{REDACTED} Security Assessment Checklist Appendix A – External Scan Report

Prepared for {CLIENT} {CLIENT} by Sean Cooper for {REDACTED}

Table of Contents

Revision Control Log

Date	Old Version #	New Version #	Revised By:	Description
2014-09-24	0.0	0.1	Sean Cooper	Initial Document Composition
2014-09-25	0.1	1.0	Sean Cooper	Initial Document Delivery

Introduction

{REDACTED} ({REDACTED}) was retained by {CLIENT} {CLIENT} to perform a network security audit after a third-party vendor (TPV) indicated that {CLIENT} {CLIENT} may have had a security incident that resulted in the disclosure of customer data to an unknown party. As part of the remedy for this security incident, {REDACTED} performed a network scan and audit of the {CLIENT} {CLIENT} network. This artifact contains those results along with an interpretation and recommendation section.

Scope

The scope of this network security audit is such that the following systems were analyzed:

- Perimeter defenses, including network firewalls
- Internal defenses, including host-based security systems (HBSS)
- Service configurations of infrastructure components that provide network services
- Workstation logging and event capture
- TPV service interface configuration, with regards to encryption
- Internal network traffic analysis

This analysis also includes an interpretation section as well as a recommendations section, to better align the {CLIENT} {CLIENT} network with modern security best-practices.

Limitations

This analysis does not include specific implementation instructions, as it is up to the client to decide if the TCO of suggested vulnerability mitigations outweighs the risk of the potential security threats to the {CLIENT} {CLIENT} network. Should {CLIENT} {CLIENT} wish to engage {REDACTED} in an engagement extension to develop specific implementation instructions, those implementation instructions will be provided under separate cover.

The analysis does not include an enterprise-wide survey or analysis, as efforts to investigate and remediate any potential threats or vulnerabilities were focused on network-based vulnerabilities, as instructed by the {REDACTED} Security Assessment Checklist.

Scan Results

PING Scan

```
Scanning {CLIENT} [7 ports]
Completed Ping Scan at 10:09, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:09
Completed Parallel DNS resolution of 1 host. at 10:09, 0.00s elapsed
```

TCP Scan

```
Scanning {CLIENT} ({CLIENT}) [1000 ports]
Discovered open port 554/tcp on {CLIENT}
Discovered open port 80/tcp on {CLIENT}
Discovered open port 22/tcp on {CLIENT}
Discovered open port 443/tcp on {CLIENT}
Discovered open port 21/tcp on {CLIENT}
Discovered open port 7070/tcp on {CLIENT}
Completed SYN Stealth Scan at 10:10, 32.63s elapsed (1000 total ports)
```

UDP Scan

```
Scanning {CLIENT} ({CLIENT}) [1000 ports]
UDP Scan Timing: About 2.05% done; ETC: 10:35 (0:24:41 remaining)
UDP Scan Timing: About 9.95% done; ETC: 10:35 (0:23:23 remaining)
UDP Scan Timing: About 12.55% done; ETC: 10:34 (0:21:29 remaining)
UDP Scan Timing: About 17.30% done; ETC: 10:33 (0:19:41 remaining)
UDP Scan Timing: About 20.55% done; ETC: 10:33 (0:18:26 remaining)
UDP Scan Timing: About 26.40% done; ETC: 10:33 (0:17:12 remaining)
UDP Scan Timing: About 32.50% done; ETC: 10:33 (0:15:57 remaining)
UDP Scan Timing: About 37.95% done; ETC: 10:33 (0:14:18 remaining)
UDP Scan Timing: About 41.80% done; ETC: 10:32 (0:13:07 remaining)
UDP Scan Timing: About 46.30% done; ETC: 10:31 (0:11:45 remaining)
Discovered open port 500/udp on {CLIENT}
UDP Scan Timing: About 52.75% done; ETC: 10:32 (0:10:39 remaining)
UDP Scan Timing: About 58.90% done; ETC: 10:33 (0:09:30 remaining)
UDP Scan Timing: About 66.05% done; ETC: 10:31 (0:07:16 remaining)
UDP Scan Timing: About 71.55% done; ETC: 10:31 (0:06:07 remaining)
UDP Scan Timing: About 85.10% done; ETC: 10:28 (0:02:47 remaining)
UDP Scan Timing: About 90.40% done; ETC: 10:29 (0:01:50 remaining)
Completed UDP Scan at 10:28, 1102.83s elapsed (1000 total ports)
```

