

```
<?xml version="1.0" encoding="UTF-8"?>
<NessusClientData_v2>
<Policy><policyName>Basic Network Scan</policyName>
<Preferences><ServerPreferences><preference>
<name>bw_prevent_core_updates</name>
<value>yes</value>
</preference>
<preference><name>scan.enable_utf8_output</name>
<value>no</value>
</preference>
<preference><name>bw_prevent_plugin_updates</name>
<value>yes</value>
</preference>
<preference><name>plugin_set</name>
<value>146991;216142;16321;15713;19939;16046;11591;11480;11592;173677;11475;
23735;10747;40613;73190;31094;11714;11187;14195;14196;18212;14241;21020;1820
8;91230;109799;109800;173712;109730;180360;209231;211725;242639;214542;23750
;31607;29749;33218;91231;18414;18415;18413;58484;26020;58321;10277;10949;107
15;14256;10973;10974;11604;17307;10975;11283;10977;10978;10979;10976;11287;1
0981;10980;10983;11288;10982;11289;14718;11292;11382;11290;11291;10984;10985
;10986;11294;11381;11293;10987;11295;11379;12039;11056;11296;11297;11285;113
80;11594;11383;11547;14337;12270;12199;16217;15782;17630;17629;20933;17988;2
0807;17635;15627;17986;24741;24736;19771;24744;20808;20134;19377;24019;24737
;24740;20744;24739;10001;10962;11393;11276;11202;10963;10961;10993;10990;109
91;10820;11032;11003;10994;10998;10999;10997;10995;10996;11000;11001;10826;1
1208;10798;10819;11004;11205;11204;11206;11207;11203;10778;11098;11833;99767
;99764;99766;99765;99770;99769;99768;99777;99773;99776;99774;99772;99771;997
75;99780;99782;99781;99784;99778;99779;99783;99786;99791;99787;99785;99789;9
9790;99788;99794;99792;99796;99797;99795;99798;99793;99801;99804;99799;99800
;99805;99802;99803;99810;99806;99808;99807;99809;99811;99812;99815;97416;998
13;99814;99816;99817;99819;99818;99820;99821;99825;99822;99823;99824;99828;9
9827;99826;99829;99831;99830;99833;99832;99834;99835;99836;99838;99837;99841
;99839;99840;99843;99842;99847;99846;99845;99844;99848;99849;99850;99855;998
54;99852;99853;99851;99856;99860;99858;99857;99859;99863;99861;99862;99867;9
9865;99864;99870;99866;99868;99869;99871;99873;99872;99876;99875;99874;99877
;99882;99880;99878;99881;99883;99879;99884;99885;99888;99887;99886;99890;998
91;99889;99893;99892;99897;99898;99894;99895;99896;99902;99899;99900;99901;9
9905;99904;99903;99908;99909;99910;99911;99913;99914;99912;99915;99916;99936
;99937;99938;99939;99940;99941;99945;99942;99943;99946;99944;99947;99948;999
50;99949;99953;99952;99951;100683;100684;100685;100686;100687;100688;100812;
```

