



```
ping
```

```
ping -n 0 127.0.0.1
```

```
ping /n 0 127.0.0.1
```

```
find /i keyword
```

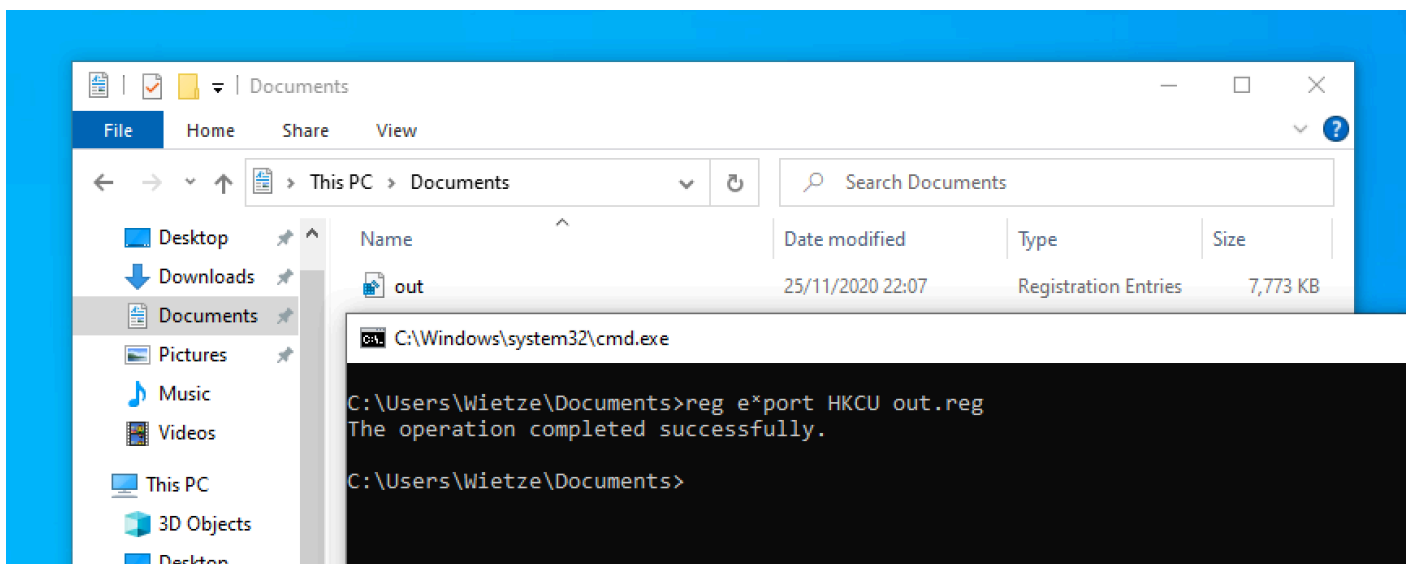
```
find -i keyword
```

```
certutil
```

```
reg
```

```
reg export HKCU out.reg
```

```
reg e*port HKCU out.reg
```

