CSCI 345 Lab #2

Brandi Durham, Andrew Miller

The website we found, was for the company Opus One. This is a consulting and information technology firm. The company was established in 1989 and is still in business today. The sites below were all discovered using the ext:config + “password=”+” search in google. Most of the information found was from the business before it expanded and is apart of the old website for the company. While these passwords may not grant access to the company’s current networking hardware leaving old passwords, naming conventions and hashes is a potential breach in the company's security. From researching online the company Opus One (<https://opus1.com> ), which was founded by Joel Synder was later re-established in 2011 as Opus One Solutions (<https://www.opusonesolutions.com/> ). The new company is an software engineering company that consults utility companies about electricity distribution systems and better manage DERs.

1. This link had information pertaining to the type of encryption used throughout the site (MD5) which is known to be weak now. Things such as preshared keys and public ip addresses used for the company's cisco VPN.
2. This link included critical information such as hashed passwords as well as plaintext usernames and passwords, levels of privilege. Importantly this link had the root password for this equipment as well.
3. This link included information such as the admin password for this network switch, a physical location, and a private cell phone number as well as the name of the hardware owner.
4. This link included encrypted passwords for the secure connection which given enough time could theoretically be decrypted as well as more hardware default passwords.
5. This link included multiple usernames and hashed passwords that were hashed using the weak MD5 algorithm including the one for root and administrator.
6. This link for the juniper network hardware revealed many hashed passwords as well as usernames and the port. It also gave IP addresses for admin and infranet controller.
7. This page also included network access control infrastructure passwords in plaintext. This is not the only example but proves to be a monumentally bad idea in terms of security.
8. <http://www.opus1.com/vpn/cisco/cisco.config>
   1. crypto isakmp policy 200  
       encr 3des  
       hash md5  
       authentication pre-share  
       lifetime 43200  
      !  
      crypto isakmp policy 300  
      crypto isakmp key 12345678901234567890 address 45.210.50.115   
      crypto isakmp key 12345678901234567890 address 45.210.50.111   
      crypto isakmp key 12345678901234567890 address 45.210.50.102   
      crypto isakmp key 12345678901234567890 address 45.210.50.104   
      crypto isakmp key 12345678901234567890 address 45.210.50.106   
      crypto isakmp key 12345678901234567890 address 45.210.50.109   
      crypto isakmp key 12345678901234567890 address 45.210.50.113   
      crypto isakmp key 12345678901234567890 address 45.210.50.114   
      crypto isakmp key 12345678901234567890 address 45.210.50.116   
      crypto isakmp key 12345678901234567890 address 45.210.50.117   
      crypto isakmp key 12345678901234567890 address 45.210.50.118   
      crypto isakmp key 12345678901234567890 address 45.210.50.119   
      crypto isakmp key 12345678901234567890 address 45.210.50.120
9. <http://www.opus1.com/nac/ny06configs/tcg-cisco-ap.config>
   1. enable secret 5 $1$0WmC$ij4QTMBICqU85HEBF1QTK/  
      enable password 7 0208055805070C711A
   2. username Cisco password 7 011D0707550A055F77  
      username admin privilege 15 password 7 1040081A0B16115B5A  
      username administrator privilege 15 password 7 000A12050A5A085659  
      username root privilege 15 password 7 09424F0A170414425D  
      username nac privilege 15 password 7 04550A0501204F1E5F
10. <http://www.opus1.com/nac/lv08configs/force10-switch.config>
    1. enable password 7 b125455cf679b20820073e8e6eaa171c592ee28a06ac4ef8  
       !  
       username admin password 7 b6fd3505d58aa300783039e19b45cc23  
       !  
       enable restricted 7 2c99cc9784afd292
    2. snmp-server community public ro PERMIT\_SNMP\_RO  
       snmp-server contact "Greg Hankins +1 404 542 5530"  
       snmp-server enable traps snmp authentication coldstart linkdown linkup   
       snmp-server enable traps envmon fan supply temperature   
       snmp-server host 45.200.1.75 informs version 2c public udp-port 162  
       snmp-server location "On a table in a warehouse..."  
       snmp-server trap-source Vlan 1000
11. <http://www.opus1.com/nac/lv08configs/trapeze-mx8.config>
    1. set radius server radiator-proxy address 45.200.1.74 timeout 5 retransmit 3 deadtime 0 encrypted-key 04550a0501204f1e51  
       set radius server smartpass address 45.200.1.60 encrypted-key 011d0707550a055f79  
       set radius server test address 45.200.1.164 encrypted-key 011d0707550a055f79  
       set server group radiator members radiator-proxy  
       set server group smartpass-grp members smartpass  
       set server group test-grp members test  
       set radius dac test-rfc3576 address 45.200.1.164 replay-protect disable encrypted-key 09424f0a1704144253  
       set radius dac smartpass-rfc3576 address 45.200.1.60 replay-protect disable encrypted-key 09424f0a1704144253  
       set enablepass password ca3b82b92bef74a74fd06d5b7ac2a02c543f
    2. set user admin password encrypted 135143100e0916397f25243f
12. <http://www.opus1.com/nac/ny06configs/tcg-cisco.config>
    1. enable secret 5 $1$He/E$0Hfay7ggY6cWfHd8O5EUW.  
       enable password 7 09424F0A170414425D  
       !  
       username nac privilege 15 password 7 06080E22424F0A4953  
       username jms privilege 15 password 7 011D0F100F5F080E22  
       username administrator privilege 15 password 7 121704141C0A0F547C  
       username root privilege 15 password 7 0505070C2F4D4D594F  
       username cisco privilege 15 password 7 1040081A0B16115B5A
13. <http://www.opus1.com/nac/ny06configs/tcg-juniper.config>
    1. set auth radius accounting port 1646  
       set admin name "admin"  
       set admin password "nMHiJbrxIUAAc0EB4saGyDEtH+GMJn"  
       set admin manager-ip 45.0.0.0 255.0.0.0
    2. set infranet controller name "IC" host-name 45.200.1.55 port 11122  
       set infranet controller name "IC" src-interface ethernet1  
       set infranet controller name "IC" password "sN/C2bHXN660xJseJgC4rm5VTvnPJvAKGw=="  
       set infranet controller name "IC" ca-hash "806BFF671DF05583269038963F09F4829F48840B"
14. <http://www.opus1.com/nac/ny06configs/tcg-hp.config>
    1. ip authorized-managers 45.200.0.0 255.255.0.0  
       aaa authentication port-access eap-radius  
       radius-server host 45.200.1.55 key nacnac06