100811;100689;100690;100691;100695;100692;100694;100693;100696;100697;100698;
100700;100699;100702;100701;100813;100722;100814;101849;101848;101306;100723;
101307;101850;101851;101852;101309;101853;101308;101310;101854;101311;101855;
101312;101313;101314;101315;102221;102479;102222;102480;102223;102224;102226;
102225;102229;102228;102227;102231;102230;102235;102236;102238;102233;102237;
102232;102234;102240;102241;102242;102244;102243;102245;102239;102999;102998;
102997;103000;103001;103002;103003;103005;103006;103004;103008;103007;
103009;103010;103011;103012;103013;103014;103015;103017;103018;103016;103019;
103020;103021;103022;103023;103024;103025;103026;103027;103028;103029;103031;
103030;103033;103032;103034;103055;103057;103056;103058;103059;103060;103061;
103062;103063;103065;103064;103066;103069;103068;103067;103070;103071;103072;
103074;103075;103073;103076;103078;103077;103080;103082;103081;103079;103084;
103083;103085;103088;103087;103733;103086;103734;103735;103737;103736;103738;
103739;103740;104576;103821;103820;104577;103878;103879;104578;103937;
103938;103939;103941;103940;103942;104277;104278;104279;104280;104281;104282;
104283;104284;104285;104289;104288;104287;104286;104290;104291;104292;104296;
104295;104293;104294;104327;104325;104326;104329;104330;104331;104328;10432;
104333;104463;104334;104904;104903;104902;104906;104905;104907;104911;104909;
104910;104908;104912;104913;105164;104914;104915;104917;104919;104916;104918;
104920;104922;104921;104923;104924;104926;104925;104929;104927;104930;104928;
104932;104933;104931;104934;105046;104935;105301;105302;105047;105303;
105304;105306;105305;105308;105309;105307;105310;105312;105311;105313;105315;
105314;105317;105316;105318;105319;105320;105323;105321;105322;105618;105655;
106144;106145;106147;106146;106149;106148;106150;106151;106156;106154;106153;
106152;106155;106157;106159;106160;106158;106161;106162;106163;106165;106166;
106164;106167;106402;106404;106403;106406;106405;106760;106761;106762;106763;
106764;106765;106767;106766;106768;106769;106773;106770;106775;106772;106771;
106774;106777;108455;108457;106776;106778;108456;108458;108460;108459;
108463;108462;108461;108464;108469;108465;108468;108467;108466;108470;108472;
108471;108474;108473;108475;109470;109472;109471;109475;109474;109476;109473;
109478;109477;109481;109479;109480;109482;109484;109483;109486;109488;109487;
109485;109491;109490;109493;109492;109489;109499;109495;109496;109497;109498;
109500;109494;109505;109501;109504;109502;109503;109506;109507;73189;109512;
109511;109508;109510;109513;109509;109514;109515;109620;109813;110126;109619;
110127;109516;110128;110129;110136;110131;110135;110137;110130;110133;110132;
110134;110140;110138;110139;110141;110143;110142;110144;110145;110146;
110151;110147;110152;110149;110148;110150;110153;110733;110617;110731;110732;
110730;110154;110156;110155;110735;110736;110737;110739;110734;110738;110740;
110741;110742;110743;110745;110747;110746;110744;110825;110748;110828;110841;
110842;110826;110827;110843;110844;110845;110847;110846;110849;110848;110840;

850;110851;110853;110852;110854;110855;110858;110857;110856;110861;110859;110860;110863;110862;110864;110865;110866;110868;110867;110869;110872;110870;110871;110874;110873;110876;110875;110878;110880;110879;110881;110877;110882;110883;111182;111183;111184;111643;111646;111645;111644;111647;117540;111649;111648;111650;117542;117541;117543;117544;117547;117545;117550;117549;117548;117546;117551;117552;117555;117557;117554;117558;117556;117553;117559;117561;117562;117563;117560;117564;117565;117566;117568;117567;117570;117569;117571;117573;117572;117575;117574;117576;117581;117580;117577;117578;117579;117582;117583;117585;117430;117584;112237;112238;117586;117726;117725;117728;117729;117730;117727;117731;117732;117734;117733;117737;117736;117738;117735;117742;117741;117739;117740;117744;117745;117743;118049;117746;117747;117748;117749;117750;117752;117751;117753;117754;117756;117759;117755;117760;117761;117757;117758;117763;117762;118411;118412;118367;118366;118413;118415;118414;118418;118419;118420;118416;118417;118421;118422;118423;118424;118425;118427;118426;118428;118430;118429;118431;118433;118432;118434;118435;118439;118438;118436;118437;118440;118736;118739;118740;118737;118741;118738;118743;118742;118756;118757;118755;118758;118759;118760;119059;119060;119061;118761;119062;119063;119064;119065;119069;119066;119067;119068;119070;119072;119071;119073;119513;119564;119074;119515;119514;119516;119517;119518;119519;119520;119521;119523;119522;119526;119525;119527;119524;119530;119528;119531;119529;119533;119565;119532;119897;119896;119899;119900;119898;119903;119901;119902;119904;119906;119907;119905;119909;119911;119910;119908;119913;119912;119914;119916;119918;119919;119915;119920;119917;119921;119922;119923;119924;119927;119926;119925;119932;119928;119933;119929;119931;119930;119935;119934;120974;119936;120990;120991;120993;120992;120997;120995;120994;120996;120999;120998;121002;121000;121001;121275;121277;121276;122166;121278;122167;122169;122168;122171;122172;122170;122174;122201;122173;122202;122203;122206;122204;122205;122208;122207;122210;122209;122211;122213;122212;122214;122215;122217;122216;122218;122373;122375;122374;122376;122380;122377;122378;122379;122383;122382;122381;122386;122385;122384;122414;122387;122388;122687;122459;122693;122691;122688;122689;122690;122694;122692;122695;122696;122697;122698;122699;122770;122700;122701;122704;122703;122702;122707;122706;122705;122708;123102;122709;122710;123105;123103;123110;123109;123106;123104;123107;123108;123114;123113;123111;123112;123116;123115;123117;123118;123120;123119;12383;123121;123584;123588;123585;123586;123589;123587;123593;123590;123591;123596;123592;123595;123594;123597;123598;123599;123601;123600;123603;123602;123604;123605;123606;123608;123607;123609;123610;123612;123611;123613;123614;123615;123618;123616;123617;123619;123620;123621;123624;123623;123622;123625;123626;123628;123843;123627;123630;123629;123844;123845;123846;123850;123848;123847;123851;123852;123849;123853;123857;123854;123856;123860;123855;12385

