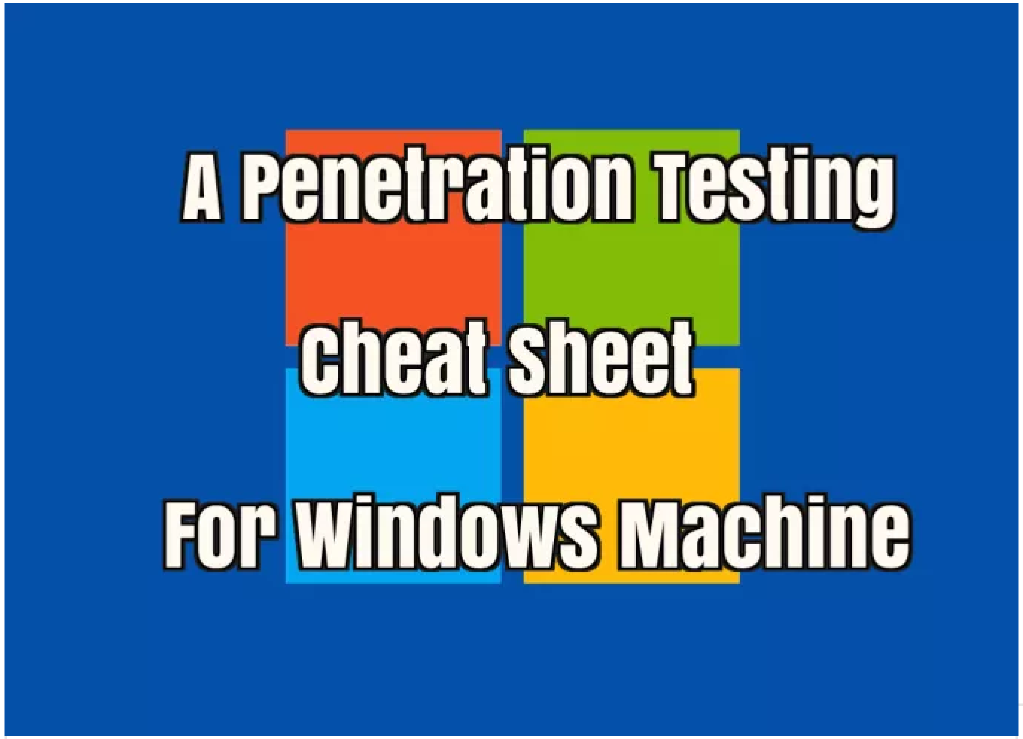
TECHINCIDENTS

SECURITY

Penetration Testing Cheat Sheet For Windows Machine – Intrusion Detection

By **Anonymous Geek** - November 5, 2017 0

SHARE Facebook Twitter



In the event that your Windows machine has been compromised or for any other reason, this Penetration Testing Cheat Sheet is intended to help.

This Penetration Testing Cheat Sheet article is for Windows Administrators and security personnel to better execute a thorough examination of their framework (inside and out) keeping in mind the end goal is to search for indications of compromise.

Recent Posts

How To Turn On Gmail Offline Mode To Use Gmail Without...

RanJitH - May 29, 2018 0

Gmail was as of late updated after a long stretch of around a long time since its released in 2004. Of all the outstanding...

Look for unusually scheduled tasks, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name.

Some legitimate Windows apps can be scheduled to perform certain actions without direct user interaction. For example, you can download this tool to **convert MP4 to AVI** and set it to shut down your PC when conversion process finishes. This is a healthy expected outcome. However, risky apps may abuse your system, so follow our checkup guide below.

Apart From this You can Read Many Penetration testing Articles Here .

Also Read – **Become Master in Cyber Security with Complete Advance Level Security Course Bundle**

1.Unusual Log Entries:

Check your logs for suspicious events, such as:

- **“Event log service was stopped.”**

How To Download WhatsApp Statuses

RanJitH - May 23, 2018 0

A year ago, WhatsApp thinks of an extremely imaginative element of WhatsApp Statuses which enable clients to include Videos, Photo or Text with Emoji...

How To Protect Your Wi-Fi Network

RanJitH - May 19, 2018 0

Wi-Fi is one section point hackers can use to get into your system without setting foot inside your building since remote is substantially more...

- **“Windows File Protection is not active on this system.”**
- **“The protected System file [file name] was not restored to its original, valid version because of the Windows File Protection…”**
- **“The MS Telnet Service has started successfully.”**
- **Look for a large number of failed logon attempts or locked out accounts.**

Penetration Testing Cheat Sheet To do this using the GUI, run the Windows event viewer:

C:> eventvwr.msc

Using the command prompt:

C:> eventquery.vbs | more

Or, to focus on a particular event log:

C:> eventquery.vbs /L security

Also Read: **Google : Microsoft is putting Windows 7 and 8.1 users in danger By only patching Windows 10**

How To Use Google Services As Proxy Server

RanJitH - May 4, 2018 0

You can utilize the services of google as a proxy server, yes, it is conceivable and this will work perpetually on your server to...

How To Secure Your Gmail Account From Hackers

RanJitH - April 26, 2018 0

The vast majority doesn't understand how helpless their Gmail Account is to digital hackers. A portion of our most touchy data is put away...

