SAMPLE CLIENT

Cybersecurity Risk Assessment Test (CRAT) Summary

CONFIDENTIAL

JULY 2016

Prepared By:

Patriot Techcorp, Inc.
2215–B Renaissance Drive
Las Vegas, NV 89119
www.patriottechcorp.com

Executive Summary

Patriot Techcorp custom tailors the Cybersecurity Risk Assessment Test Summary to address each client's specifics but will generally resemble the following outline.

Testing Process and Procedures

Please note that to avoid the risk of bringing down services during the actual scanning process of the client's systems and network, Patriot Techcorp uses a **Non-destructive** series of attacks that relies on banners rather than exploiting real flaws to determine if vulnerabilities are present.

Patriot Techcorp, Inc. (Patriot) performs Cybersecurity Risk Assessment Testing as the primary means to evaluate overall system and network security. The tools, methods, and techniques employed by Patriot to perform these tests are generally well known throughout both the computer security and "hacker" communities. Vulnerabilities or configuration liabilities discovered as a result of these tests can be viewed as those that any intruder may find while testing the network and connected systems. Tests were conducted over the Internet to determine if external network security controls (firewalls, servers, routers, etc.) are effective in preventing unwanted external intrusion. All Internet tests were accomplished from the perspective of an outsider [1] trying to gain unauthorized access.

1 An outsider is someone who has no authorized access to the data or systems to which they wish to login. These are the persons commonly referred to as "hackers" as their goal is to gain inside access by utilizing some form of security override.

Cybersecurity Risk Assessment Test

Network Layer Attacks

An entire class of attacks is directed at circumventing any distinction between the inside and outside of the network as might be defined by a firewall, screening router, or other device. Before attempting to penetrate individual services, attempts are made to confuse the networking implementation to give more access than authorized by policy:

Sequence Number Prediction: By spoofing the source address and attempting to predict the TCP sequence number (which a firewall will send in reply to our spoofed packet) a full TCP connection can be started from a putative address. If successful, the firewall will pass packets from the false address to the inside of the firewall. Another possible attack is if the firewall believes the incoming packet's address is from the inside even though it's being received from an external daemon.

ICMP Bombing: By sending an ICMP host unreachable (or net unreachable) packets to a specific host, service can be denied to specific internal connections. Most systems will blindly accept a "host unreachable" message from any system and instantly terminate every connection to the host reference in the ICMP message.

Source Routing: By spoofing the source address and adding a "source route" entry into the IP packet, it is usually possible to contact a target, make it believe the packet came from the spoofed source computer, but still send its responses back to the source routing computer. Common attacks have the source routing computer be the attacking system so that replies to the attacks are sent directly back to the intruder.

***Routing Information Protocol (RIP)*:** By sending RIP messages, it is possible to change a host's routine tables.

ARP Cache Problems: By sending gratuitous ARP replies, it's possible to change the physical address to IP address mapping of a system.

"Sniffing" or Network Monitoring: By monitoring all traffic on a network, its possible to record users' passwords as they type them to login to a system.

TCP Hijacking: By monitoring and inserting packets into a network, it is possible to steal a connection from users who have already authenticated themselves.

IP Fragmentation Overwriting: Because IP can be fragmented to travel over networks with smaller packet sizes, it's often the case where a packet is split up into several pieces and reassembled on the destination host. Many firewalls make decisions about whether data should be allowed to pass based upon whether or not the TCP "SYN" bit is set with no TCP "ACK" bit. If a "SYN"-only packet is received, it indicates a new connection is being established from the outside of the firewall. On the other hand, if a "SYN"/"ACK" packet is received it means a host internal to the firewall is attempting to start a connection. Filter rules based upon these bits is often important if you wish to allow outgoing connections, but not incoming ones. According to the Internet RFC', the first fragmented packet of a TCP/IP connection must be large enough to include the TCP flags. As a result, firewalls may filter on the first packet alone. Unfortunately, it is possible that if the IP packet is fragmented, the first fragment contains the "SYN"/"ACK" flags, and the second contains data which overwrites the original's TCP flags with a simple "SYN". Because the firewall is filtering out the first case, the second packet is ignored. However, on the destination host, when the packet is reassembled, it appears as a "SYN" only packet, thus starting a new connection.

