Scan Report

September 29, 2013

Summary

This document reports on the results of an automatic security scan. The scan started at Sun Sep 29 01:34:37 2013 UTC and ended at Sun Sep 29 01:38:32 2013 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	Most Severe Result(s)	High	Medium	Low	Log	False Positives
120.115.20.1 (dns.htps.tn.edu.tw)	Severity: Medium	0	1	1	13	0
Total: 1		0	1	1	13	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.

This report contains all 15 results selected by the filtering described above. Before filtering there were 15 results.

2 Results per Host

2.1 120.115.20.1

Host scan start	Sun Sep 29 01:34:40 2013 UTC
Host scan end	Sun Sep 29 01:38:32 2013 UTC

Service (Port)	Threat Level
domain (53/tcp)	Medium
domain (53/udp)	Low
domain (53/udp)	Log
general/CPE-T	Log
general/HOST-T	Log
general/tcp	Log
ssh (22/tcp)	Log

2.1.1 Medium domain (53/tcp)

Medium (CVSS: 5.0)
NVT: DNS Amplification Attacks

```
 Summary:
 A misconfigured Domain Name System (DNS) server can be exploited to participate
in a Distributed Denial of Service (DDoS) attack.
A Domain Name Server (DNS) Amplification attack is a popular form of
Distributed Denial of Service (DDoS) that relies on the use of publically
accessible open recursive DNS servers to overwhelm a victim system with DNS
```

... continues on next page ...

... continued from previous page ...

response traffic.
The basic attack technique consists of an attacker sending a DNS name lookup request to an open recursive DNS server with the source address spoofed to be the victim's address. When the DNS server sends the DNS record response, it is sent instead to the victim. Attackers will typically submit a request for as much zone information as possible to maximize the amplification effect. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. By leveraging a botnet to perform additional spoofed DNS queries, an attacker can produce an overwhelming amount of traffic with little effort. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks.
We send a DNS request of 17 bytes and received a response of 244 bytes.

OID of test routine: 1.3.6.1.4.1.25623.1.0.103718

References
CVE: CVE-2006-0987
Other:
URL:http://www.us-cert.gov/ncas/alerts/TA13-088A
URL:http://www.isotf.org/news/DNS-Amplification-Attacks.pdf
URL:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-0987

[return to 120.115.20.1]

2.1.2 Low domain (53/udp)

Low (CVSS: 5.0)
NVT: Determine which version of BIND name daemon is running

BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.
The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information. The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.
The remote bind version is : 9.8.1-P1
Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.

OID of test routine: 1.3.6.1.4.1.25623.1.0.10028

[return to 120.115.20.1]

2.1.3 Log domain (53/udp)

Log (CVSS: 0.0)
NVT: DNS Server Detection

```
 Summary:
 A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it
possible for a user to access a website by typing in the domain name instead of
the website's actual IP address.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100069

[return to 120.115.20.1]

2.1.4 Log general/CPE-T

Log (CVSS: 0.0)
NVT: CPE Inventory

```
120.115.20.1|cpe:/a:openbsd:openssh:5.9p1
120.115.20.1|cpe:/o:canonical:ubuntu_linux
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810002

[return to 120.115.20.1]

2.1.5 Log general/HOST-T

Log (CVSS: 0.0)
NVT: Host Summary

```
traceroute:10.0.2.15,10.0.2.2,120.115.20.1
TCP ports:
UDP ports:
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.810003

[return to 120.115.20.1]

2.1.6 Log general/tcp

Log (CVSS: 0.0)
NVT: Ping Host

```
Nmap was selected for host discovery but is not present on this system.
Falling back to build in discovery method.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.100315

Log (CVSS: 0.0)
NVT: OS fingerprinting

```
ICMP based OS fingerprint results: (80% confidence)
HP JetDirect
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.102002

Log (CVSS: 0.0)
NVT: DIRB (NASL wrapper)

```
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.103079

Log (CVSS: 0.0)
NVT: Checks for open udp ports

```
Open UDP ports: [None found]
```

. . . continues on next page . . .

... continued from previous page ...

OID of test routine: 1.3.6.1.4.1.25623.1.0.103978

Log (CVSS: 0.0)
NVT: arachni (NASL wrapper)

```
Arachni could not be found in your system path.
OpenVAS was unable to execute Arachni and to perform the scan you
requested.
Please make sure that Arachni is installed and that arachni is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.110001

Log (CVSS: 0.0)
NVT: Nikto (NASL wrapper)

```
Nikto could not be found in your system path.
OpenVAS was unable to execute Nikto and to perform the scan you
requested.
Please make sure that Nikto is installed and that nikto.pl or nikto is
available in the PATH variable defined for your environment.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.14260

Log (CVSS: 0.0)
NVT: Traceroute

```
Here is the route from 10.0.2.15 to 120.115.20.1:
10.0.2.15
10.0.2.2
120.115.20.1
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.51662

Log (CVSS: 0.0)
NVT: SSH Authorization Check

... continues on next page ...

... continued from previous page ...

```
No port for an ssh connect was found open.
Hence authenticated checks are not enabled.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.90022

Log (CVSS: 0.0)
NVT: Checks for open tcp ports

```
Open TCP ports: [None found]
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.900239

[return to 120.115.20.1]

2.1.7 Log ssh (22/tcp)

Log (CVSS: 0.0)
NVT: SSH Server type and version

```
Detected SSH server version: SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
Remote SSH supported authentication: (not available)
Remote SSH banner:
(not available)
CPE: cpe:/a:openbsd:openssh:5.9p1
Concluded from remote connection attempt with credentials:
  Login: OpenVAS
  Password: OpenVAS
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10267

[return to 120.115.20.1]