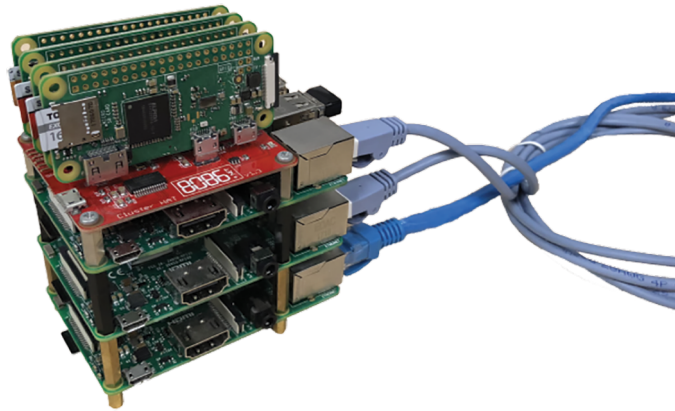


Prowler

Distributed Network Vulnerability Scanner

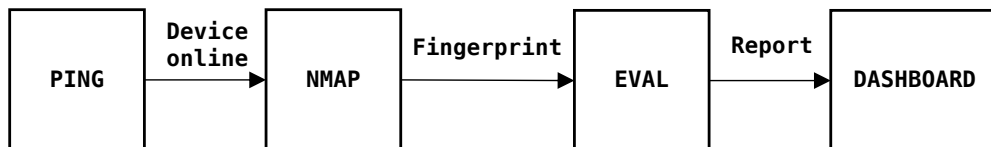
Timothy Liu
Wong Chi Seng
Faith See

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN



Often, security breaches are not due to hackers breaking through layers of tough security. They happen because someone didn't change their default passwords.

Prowler finds weakly secured devices on networks and notifies the administrator.



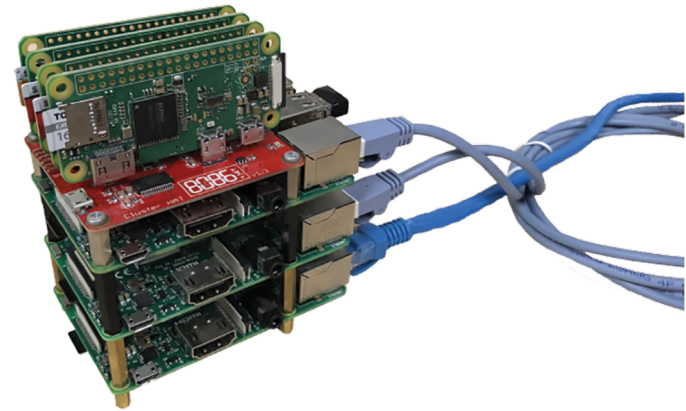
<https://tlkh.github.io/prowler>

Prowler

Distributed Network Vulnerability Scanner

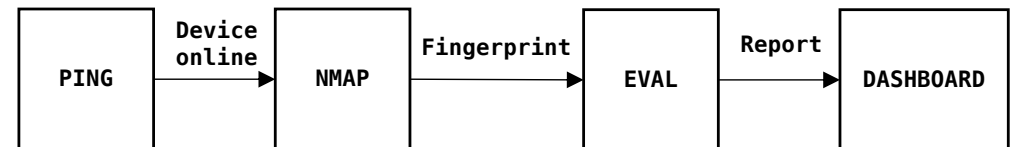
Timothy Liu
Wong Chi Seng
Faith See

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN



Often, security breaches are not due to hackers breaking through layers of tough security. They happen because someone didn't change their default passwords.

Prowler finds weakly secured devices on networks and notifies the administrator.



<https://tlkh.github.io/prowler>

PROWLER Dashboard

Dashboard / Main Network

7 SSH-enabled devices
View Details

3 VNC-enabled devices
View Details

10 devices on network
View Details

0 device with weak credentials
View Details

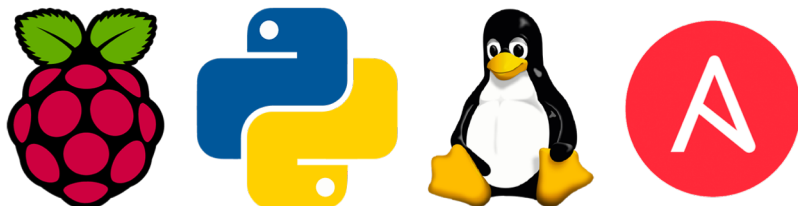
Network Devices

Show 10 entries Search:

ID	Hostname	Type	Open Ports	Status
0	192.168.0.1	general purpose: Linux, Linux(2.6.X),general purpose: Linux, Linux(3.X),media device: Linux, Linux(2.6.X),general purpose: Linux, Linux(2.6.X),media device: Linux, Linux(3.X),WAP: Linux, Linux(3.X),specialized: Linux, Linux,broadband router: Linux, Linux(3.X),WAP: Linux, Linux(2.4.X),WAP: Linux, Linux(2.4.X),WAP: Linux, Linux(2.6.X)	80/http,5500/hotline,9000/cslistener,10004/emcmircdd	false
1	192.168.0.110	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc	false
2	192.168.0.111	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
3	192.168.0.123			false
4	192.168.0.133	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc	false
5	192.168.0.142	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc,8181/intermapper	false
6	192.168.0.153	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
7	192.168.0.170	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
8	192.168.0.193			false

Capabilities

- Scan a network (a particular subnet or a list of IP addresses) for all IP addresses associated with active network devices
- Determine the type of devices using fingerprinting
- Determine if there are any open ports on the device
- Associate the ports with common services
- Test devices against a dictionary of factory default and common credentials
- Notify users of security vulnerabilities through an dashboard (above).



PROWLER Dashboard

Dashboard / Main Network

7 SSH-enabled devices
View Details

3 VNC-enabled devices
View Details

10 devices on network
View Details

0 device with weak credentials
View Details

Network Devices

Show 10 entries Search:

ID	Hostname	Type	Open Ports	Status
0	192.168.0.1	general purpose: Linux, Linux(2.6.X),general purpose: Linux, Linux(3.X),media device: Linux, Linux(2.6.X),general purpose: Linux, Linux(2.6.X),media device: Linux, Linux(3.X),WAP: Linux, Linux(3.X),specialized: Linux, Linux,broadband router: Linux, Linux(3.X),WAP: Linux, Linux(2.4.X),WAP: Linux, Linux(2.4.X),WAP: Linux, Linux(2.6.X)	80/http,5500/hotline,9000/cslistener,10004/emcmircdd	false
1	192.168.0.110	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc	false
2	192.168.0.111	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
3	192.168.0.123			false
4	192.168.0.133	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc	false
5	192.168.0.142	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh,5900/vnc,8181/intermapper	false
6	192.168.0.153	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
7	192.168.0.170	general purpose: Linux, Linux(3.X),general purpose: Linux, Linux(4.X)	22/ssh	false
8	192.168.0.193			false

Capabilities

- Scan a network (a particular subnet or a list of IP addresses) for all IP addresses associated with active network devices
- Determine the type of devices using fingerprinting
- Determine if there are any open ports on the device
- Associate the ports with common services
- Test devices against a dictionary of factory default and common credentials
- Notify users of security vulnerabilities through an dashboard (above).