Flooding TCP Service Queues: TCP is a stateful protocol. The first packet, (a "SYN") forces the receiver into "SYN RECVD" state, whereby it responds with a "SYN"/"ACK" packet. The receiver then waits for a long period of time (30-60 seconds) for the original sender to respond to the "SYN"/"ACK" packet. If the original sender never responds, the receiver closes the connection and returns to the "LISTEN" state. The problem here is that many systems only allow a finite number of "SYN RECVD" connections. If any packets are received after that number is reached, they are simply dropped off. As a result, specific protocols can be turned off by anyone.

Service Layer Attacks

Another class of attacks is directed at defeating individual services offered by a system on the network. If a service can be convinced to pass data to the inside, accept dangerous commands, or have its access controls otherwise circumvented, internal machines are vulnerable to attack.

Sendmail: Sendmail is probably the most historically unsecured service with many ways to exploit older versions of this program.

Finger Buffers*:* Some finger daemon implementations have a bug in which sending too much data will overflow the input buffer resulting in data being placed directly on the stack. It then is relatively trivial to force the finger daemon to directly execute the instructions that were forced on the stack. In this way, a machine running a buggy finger daemon can be forced to execute arbitrary instructions. This is one of the attacks used by the Morris/Internet Worm about five years ago.

HTTPD Buffers: Programmers tend not to learn by their mistakes. The most common version of the HTTP daemon had the exact same bug as the finger daemon once had. Input lengths were not appropriately truncated. Consequently, the HTTP daemon would execute arbitrary instructions.

NFS/Mountd: The NFS and Mount daemons are fraught with security holes. We attempt to exploit many of then, including file handle guessing, export field length overflows, and uid mapping bugs.

Portmapper Indirect Calls: The default portmapper shipped with many UNIX systems will forward requests to service daemons directly to increase efficiency. Unfortunately, many of these service daemons trust the machine they are running on. As a result, when the portmapper forwards the service request, it appears to the daemon that the request is coming from localhost and grants access.

TFTP: Although useful, this protocol has many possible security vulnerabilities.

Anonymous FTP Directory Ownership: Many configuration manuals suggest making the anonymous FTP directory owned by the user 'ftp". However, if the directory is owned by FTP, the anonymous FTP user could insert a file under any name into the FTP user's home directory. This file could be ".rhosts", "login", or even a .plan linked to the/etc/ passwd file so when the ftp user is fingered the password file is displayed. In addition to adding administrative files new binaries could be uploaded to replace standard ones such as uploading a shell to replace ~ftp/bin/ls.

Real Passwords in the Anonymous FTP passwd File: When configuring an anonymous FTP directory, many configuration manuals have the user simply copy the real password file into the anonymous FTP directory structure. This allows any anonymous user to retrieve the real passwd file and run a cracking program on it.

NNTP: Many of the newer NNTP servers simply pass control messages to the mail program or to the shell. A malicious user can insert mail (or shell) escape sequences into forged control messages, causing the server to execute arbitrary instructions.

FTP Service: The FTP protocol is complex in that it must accept incoming connections, as well as initiate outgoing connections to carry transmitted data. As a result of the complexity, the FTP protocol is difficult to secure.

Xwindows Proxy: If internal hosts are allowed to start clients on remote machines, the access control granted to the remote machine must be carefully monitored. Several commonly available programs allow the remote host to monitor (and even insert data) an internal host that has started a client.

Fingerback: Many Host systems implement a finger back trap to catch suspicious users in the act. When a suspicious action is detected, the host will automatically finger the remote machine. Several problems result from this -- the data which is saved from the remote machine may not have a length limit, resulting in the remote user sending infinite data streams back to the host; or the remote host may finger back to the firewall, which could cause an infinite loop as the firewall fingers back.

External DNS Zone Xfers: Retrieve internal DNS from the outside.

FTP "site exec sh-c id": A recent version of the FTP daemon allows specific commands to be executed. However, many daemons are not very careful about which commands the user specifies.

Project Overview

This summary has been prepared after performing a series of Cybersecurity Risk Assessment Tests on the existing network controls, including the firewall and routers for SAMPLE CLIENT.

The objective of the CRAT is to measure the exposure of the network resources and online services to attacks from the Internet, and evaluate the effectiveness of the network controls, including firewalls, routers, and servers, in order to prevent such attacks.

This summary has been prepared and arranged in a format that is easily read and understood.

It will demonstrate and outline the technical aspects of the aforementioned as well as provide information on particular risk factors associated with identified issues of concern.

Furthermore, it will provide insight as to possible violations that may occur as a result of specific vulnerabilities along with a source for possible solutions to correct the problems, in order to facilitate a smoother and more secure flow of operation.

