A Penetration Testing Cheat Sheet For Windows Machine – Intrusion Detection

gurubaran

March 26, 2017 | Views: 22402

Save

Email

In the event that your Windows machine has been compromised or for any other reason, this cheat sheet is intended to help. This 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.

1.Unusual Log Entries:

Check your logs for suspicious events, such as:

- **"Event log service was stopped."**

- **“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.**

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
```

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:

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

For a list of services associated with each process:

C:> tasklist /svc

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:

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>
```

4.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.

You can get more articles in our Website https://gbhackers.com/

Ready to share your knowledge and expertise?

Submit to 0P3N

10 Comments

INFOSECTDK

10:15 am on March 12, 2018

I useful reminder that tipped me off to try something on a server.

Log in to Reply

MasterK

11:30 pm on April 2, 2017

Very good checklist.

Thanks for your time.

Log in to Reply

A Farook

11:03 am on March 30, 2017

Great article

Log in to Reply

w@y&3

5:52 am on March 29, 2017

Great thanks and I would like to add something to be more effective of these commands. You can export the command results by doing “Command > ...txt”. By doing so you can see various outputs to a text file as export.

Log in to Reply

THEDUDE

1:31 am on March 29, 2017

Thanks for taking time to do this, man. Very helpful reference.

Log in to Reply

Comment on This

You must be logged in to post a comment.

Related Reads

Cloud-Based Application

December 6, 2016 7578
By: Hari Charan

A Penetration Testing Cheat

March 26, 2017 22402
By: gurubaran

September 2017 Hall of Fame

October 9, 2017 352
By: Bugcrowd

WannaCry Ransomware

June 22, 2017 370
By: Tripwire

OUR REVOLUTION

We believe Cyber Security training should be free, for everyone, FOREVER. Everyone, everywhere, deserves the OPPORTUNITY to learn, begin and grow a career in this fascinating field. Therefore, Cybrary is a free community where people, companies and training come together to give everyone the ability to collaborate in an open source way that is revolutionizing the cyber security educational experience.

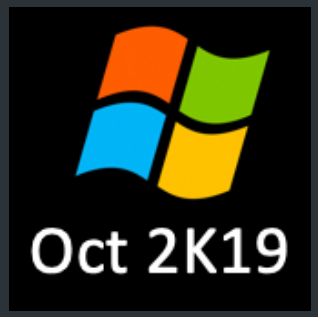
STUDENT SUPPORT

Get Support

OTHER PAGES

- About
- Join Our Team
- Press
- Terms of Service
- Verify Certificate
- Submit Suggestions
- Companies

SUPPORT CYBRARY



Donate Here to Get This Month's Donor Badge

CYBRARY|0P3N

charon223
What is the need of secure and strong passwords?
Views: 338 / October 8, 2019

rebeccaberis2
PCI Security Compliance Challenges and Best Practices
Views: 427 / October 7, 2019

slwelty
National Cybersecurity Awareness Month
Views: 1614 / October 4, 2019

GarrettsG2
When Should IT Pros Take CISSP Training?
Views: 2046 / October 3, 2019