Worker - 14th Nov 20

by ippsec

Scanning

We ran services.nse against all open TCP ports from our initial nmap scan, WinRM ports, and the Azure Devops port. We found that port 5985 is open, which means we can use Evil-WinRM to connect to the box.

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|   Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: IIS Windows Server
3690/tcp open  svn     (access denied)
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Not Found
8080/tcp open  http    Microsoft IIS 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|   Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: Azure DevOps
Service Info: Host: WORKER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Enumeration

There's no reason to enumerate port 5985, as if we find more time to be able to access port 80 or port 8080 then we can then create.

I didn't think the enumeration port 3690, as we can see that port failed we can access port 80 and port 8080.

SVN

SVN is a VCS, which can be accessed via another client.

```
svn: E170013: Unable to connect to host 'worker.htb': No route to host
svn: E170013: Unable to connect to host 'worker.htb': No route to host
```

Subversion

Use `svn ls svn://10.10.10.203` to list the directories that exist on the server, and use `svnlook -r 2 -t dump /var/svn/dimension` to dump the contents of the commit.

```
dev/
dev/hm.txt
dev/iis.txt
dev/nt.txt
Revision: 2
Prop-content-length: 129
Content-length: 129

K 7
svn:log
V 27
Initial dimension commit
K 10
svn:author
V 7
nathan
K 8
svn:date
V 27
2020-06-04T14:09:03.000000Z
PROPS-END

Node-path: dev/hm.txt
Node-kind: file
Node-action: add
Text-content-length: 0
Text-length: 0
Content-length: 10

PROPS-END
```

Hooks Enumeration

We can automate this from commits, and put it in the file `hook.sh`

```
svnlook -r 2 -t dump /var/svn/dimension | ./hook.sh -
```

If we change the hook class into the IO.Write gem, we can write a file. We can then use `rubber` gem with `-p` option to create a payload.

```
rubber -p -f /home/ippsec/.ssh/id_rsa.pub -m 'ippsec' -c '/var/www/html'
svnlook -r 2 -t dump /var/svn/dimension | ./hook.sh -
```

Log in as `ippsec` and we can SSH into the machine `worker$`

Hooks Exploit

Use `ln -s /var/svn/hooks/post-commit post-commit` to create a symlink to the post-commit hook, and then `svnadmin -r 2 -t dump /var/svn/dimension` to trigger the post-commit hook.

```
ln -s /var/svn/hooks/post-commit post-commit
svnadmin -r 2 -t dump /var/svn/dimension
```

Port 80 Enumeration

Use `ln -s /var/www/html/ /var/svn/dimension/www` to create a symlink to the web root, then `svn ls file://www`

```
svn ls file://www
svn: E000013: Commit failed (details follow):
svn: E000013: Unable to open file '/var/svn/dimension/db/revprops/0/0': Permission denied
```

`devops-restore.bat` is a cron job to restore it with git every one minute. It's given the create, update, and delete permissions.

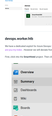
```
svn: E200009: Cannot verify lock on path '/www'
svn: E195020: Cannot lock path '/www', another working copy is holding a lock
```

Create a file `test` and run `svnlook -r 2 -t dump /var/svn/dimension | ./hook.sh -` to create the `test` file. Wait a few seconds and then `svn ls file://www` and we can see the `test` file.

```
svnadmin create test
svn ls file://test
svn import -m "test" test file://test
svn ls file://www
svn import -m "test" test file://www
svn ls file://www
svn: E200009: Cannot verify lock on path '/www'
svn: E195020: Cannot lock path '/www', another working copy is holding a lock
svnlook -r 2 -t dump /var/svn/dimension | ./hook.sh -
svn ls file://www
test
```

Azure Devops

Log in as `nathan` and we can see a project called `Smartit`. We can then create a new branch and upload a file. We can then create a pull request and approve it. Finally, we can create the `test.aspx` file and access it by running our payload from the `test.aspx` file. We can then use `Evil-WinRM` to connect as `iis apppool\defaultapppool`.


Azure DevOps
Smartit
Overview
Summary
Dashboards
Boards
Work items
Repos
Pipelines
Test Plans
Artifacts
Project settings
Smartit
About this pr
Our vision - The sh
+ Smartworkb
Tailwind T
Applicatio
We are happy to
showcasing the Sm
Tailwind Traders
through devops.
Work item to link
No work items
Attachment
No attachments
Reviewers
nathan
Approved
Tags
No tags
Complete
Abandon
Draft
Comments
Files
Updates
Commits
Checks
Policies
Work items
Discussion
Overview
Contents
History
Compare
Branches
Tags
Pushes
Contributors
Graph
master
Branch: master
Path: /www
test.aspx
nathan
Initial commit
Commit to new branch
Commit to new branch
Commit
Name
Branch name
Commit message
Extended commit description
Author
nathan
Committer
nathan
Commit to new branch
Commit
Commit to new branch
Commit
Commit to new branch
Commit