2.Unusual Processes and Services:

Look for unusual/unexpected processes, and focus on processes with User Name “SYSTEM” or “Administrator” (or users in the Administrators’ group). You need to be familiar with normal processes and services and search for deviations.

Using the GUI, run Task Manager:

C:> taskmgr.exe

Using the command prompt:

C:> tasklist

C:> wmic process list full

Also look for unusual services.

Using the GUI:

C:> services.msc

Using the command prompt:

How to Compress Images Online without Losing Quality

RanJitH - April 24, 2018 0

At the point when a picture size is more, it might have a good pixels, and that implies putting away all data for a...

How To Check If Your Facebook Data Was Leaked To Cambridge...

RanJitH - April 18, 2018 0

Facebook has begun notifying up to 87 million individuals that their data was disgracefully acquired by Cambridge Analytica, however not every person has gotten...

```
C:> net start
C:> sc query
```

For a list of services associated with each process:

```
C:> tasklist /svc
```

Also Read –

Also Read –

Also Read –

3 Complete Advance Level Security Course Bundle for just $59

3.Unusual Files and Registry Keys

Check file space usage to look for sudden major decreases in free space, using the GUI (right-click on a partition), or type:

```
C:> dir c:
```

How To Hack Facebook Account Password

RanJitH - April 17, 2018 0

Hack Facebook account password is a standout amongst the most looked and hotly debated issues around the web. Facebook assumes a critical part in...

How To Find Out How Safe Is Your Android Smartphone

RanJitH - April 16, 2018 0

It appears that some Android cell phone creators are deceiving clients about the fix status of their gadgets, disclosing to them that they're up...

Look for unusually big files:

Start–> Search–>For Files of Folders… Search Options–>Size–>At Least 10000KB

Look for strange programs referred to in registry keys associated with system start up:

HKLMSoftwareMicrosoftWindowsCurrentVersionRun

HKLMSoftwareMicrosoftWindowsCurrentVersionRunonce

HKLMSoftwareMicrosoftWindowsCurrentVersionRunonceEx

Note that you should also check the HKCU counterparts (replace HKLM with HKCU above).
Using the GUI:

C:> regedit

Using the command prompt:

C:> reg query <reg key>

How to Clear Application Cache In 4 Quick Ways

RanJitH - April 9, 2018 0

Cached data are app-specific Files stored by an application in a reserved space so that every time you load the application, it already has…

4.Penetration Testing Cheat Sheet for Unusual Network Usage

Look at file shares, and make sure each has a defined business purpose:

C:> net view \127.0.0.1

Look at who has an open session with the machine:

C:> net session

Look at which sessions this machine has opened with other systems:

C:> net use

Look at NetBIOS over TCP/IP activity:

C:> nbtstat –S

Look for unusual listening TCP and UDP ports:

C:> netstat –na

For continuously updated and scrolling output of this command every 5 seconds:

C:> netstat –na 5

The –o flag shows the owning process id:

C:> netstat –nao 5

The –b flag shows the executable name and the DLLs loaded for the network connection.

C:> netstat –naob 5

Note that the –b flag uses excessive CPU resources. Again, you need to understand normal port usage for the system and look for deviations.

Also, check Windows Firewall configuration:

C:> netsh firewall show config

5.Unusual Scheduled Tasks

Look for unusually scheduled tasks, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name.

Using the GUI, run Task Scheduler:

Start–>Programs–>Accessories–>System Tools–>Scheduled Tasks

Using the command prompt:

C:> schtasks

Check other autostart items as well for unexpected entries, remembering to check user autostart directories and registry keys.

Using the GUI, run msconfig and look at the Startup tab:

Start –> Run, msconfig.exe

Using the command prompt:

C:> wmic startup list full

6.Unusual Accounts

Look for new, unexpected accounts in the Administrators group:

C:> lusrmgr.msc

Click on Groups, Double Click on Administrators, then check members of this group.
This can also be done at the command prompt:

```
C:> net user
C:> net localgroup administrators
```

7.Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU:

Task Manager –> Process and Performance tabs

Look for unusual system crashes, beyond the normal level for the given system.

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

TAGS CHEAT SHEET WINDOWS

SHARE f G+ Like 458 Tweet

Previous article

OMG: Apple could Become World's First Trillion Dollar Company

Next article

Top 5 Dangerous Hackers Groups that made the Invisible Internet as a Background

Anonymous Geek

http://www.techincidents.com

I am here to guide you for Learning New Technology and Hacking to make a Better Technical Community

RELATED ARTICLES MORE FROM AUTHOR

Why Is CompTIA Security+ Certification So Popular? – Build Your Cyber security Career

Here Are A Few Shocking Statistics On Cyber security

Most Important Penetration Testing commands Cheat Sheet for Linux Machine

Comments Community 1 Login

♡ Recommend Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus Privacy Policy DISQUS

TECHINCIDENTS

About Us

With Techincidents we cover all the Tech Updates around the Globe, Mobile, Hardware, Software products Specifications and Genuine Review

Contact us:
admin@techincidents.com

Recent Posts

The Three Best Web Browsers for Smartphones

Top Benefits Of Software Project Development Outsourcing For Your Business

New Best Putlocker Proxy 2018 & Putlocker Unblocked Mirror WebSites List (100% Working)

Home TECH Hacking GADGETS HOW TO TOP 5 What Is
Advertise Entertainment