Collegiate Cyber Defense Competitions

Inject Name	Export Firewall Security Policy for Auditors,
Inject ID	TOOL26T

Description	Extract the current firewall's security policy configurations for analysis by an external auditor which we have hired to certify our security posture for a large customer that is important to the organization. Consider the following scripts, noted in the Reference section, for use with Palo Alto and Cisco Fire Power firewalls to accomplish this. Be sure to enable SSH and obtain CLI rights. API rights need to be enabled for Cisco.
Deliverables	Do not respond with a memo. Rather, upload the result files from the configuration extract to the Inject Scoring Engine. Follow competition guidelines for exporting data/ logs from the topology.

Reference

Palo Alto (Export text file)

```
# palo_export.py
import paramiko

FIREWALL_IP = '192.0.2.1'
USERNAME = 'admin'
PASSWORD = 'yourpassword'

def export_palo_policies():
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    client.connect(FIREWALL_IP, username=USERNAME, password=PASSWORD,
look_for_keys=False)

    stdin, stdout, stderr = client.exec_command('show running security-policy')
    output = stdout.read().decode()

    with open('palo_security_policy.txt', 'w') as f:
        f.write(output)

    client.close()
    print("Palo Alto policy exported to palo_security_policy.txt")

if __name__ == "__main__":
    export_palo_policies()
```

Description	**Cisco Fire Power (Export in JSON format)** *# fmc_export.py* *import requests* *import json* *FMC_IP = "192.0.2.10"* *USERNAME = "admin"* *PASSWORD = "yourpassword"* *def get_auth_token():* *url = f"https://{FMC_IP}/api/fmc_platform/v1/auth/generatetoken"* *response = requests.post(url, auth=(USERNAME, PASSWORD), verify=False)* *token = response.headers["X-auth-access-token"]* *domain_uuid = response.headers["DOMAIN_UUID"]* *return token, domain_uuid* *def export_fmc_policies():* *token, domain_uuid = get_auth_token()* *headers = {* *"X-auth-access-token": token,* *"Content-Type": "application/json"* *}* *url = f"https://{FMC_IP}/api/fmc_config/v1/domain/{domain_uuid}/policy/accesspolicies"* *resp = requests.get(url, headers=headers, verify=False)* *policies = resp.json()["items"]* *for policy in policies:* *policy_id = policy["id"]* *policy_name = policy["name"]* *rules_url = f"https://{FMC_IP}/api/fmc_config/v1/domain/{domain_uuid}/policy/accesspolicies/{policy_id}/accessrules?limit=1000"* *rules_resp = requests.get(rules_url, headers=headers, verify=False)* *rules = rules_resp.json()* *with open(f"fmc_policy_{policy_name}.json", "w") as f:* *json.dump(rules, f, indent=2)* *print(f"Exported policy {policy_name} to fmc_policy_{policy_name}.json")* *if __name__ == "__main__":* *requests.packages.urllib3.disable_warnings()* *export_fmc_policies()* **Requirements:** ***pip install requests***