Security Tools

Most Important Endpoint Security & Threat Intelligence Tools List for Hackers and Security Professionals

By **BALAJI N** - June 4, 2018 0

Most Important Endpoint Security
Threat Intelligence Tools List

Endpoint Security & Threat Intelligence Tools are more often used by security industries to test the vulnerabilities in network and applications. Here you can find the Comprehensive Endpoint Security & Threat Intelligence Tools list that covers Performing Penetration testing Operation in all the Corporate Environments.

Also Read: **Here is the list of Black Hat Arsenal Europe 2017 Tools List**

Newsletter

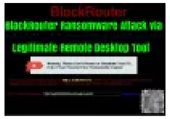
Signup to get Hacking News & Tutorials to your Inbox

Name

Email *

Subscribe

Most Popular



New Ransomware Called “BlackRouter” Attack launched through Well-known Legitimate Remote Desktop...

May 5, 2018

New Sophisticated Blackmailing RedDrop Malware that Records

Endpoint

Anti-Virus / Anti-Malware

- Linux Malware Detect – A malware scanner for Linux designed around the threats faced in shared hosted environments.

Content Disarm & Reconstruct

- DocBleach – An open-source Content Disarm & Reconstruct software sanitizing Office, PDF and RTF Documents.

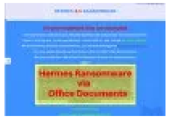
Configuration Management

Nearby Audio on Infected...

February 28, 2018

Russia Ordered Telegram to Handover the Encryption keys

March 22, 2018



Hermes Ransomware Distributed Through Malicious Office Documents Embedded Flash Exploit

March 17, 2018

87 Million Facebook Users Affected by the Cambridge Analytica Data Breach...

April 5, 2018

Recommended

4 Cybersecurity Risks We willl Face With New WhatsApp Status...

5 Methods to Secure Your Company's Data from Cybercriminals

- Rudder – Rudder is an easy to use, web-driven, role-based solution for IT Infrastructure Automation & Compliance. Automate common system administration tasks (installation, configuration); Enforce configuration over time (configuring once is good, ensuring that configuration is valid and automatically fixing it is better); Inventory of all managed nodes; Web interface to configure and manage nodes and their configuration; Compliance reporting, by configuration and/or by node.

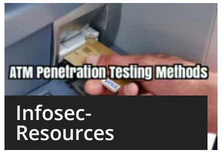
Authentication

- google-authenticator – The Google Authenticator project includes implementations of one-time passcode generators for several mobile platforms, as well as a pluggable authentication module (PAM). One-time passcodes are generated using open standards developed by the Initiative for Open Authentication (OATH) (which is unrelated to OAuth). These implementations support the HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226 and the Time-based One-time Password (TOTP) algorithm specified in RFC 6238. Tutorials: How to set up two-factor authentication for SSH login on Linux

Mobile / Android / iOS

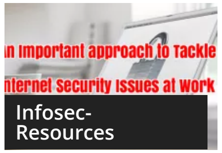
A perfect way to Start and Strengthen your Cyber Security Career

Adobe & Microsoft released New Critical Security updates for software...

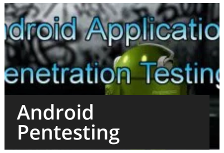


Advanced ATM Penetration Testing Methods

All that You Should Know About Bitcoins and How Does Bitcoin...


n important approach to Tackle
nternet security issues at work
Infosec-Resources

An Important Protection Approach to Tackle Internet Security Issues at Work



Android Application Penetration Testing – Part 1

- SecMobi Wiki – A collection of mobile security resources which including articles, blogs, books, groups, projects, tools and conferences. *
- OWASP Mobile Security Testing Guide – A comprehensive manual for mobile app security testing and reverse engineering.
- OSX Security Awesome – A collection of OSX and iOS security resources

Forensics

- grr – GRR Rapid Response is an incident response framework focused on remote live forensics.
- Volatility – Python based memory extraction and analysis framework.
- mig – MIG is a platform to perform investigative surgery on remote endpoints. It enables investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security.
- ir-rescue – *ir-rescue* is a Windows Batch script and a Unix Bash script to comprehensively collect host forensic data during incident response.

Threat Intelligence Tools

Android Pentesting

Android Application Penetration Testing – Part 8

Android Pentesting

Android Application Penetration Testing – Part 9

Android Pentesting

Android Application Penetration Testing – Part 10

Android Pentesting

Android Application Penetration Testing – Part 11 – Android Checklist

Android Pentesting

Android Application Penetration Testing – Part 12

Android Pentesting

Android Application Penetration Testing – Part 5

Android Pentesting

Android Application

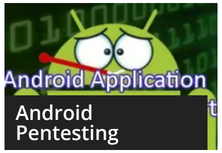
Android Pentesting

Android Application

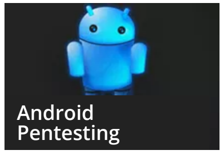
- abuse.ch – ZeuS Tracker / SpyEye Tracker / Palevo Tracker / Feodo Tracker tracks Command&Control servers (hosts) around the world and provides you a domain- and an IP-blocklist.
- Emerging Threats – Open Source – Threat Intelligence Tools fo Emerging Threats began 10 years ago as an open source community for collecting Suricata and SNORT® rules, firewall rules, and other IDS rulesets. The open source community still plays an active role in Internet security, with more than 200,000 active users downloading the ruleset daily. The ETOpen Ruleset is open to any user or organization, as long as you follow some basic guidelines. Our ETOpen Ruleset is available for download any time.
- PhishTank – PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
- SBL / XBL / PBL / DBL / DROP / ROKSO – The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective anti-spam legislation.

