The People’s Government of Pangea

Department of Information Technology

Cyber Operations Team 15 (Wright State University)

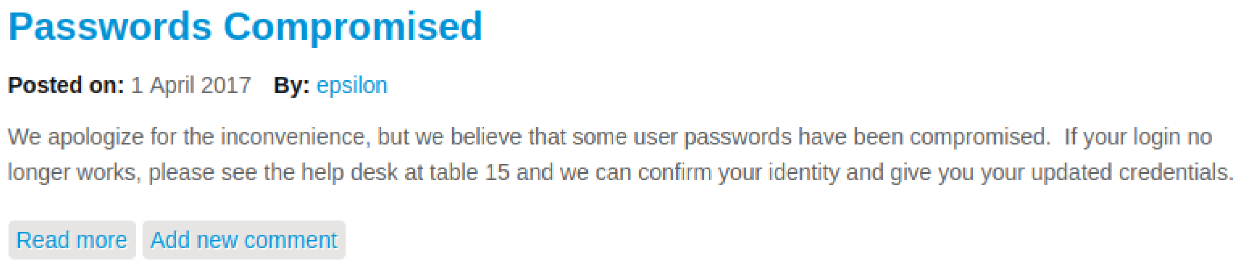
Intrusion Report

After seeing complaints from users about the fact that the file upload and download capability in Drupal was not downloading files, we looked into it and found that Drupal was displaying the contents of the text files that users were uploading in the web browser. We modified the Apache configuration to force files to be downloaded instead of viewed in the browser. We did this by forcing anything in the /filebrowser/download location on the webserver to have a content type of “application/octet-stream”:

```
<Location /filebrowser/download>
    ForceType application/octet-stream
    Header set Content-Disposition attachment
    Header set Content-Type "application/octet-stream"
</Location>
```

At 12:42 pm, the water pump shut off and the Apache logs showed an access attempt from Jane Wright (j.wright). She hadn’t been logged into the website for 53 minutes, so we suspect she may have compromised credentials. We have reset her password and made a generic blog post on the website explaining that the users can see us for new credentials (no identifying information about Jane specifically).

Because we saw recent login attempts into the website from users that should not have been active at the time, we also reset the passwords for f.castle, s.taylor, and k.holmes. They should see the same notice if they wonder why their passwords were reset.

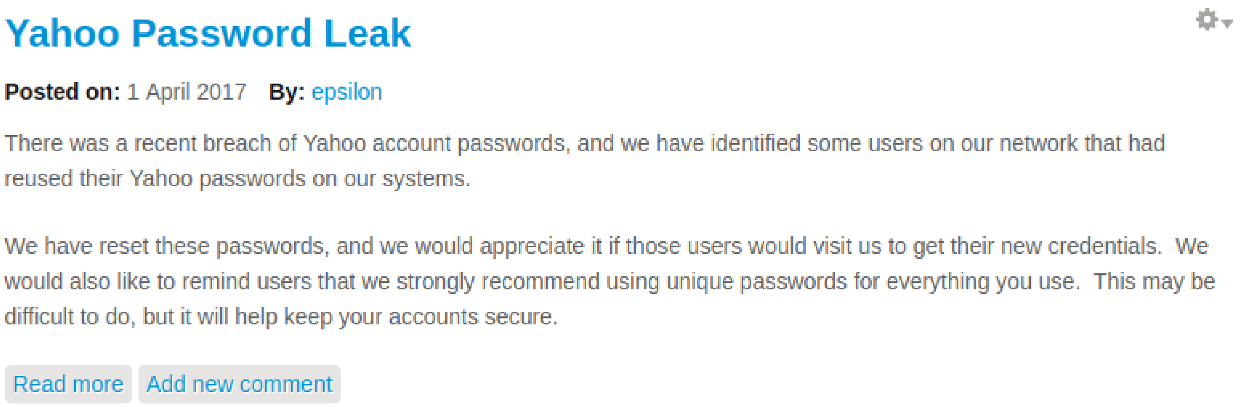


Passwords Compromised

Posted on: 1 April 2017 **By:** epsilon

We apologize for the inconvenience, but we believe that some user passwords have been compromised. If your login no longer works, please see the help desk at table 15 and we can confirm your identity and give you your updated credentials.

