https://github.com/OpenNetworkingFoundation/DELTA

Mallet: Intercepting agent for any protocol

Https://github.com/sensepost/mallet

PowerUpSQL: PowerShell Toolkit for attacking SQL Server in an enterprise environment
https://github.com/NetSPI/PowerUpSQL

WarBerryPi
https://github.com/secgroundzero/warberry

Network Defense
ANWI (New Wireless IDS): $5 WIDS
https://github.com/SanketKarpe/anwi

CHIRON: Home-based network analysis and machine learning threat detection framework
https://github.com/jzadeh/chiron-elk

Cloud Security Suite: One-stop tool for AWS / GCP / Azure security auditing at
https://github.com/SecurityFTW/cs-suite

DejaVu: An open source spoofing framework
https://github.com/bhdresh/Dejavu

OSINT—Open Source Smart
DataSploit 2.0
https://github.com/DataSploit/dataspLoit

Dradis framework: Learn how to reduce reporting time by half
https://github.com/dradis/dradis-ce

Reverse Engineering
Snake: Malware Storage Zoo
https://github.com/countercept/snake

Smart Grid/Industrial Safety
GRFICS: Graphic Realism Framework for Industrial Control Simulation
https://github.com/djformby/GRFICS

Vulnerability Assessment
Robustness Toolbox for Machine Learning Models
https://github.com/IBM/adversarial-robustness-toolbox

Android Dynamic Analysis Tool (ADA)
https://github.com/ANELKAOS/ada

Archery: Open Source Vulnerability Assessment and Management
https://github.com/archerysec/archerysec

Boofuzz
https://github.com/jtpereyda/boofuzz

BTA
https://github.com/airbus-seclab/bta

Take advantage of
https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit

Halcyon IDE: for Nmap script developers
https://github.com/s4n7h0/Halcyon

SimpleRisk
https://github.com/simplerisk

TROMMEL
https://github.com/CERTCC/trommel

Web AppSec
Take a look at NGINX's ModSec 3.0: Software Web Application Firewall
https://github.com/SpiderLabs/ModSecurity

Astra: Automatic security testing of the REST API
https://github.com/flipkart-incubator/Astra

Burp Replicator: Replication of automated complex vulnerabilities
https://github.com/PortSwigger/replicator

OWASP offensive web testing framework
https://github.com/owtf/owtf

OWASP JoomScan project
https://github.com/rezasp/joomscan

WSSAT
https://github.com/YalcinYolalan/WSSAT

Blackhat | Information Security | Infosec | Penetration Testing | Pentesting

Fool that mlAuth

Files

https://drive.google.com/file/d/1QvZBVns4ei1fqnhDe2uEBKiaEeusp=sharing

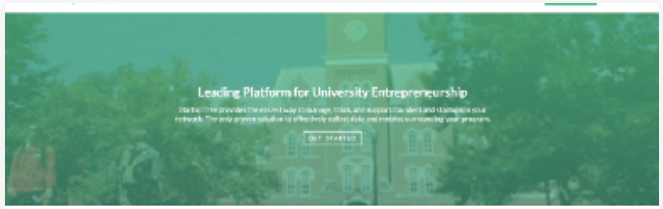
Related reads

Nullcon-HackIM CTF 2019- MLAuth-Misc(500)Writeup

Aagam shah

Feb 3 · 4 min read

352



Related reads

Open Redirects & Security Done Right!

Akshay 'Ax' Sharma

Jun 19, 2018 · 3 min read

390

Related reads

Secnotes Write-up (HTB)

George O

Jan 20 · 6 min read

213