HTTP XSSED Scan:

```
|_http-xssed: No previously reported XSS vuln.
| ssl-cert: Subject: commonName={CLIENT}/organizationName=HTTPS Management
Certificate for SonicWALL (self-
signed)/stateOrProvinceName=California/countryName=US
| Issuer: commonName={CLIENT}/organizationName=HTTPS Management Certificate for
SonicWALL (self-signed)/stateOrProvinceName=California/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 1970-01-01T00:00:01+00:00
| Not valid after:  2038-01-19T03:14:07+00:00
| MD5:   9673 563d 1079 1ede 6346 97e9 63f6 53b1
|_SHA-1: 6c50 2741 5979 32da 8091 c5f1 38ac a35c 8518 b4ca
|_ssl-date: 2014-09-24T15:28:45+00:00; -2s from local time.
```

Interpretation

Utilizing network scanning done on a remote site with knowledge of the {CLIENT} {CLIENT} network gathered from an on-site visit, an analysis of the network strengths and weaknesses is as follows.

Strengths

The {CLIENT} {CLIENT} network administrator has done his due diligence in securing this network. Significant effort has been expended to successfully de-activate un-needed services along the perimeter firewall, providing for a much-reduced surface for attack.

Network Address Translation was being used to provide one-to-many Internet connectivity, as well as provide a firewalling mechanism for the Intranet zone.

Weaknesses

Internal defenses are moderate, with some area for improvement.

There was no indicated policy document with regards to a configuration management plan or change control plan for the network edge devices. Changes were made during the information-gathering stages of the analysis that should have been vetted by a change control board or similar entity.

There was minimal internal segregation of network traffic observed between different functional zones, mostly consisting of a WAN/LAN/WLAN firewall zoning consistent with a NAT-based firewall.

There were no observed IDS/IPS in-line with the Internet-facing network link. Such a capability could identify suspicious network traffic and prevent it from propagating across the network link.

There was moderate installation of extraneous software packages on the user workstations, such as Spotify, Apple Bonjour, and others.

Specific Threats & Vulnerabilities

During the externally-facing network scan, it was discovered that the self-signed SSL certificate used on the SonicWALL firewall appliance was leaking information about the internal IP address schema, along with information about itself that could be used to tailor a more successful attack at the device.

It was also discovered that several unencrypted services were available as inbound destination ports on the firewall appliance. These ports are TCP ports 21, 80, 554, and 7070. More information was requested from the network administrator about the need for those specific ports to be open.

Recommendations

It is recommended that the following remediation be implemented to increase the security profile of the {CLIENT} {CLIENT} network, which will have the effect of making compromise of the network from an outside entity much less likely.

Infrastructure

Compartmentalization of the workstations, servers, appliances and utility machines would enhance the security of the network by restricting data flow between the network segments to authorized traffic. Unauthorized traffic would be blocked by the firewall device. The suggested network topology would be a 3-tiered network to segregate Internet, DMZ and Intranet traffic into their respective zones.

Firewall

Configuration of the firewall to block all inbound services would be the most secure, but may be impractical based on the needs of the business. If a "DENY ALL" policy isn't feasible for business needs, an Acceptance of Risk (AoR) might need to be done to inform management of the risk of continuing to allow those ports and services to be accessible.

Configuration of the firewall device to utilize a VLAN-type network segregation would increase the security of the {CLIENT} {CLIENT} network by disallowing unauthorized traffic between the different VLAN segments. It could also increase the performance of the network by restricting broadcast traffic to specific sets of machines.

Configuration of the firewall appliance to utilize an inbound white-list mechanism would also increase the security of the network perimeter defenses by only allowing authorized traffic from authorized Internet hosts (such as ImageSilo, Vision, etc.).

Workstations

Workstation security was suitable for the risk factors encountered, but could be increased by the use of website white-listing, website filtering technology (which was installed but not enabled on the desktops), or through the use of an inline website sanitization filter such as WebSense or BlueCoat.

Signatory Page

I attest that I conducted the network vulnerability assessment as indicated in this report, and that any and all data relevant to the assessment has been included in this report.

Any and all statements made are true to the limits of my knowledge.

So sworn this 25th day of September, 2014.

_____

//S// Sean C. Cooper, CISSP