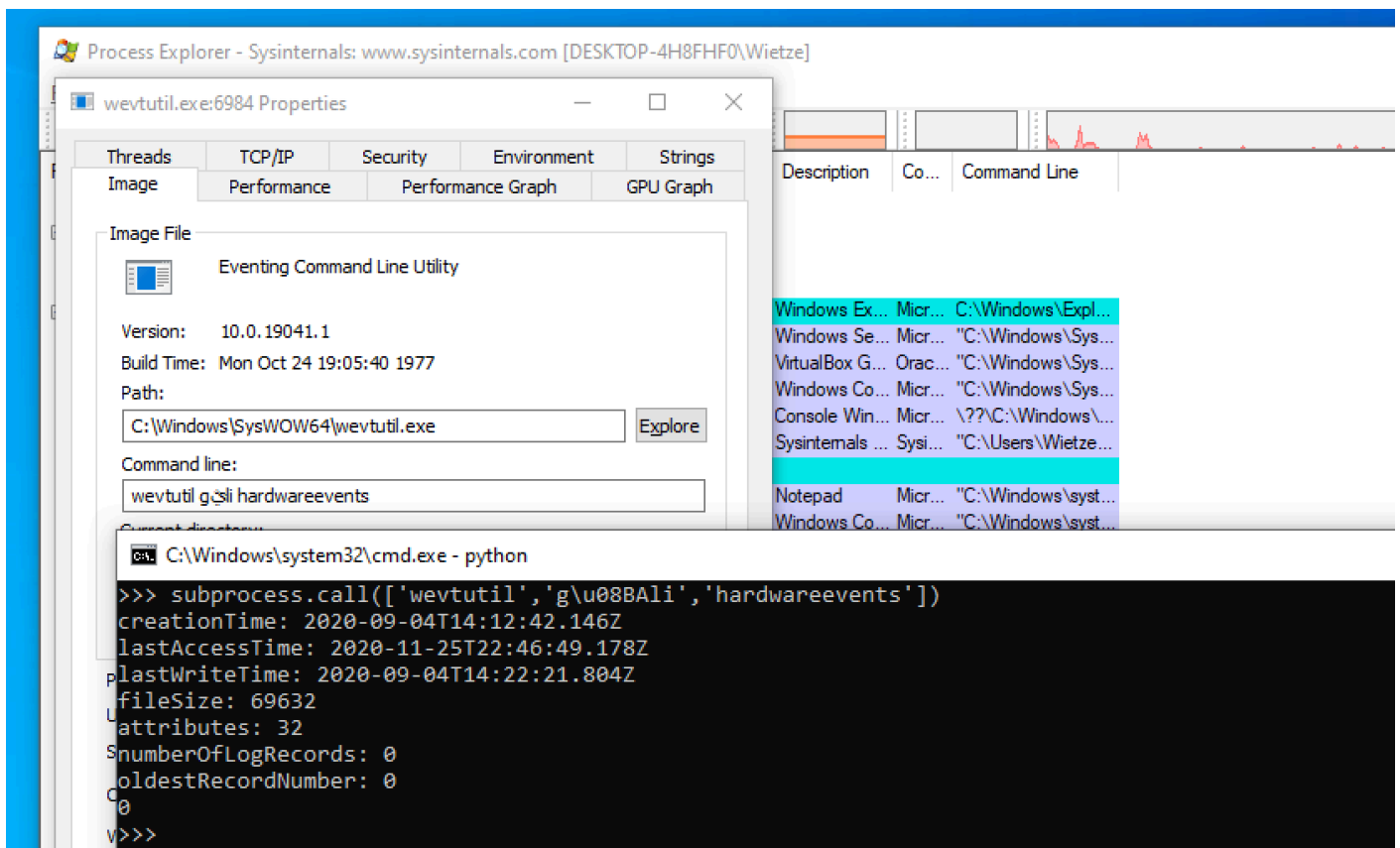


```
reg e*port HKCU out.reg
```

wevtutil

wevtutil gli hardwareevents

wevtutil gلي hardwareevents

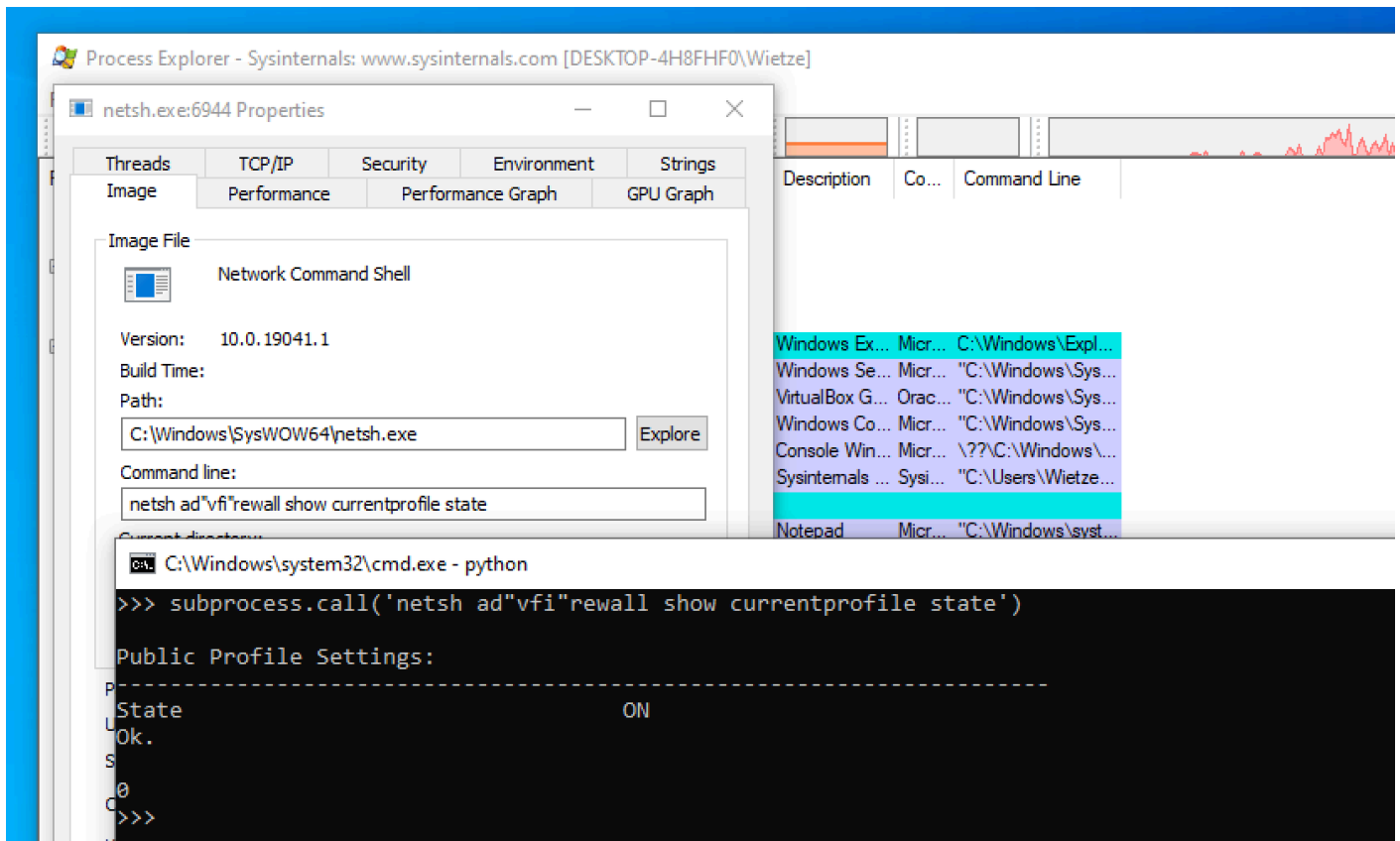


wevtutil gلي hardwareevents

dir "c:\windows\"

dir c:\windows\

```
dir c:\"win"d"ow"s"
```



```
netsh ad"vfi"rewall show currentprofile state
```

```
cmd
```

```
netsh ad""vfi""rewall show currentprofile state
```

```
grep -i keyword
```

```
grep --ignore-case keyword
```

```
cmdkey /l
```

```
cmdkey /list
```

```
wevtutil gli
```

```
wevtutil get-logininfo
```

```
Administrator: Command Prompt

C:\Windows\system32>powershell /encodedcommand ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedcomman ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedcomma ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedcomm ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedcom ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedco ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encodedc ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encoded ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encode ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /encod ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /enco ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /enc ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /en ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>powershell /e ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=
It works!

C:\Windows\system32>
```

`powershell /encodedcommand ZQBjAGgAbwAgACIASQB0ACAAdwBvAHIAawBzACEAIgA=`

`/e`

`/noprofile`

`/nop`

`/no`

`/noexit`

`/ec`

`/encodedcommand`

arp.exe					
at.exe					
bitsadmin.exe					
cacls.exe					
certutil.exe					
cmdkey.exe					
cmstp.exe					
csc.exe					
curl.exe					
findstr.exe					
fltmc.exe					
forfiles.exe					
icacls.exe					
ipconfig.exe					
jsc.exe					

nslookup -querytype=ALL (...)

nslookup

-q

```
urlcache
```

f

- "cur" "cach"e

```
/url"cach"e
```





```
detection:
  selection:
    Image: "*\\certutil.exe"
    CommandLine|contains|all:
      - "urlcache"
      - "f"
  condition: selection
```

/urlcache

f

/f

urlcache

[-/\\]

```
detection:
  selection:
    Image: "*\\certutil.exe"
    CommandLine|re: "^(?=.*[-/\\]urlcache)(?=.*[-/\\]f).+.*"
  condition: selection
```

wevtutil

wevtutil

---

---

---

---