25521;125528;125525;125527;125530;125526;125557;125529;125556;125558;125563;125559;125562;125561;125560;125564;125566;125570;125567;125565;125568;125572;125571;125569;125573;125575;125574;125576;125578;125582;125580;125579;12557;125583;125581;125584;125753;125586;125587;125585;125752;125588;126266;12668;126267;126272;126271;126269;126273;126270;126274;126275;126280;126276;126278;126279;126281;126277;126286;126283;126288;126282;126287;126284;126285;126289;126291;126290;126296;126295;126292;126293;126294;126298;126299;126415;126297;126416;126417;126418;126419;126421;126422;126420;126425;126424;126423;126929;126429;126428;126427;126426;126431;126430;126433;126432;126536;126535;126537;126538;126541;126540;126539;126542;126543;126544;126549;126548;126545;126547;126546;126550;126552;126551;126555;126553;126844;126554;126556;12643;126845;126846;126850;126849;126848;126851;126847;126852;126853;126856;126855;126930;126857;126854;126859;126858;126862;126861;126860;126863;126864;126865;126868;126869;126867;126866;126870;126871;126872;126875;126876;126877;126874;126873;126881;126932;126879;

You see the first 12 KB above and the last 18 KB below. The remaining 2 MB (98%) of the file are not displayed.

```
p" severity="0" pluginID="14272" pluginName="Netstat Portscanner (SSH)"  
pluginFamily="Port scanners">  
<agent>unix</agent>  
<description>Nessus was able to run &apos;netstat&apos; on the remote host  
to enumerate the open ports. If &apos;netstat&apos; is not available, the  
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that
the target being scanned is localhost.</description>
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also><https://en.wikipedia.org/wiki/Netstat></see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>

```
<plugin_output>Port 67/udp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="139" svc_name="netbios-ssn?" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 139/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="57621" svc_name="unknown" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
```

```
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 57621/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49784" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49784/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49674" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
```

to enumerate the open ports. If 'netstat', is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49674/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49671" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
```

```
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49671/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49668" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49668/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49665" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
```

```
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49665/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="49664" svc_name="dce-rpc" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 49664/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="8834" svc_name="www" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
```

to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 8834/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="7680" svc_name="unknown" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
```

```
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 7680/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="7070" svc_name="arcp?" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 7070/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="5040" svc_name="unknown" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
```

```
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 5040/tcp was found to be open</plugin_output>
</ReportItem>

<ReportItem port="2638" svc_name="sybaseanywhere?" protocol="tcp"
severity="0" pluginID="14272" pluginName="Netstat Portscanner (SSH)"
pluginFamily="Port scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 2638/tcp was found to be open</plugin_output>
</ReportItem>

<ReportItem port="445" svc_name="cifs" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
```

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 445/tcp was found to be open</plugin_output>
</ReportItem>
<ReportItem port="135" svc_name="epmap" protocol="tcp" severity="0"
pluginID="14272" pluginName="Netstat Portscanner (SSH)" pluginFamily="Port
scanners">
<agent>unix</agent>
<description>Nessus was able to run &apos;netstat&apos; on the remote host
to enumerate the open ports. If &apos;netstat&apos; is not available, the
plugin will attempt to use &apos;ss&apos;.
```

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.</description>

```
<fname>netstat_portscan.nasl</fname>
<plugin_modification_date>2025/05/27</plugin_modification_date>
<plugin_name>Netstat Portscanner (SSH)</plugin_name>
<plugin_publication_date>2004/08/15</plugin_publication_date>
<plugin_type>local</plugin_type>
<risk_factor>None</risk_factor>
<script_version>1.110</script_version>
<see_also>https://en.wikipedia.org/wiki/Netstat</see_also>
<solution>n/a</solution>
```

```
<solution>n/a</solution>
<synopsis>Remote open ports can be enumerated via SSH.</synopsis>
<plugin_output>Port 135/tcp was found to be open</plugin_output>
</ReportItem>
</ReportHost>
</Report>
</NessusClientData_v2>
```

Show the full file...