Penetration Testing Part – 4

Penetration Testing Part 2



Android Application Penetration testing Part 3



Android Application Penetration Testing Part 6

Android Application Penetration Testing- Part 7

APT Groups Cyber Attack to Hack Various Companies Web Servers
Cyber Attack

APT Group Cyber Attack to Hack Various Companies Web Servers Using...

- Internet Storm Center – The ISC was created in 2001 following the successful detection, analysis, and widespread warning of the Li0n worm. Today, the ISC provides a free analysis and warning service to thousands of Internet users and organizations, and is actively working with Internet Service Providers to fight back against the most malicious attackers.
- AutoShun – Threat Intelligence Tools called AutoShun is a Snort plugin that allows you to send your Snort IDS logs to a centralized server that will correlate attacks from your sensor logs with other snort sensors, honeypots, and mail filters from around the world.
- DNS-BH – The DNS-BH project creates and maintains a listing of domains that are known to be used to propagate malware and spyware. This project creates the Bind and Windows zone files required to serve fake replies to localhost for any requests to these, thus preventing many spyware installs and reporting.
- AlienVault Open Threat Exchange – Threat Intelligence Tools called AlienVault Open Threat Exchange (OTX), to help you secure your networks from data loss, service disruption and system compromise caused by malicious IP addresses.
- Tor Bulk Exit List – CollecTor, your friendly data-collecting service in the Tor network. CollecTor fetches data from various nodes and services in the public Tor network and makes it available to the world. If you’re doing research on

the Tor network, or if you’re developing an application that uses Tor network data, this is your place to start. TOR Node List / DNS Blacklists / Tor Node List

- leakedin.com – The primary purpose of leakedin.com is to make visitors aware about the risks of loosing data. This blog just compiles samples of data lost or disclosed on sites like pastebin.com.
- FireEye OpenIOCs – FireEye Publicly Shared Indicators of Compromise (IOCs)
- OpenVAS NVT Feed – The public feed of Network Vulnerability Tests (NVTs). It contains more than 35,000 NVTs (as of April 2014), growing on a daily basis. This feed is configured as the default for OpenVAS.
- Project Honey Pot – Project Honey Pot is the first and only distributed system for identifying spammers and the spambots they use to scrape addresses from your website. Using the Project Honey Pot system you can install addresses that are custom-tagged to the time and IP address of a visitor to your site. If one of these addresses begins receiving email we not only can tell that the messages are spam, but also the exact moment when the address was harvested and the IP address that gathered it.
- virustotal – VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website

scanners. At the same time, it may be used as a means to detect false positives, i.e. innocuous resources detected as malicious by one or more scanners.

- IntelMQ – IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets using a message queue protocol. It’s a community driven initiative called IHAP (Incident Handling Automation Project) which was conceptually designed by European CERTs during several InfoSec events. Its main goal is to give to incident responders an easy way to collect & process threat intelligence thus improving the incident handling processes of CERTs. ENSIA Homepage.
- CIFv2 – CIF is a cyber threat intelligence management system. CIF allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route).
- CriticalStack – Free aggregated threat intel for the Bro network security monitoring platform.

Share and Support Us :

117

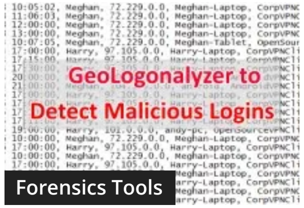
TAGS Endpoint Security Threat Intelligence

BALAJI N

http://www.gbhackers.com

BALAJI is a Security Researcher (Threat Research Labs) at Comodo Cybersecurity. He is a Certified Ethical Hacker, Editor-in-Chief, Author & Co-Creator of GBHackers On Security

RELATED ARTICLES MORE FROM AUTHOR



Forensics Tools

Open Source Tool GeoLogonalyzer to Detect Malicious Logins

Pornhub launches its own VPNHub
Surf Anonymously & Bypass censors

Security News

Pornhub launches its own VPNHub for Safe Browsing, Bypass Censors & Surf Anonymously

Computer Security

The Pirate Bay will be blocked by Sweden ISP Telenor Without Any Changes After Court Order

Crypto Attacks

Ubuntu Snap Store Apps Contains Hidden Cryptocurrency Miner Malware

‹ ›

1 Comment GBHackers on Security 1 Login

♡ Recommend Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Yossi Mor • 4 months ago

Hi

Very good artical.

Are you familier with security audit tools to examine windows os statrs?

I hadl used winspect powershellpscript, but for old os version such as xp it is not suitable.

Regards

Yossi

GBHackers on Security

ABOUT US

GBHackers on Security is Advanced Persistent Cyber Security Online platform which including Cyber Security Research,Web Application and Network Penetration Testing, Hacking Tutorials,Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: admin@gbhackers.com

FOLLOW US