Shortly afterward, we received an alert that some passwords were leaked on Yahoo and we found that s.taylor was using shared credentials with his Yahoo account. Although we already reset his password, we made another post specifically for the Yahoo breach to raise awareness about password reuse and encourage s.taylor to change his Yahoo password as well:



Yahoo Password Leak

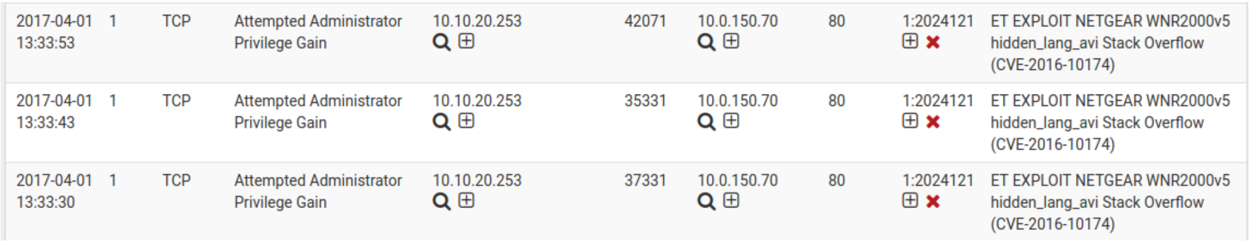
Posted on: 1 April 2017 **By:** epsilon

There was a recent breach of Yahoo account passwords, and we have identified some users on our network that had reused their Yahoo passwords on our systems.

We have reset these passwords, and we would appreciate it if those users would visit us to get their new credentials. We would also like to remind users that we strongly recommend using unique passwords for everything you use. This may be difficult to do, but it will help keep your accounts secure.

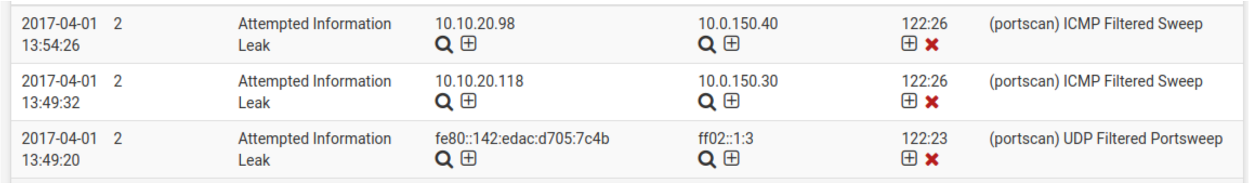
We noticed that our DNS and Files SSH services were marked as being offline from IScorE for a few minutes, but we found that they were actually online when we checked. We talked to the White Team about the incident and they said that it was likely because the Red Team was erroneously attacking the scoring server. For DNS, the request apparently timed out and there was no error message for Files SSH, so we believe that to indeed be the case. If possible, we would like for this to be considered for our score.

The attempts to exploit CVE-2016-10174 are continuing and are still occurring once about every 10 seconds:



2017-04-01 13:33:53	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253 🔍 ⊞	42071	10.0.150.70 🔍 ⊞	80	1:2024121 ⊞ ✖	ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)
2017-04-01 13:33:43	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253 🔍 ⊞	35331	10.0.150.70 🔍 ⊞	80	1:2024121 ⊞ ✖	ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)
2017-04-01 13:33:30	1	TCP	Attempted Administrator Privilege Gain	10.10.20.253 🔍 ⊞	37331	10.0.150.70 🔍 ⊞	80	1:2024121 ⊞ ✖	ET EXPLOIT NETGEAR WNR2000v5 hidden_lang_avi Stack Overflow (CVE-2016-10174)

We have disabled notifications in Snort for this particular event, as we believe the Red Team is using this to make the logs more sparse and difficult to read. After doing so, most of the traffic being picked up by Snort is simply port scans right now:



2017-04-01 13:54:26	2		Attempted Information Leak	10.10.20.98 🔍 ⊞		10.0.150.40 🔍 ⊞		122:26 ⊞ ✖	(portscan) ICMP Filtered Sweep
2017-04-01 13:49:32	2		Attempted Information Leak	10.10.20.118 🔍 ⊞		10.0.150.30 🔍 ⊞		122:26 ⊞ ✖	(portscan) ICMP Filtered Sweep
2017-04-01 13:49:20	2		Attempted Information Leak	fe80::142:edac:d705:7c4b 🔍 ⊞		ff02::1:3 🔍 ⊞		122:23 ⊞ ✖	(portscan) UDP Filtered Portsweep

We are also seeing frequent inbound emails, possibly from a spambot running on 10.10.20.236.