

EXPERIMENT 12:

OUTPUT:

The screenshot shows the 'Settings' page with the 'Compliance' tab selected. On the left, a sidebar lists categories: BASIC (selected), General, Permissions, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main content area displays the configuration for 'NetworkScan_policy'. The 'Name' field contains 'NetworkScan_policy' and the 'Description' field contains 'Scanning the local network'.

Settings	Credentials	Compliance	Plugins
BASIC			
General			
Permissions			
DISCOVERY			
ASSESSMENT			
REPORT			
ADVANCED			

Name: NetworkScan_policy

Description: Scanning the local network

This screenshot shows the 'Remote Host Ping' configuration. The 'Host Discovery' category is selected in the sidebar. The 'Remote Host Ping' section has a toggle switch for 'Ping the remote host', which is currently turned off.

Settings	Credentials	Compliance	Plugins
BASIC			
DISCOVERY			
Host Discovery			

Remote Host Ping

Ping the remote host ☐

The 'Local Port Enumerators' section contains five checked options:

- ☒ SSH (netstat)
- ☒ WMI (netstat)
- ☒ SNMP
- ☒ Only run network port scanners if local port enumeration failed
- ☒ Verify open TCP ports found by local port enumerators


The bottom section shows two settings for concurrent TCP sessions, both set to 'Unlimited':

- Max number of concurrent TCP sessions per host: Unlimited
- Max number of concurrent TCP sessions per scan: Unlimited




Authentication method	<input type="text" value="Password"/>
Username	<input type="text" value="administrator"/> <input type="button" value="Log In"/>
Password	<input type="password"/> <input type="button" value="Log In"/>
Domain	<input type="text"/>

Browser address bar: <https://localhost:8834/#/scans/reports/new>




Browser tabs: [Nessus Home / Scan Templ...](#)

Nessus  [Scans](#) [Settings](#)

HOLDINGS

-  My Scans
-  All Scans
-  Trash


RESOURCES

-  Policies
-  Plugin Rules
-  Scanners

Scan Templates

[Back to Scans](#)

[Scanner](#) [User Defined](#)



NetworkScan Policy
Scanning a network

Results 1 Vulnerabilities 10 History 4

Filter 1 Search results 1 result

<input type="checkbox"/>	Host	Vulnerabilities
<input type="checkbox"/>	192.168.16.101	<div><div></div></div>

Scan Details

Name: localnetwork
Status: Completed
Policy: NetworkScan_Policy
Scanner: Local Scanner
Start: August 1 at 2:29 PM
End: August 1 at 2:30 PM
Elapsed: 8 minutes

Vulnerabilities



Results 1 Vulnerabilities 10 History 4

Filter 1 Search results 10 vulnerabilities

<input type="checkbox"/>	See	Name	Family	Count	
<input type="checkbox"/>		MS11-034 Vulnerability in HTTP.sys Could Allow Remote...	Windows	2	✓
<input type="checkbox"/>		MS11-038 Vulnerability in DNS Server Could Allow Re...	Windows	1	✓
<input type="checkbox"/>		MS11-038 Vulnerability in DNS Server Could Allow Re...	DNS	1	✓
<input type="checkbox"/>		MS14-066 Vulnerability in Schannel Could Allow Remote...	Windows	1	✓
<input type="checkbox"/>		MS17-010 Security update for Microsoft Windows SMB...	Windows	1	✓
<input type="checkbox"/>		DNS Server (DC,LDAP,SNMP) Backdoor / Implant Detectio...	Windows	1	✓
<input type="checkbox"/>		Unsupported Microsoft DNS Server Detection	DNS	1	✓
<input type="checkbox"/>		Unsupported Windows OS	Windows	1	✓
<input type="checkbox"/>		MS12-028 Vulnerability in Remote Desktop Could Allo...	Windows	1	✓

Scan Details

Name: localnetwork
Status: Completed
Policy: NetworkScan_Policy
Scanner: Local Scanner
Start: August 1 at 2:29 PM
End: August 1 at 2:30 PM
Elapsed: 8 minutes

Vulnerabilities