Network Vulnerability Assessment Summary

Report Description

This report summarizes the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Vulnerabilities are classified as serious or high, medium or low. Serious or high risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploration of higher risk vulnerabilities. Low risk vulnerabilities are those that provide access to sensitive, yet non-lethal, network data.

!!!!!! THERE ARE CURRENT VULNERABILITIES PRESENT AS OF JULY 2016 TESTING THAT REQUIRE ATTENTION !!!!!

Summary of Open Ports and Risk Factor Levels **(Details on following pages)**

- Number of hosts that were scanned during the test: 29

- Number of SECURITY HOLES found: 0

- Number of SECURITY WARNINGS found: 2

- Number of security notes found: 6

IP Address: 64.001.00.1 - Open ports found, **YES.** Risk factors: **LOW** to **HIGH** security **WARNING** and informational security notes.

IP Address: 64.001.00.2 - Open ports found, **YES.** Risk factors: **LOW** security **WARNING** and informational security notes.

IP Addresses: 64.001.00.3 – 64.147.13.15 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.110 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.111 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.191 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.1 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192. 001.00.2 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.4 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.5 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.6 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.7 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.9 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.23 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.24 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 192.001.00.251 - Open ports found, **NONE.** Risk factors: **NONE**

IP Address: 208.001.00.178 - Open ports found, **NONE.** Risk factors: **NONE**

Risk Charts

Outline of Tested Host IP Addresses

The IP Addresses that were provided that have public exposure and were tested are: 64.001.00.1 – 64.001.00.15, 192.001.00.110, 192.001.00.111, 192.001.00.191, 192.001.00.1, 192.001.00.2, 192.001.00.4, 192.001.00.5, 192.001.00.6, 192.001.00.7, 192.001.00.9, 192.001.00.23, 192.001.00.24, 192.001.00.251, and 208.001.00.178.

The following is an outline of the provided IP Addresses that are currently being used by SAMPLE CLIENT along with the aforementioned findings being detailed on the following pages accordingly:

I. IP Addresses: 64.001.00.1

II. IP Addresses: 64.001.00.2

III. IP Addresses: 64.001.00.3 – 64.001.00.15

IV. IP Address: 192.001.00.110

V. IP Address: 192.001.00.111

VI. IP Address: 192.001.00.191

VII. IP Address: 192.001.00.1

VIII. IP Address: 192. 001.00.2

IX. IP Address: 192. 001.00.4

X. IP Address: 192.001.00.5

XI. IP Address: 192.001.00.6

XII. IP Address: 192.001.00.7

XIII. IP Address: 192.001.00.9

XIV. IP Address: 192.001.00.23

XV. IP Address: 192.001.00.24

XVI. IP Address: 192.001.00.251

XVII. IP Address: 208.001.00.178

XVIII. Risk Charts

I. IP Address: 64.001.00.1

IP Address: 64.001.00.1

Open ports: Yes

List of open ports:

- ***general/tcp* (Security notes found)**
- ***domain (53/udp)* (Security notes found)**
- ***ntp (123/udp)* (Security warnings found)**
- ***general/udp* (Security notes found)**

Information found on port general/tcp

The remote host is up

Information found on port domain (53/udp)

A DNS server is running on this port. If you do not use it, disable it.

Risk factor: Low

Warning found on port ntp (123/udp)

An NTP server is running on the remote host. Make sure that you are running the latest version of your NTP server, as some versions have been found out to be vulnerable to buffer overflows.

Solution: Upgrade
Risk factor: High!!!!!!!!
CVE: CVE-2001-0414
BID: 2540

Information found on port ntp (123/udp)

It is possible to determine a lot of information about the remote host by querying the NTP (Network Time Protocol) variables - these include OS descriptor, and time settings.

It was possible to gather the following information from the remote NTP host:

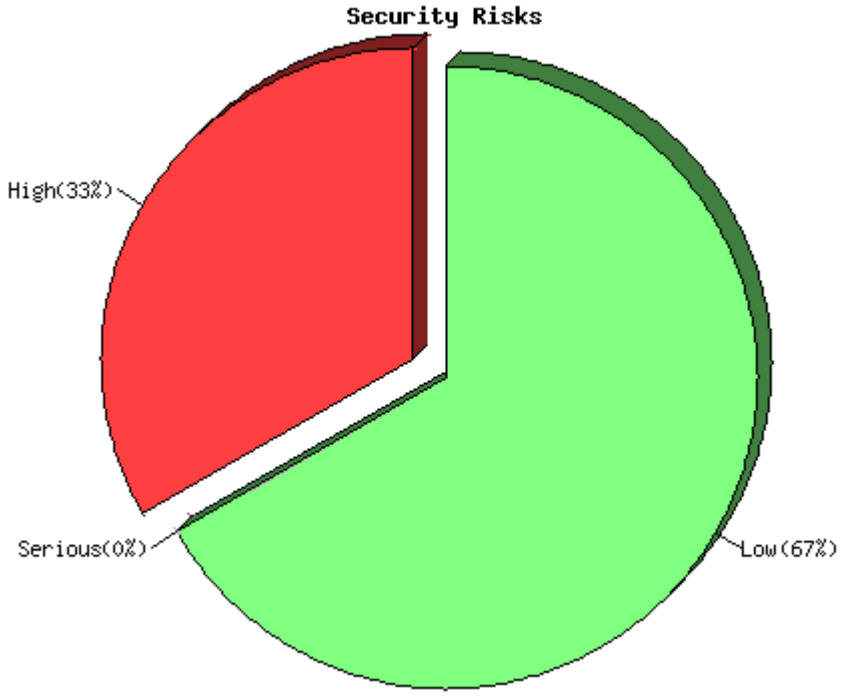
system='cisco', leap=0, stratum=2, rootdelay=60.27, rootdispersion=1.27, peer=30959, refid=172.17.1.243, reftime= 0xD6316167.8BDEC807, poll=6, clock= 0xD631617F.969C84E0, phase=-0.708, freq=-28.64, error=0.12

Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore

Risk factor: **Low**

Information found on port general/udp

For your information, here is the traceroute to 64.001.00.1:
192.001.00.8
192.001.00.1
10.6.64.1
97.75.226.253
204.001.00.65
67.001.00.78
63.001.00.34
4.69.144.79
4.53.230.66
68.1.0.185
68.001.00.229
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41
64.001.00.41


Security Risks
High(33%)
Serious(0%)
Low(67%)

II. IP Address: 64.001.00.2

IP Address: 64.001.00.2

Open ports: Yes

List of open ports:

- ***general/tcp* (Security notes found)**
- ***isakmp (500/tcp)* (Security warnings found)**
- ***general/udp* (Security notes found)**
- ***domain (53/udp)* (Security notes found)**

Information found on port general/tcp

The remote host is up

Warning found on port isakmp (500/tcp)

The remote host seems to be enabled to do Internet Key Exchange (IKE). This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.

Solution: You should ensure that:
1) The VPN is authorized for your Companies computing environment
2) The VPN utilizes strong encryption
3) The VPN utilizes strong authentication

Risk factor: Low

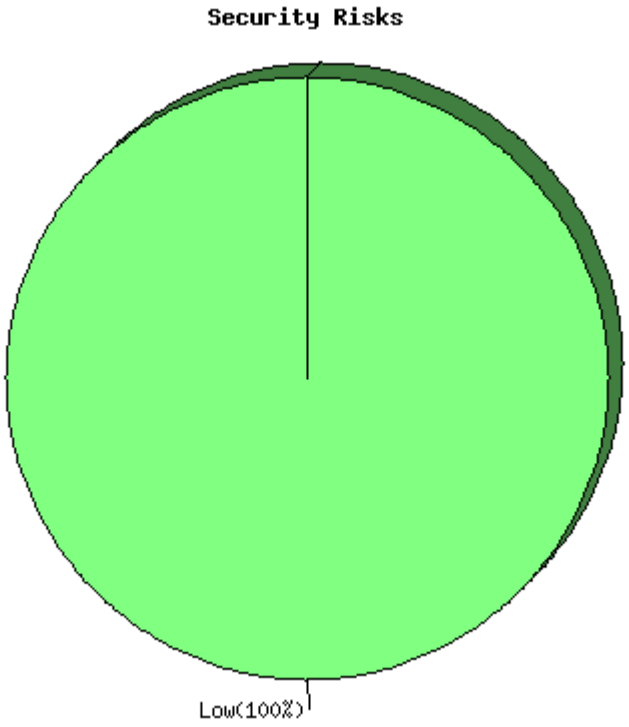
Information found on port general/udp
For your information, here is the traceroute to 64.001.00.2:
192.001.00.8
192.001.00.1
10.6.64.1
97.75.226.253
204.001.00.65
67.001.00.78
63.001.00.34
4.69.144.79
4.53.230.70
68.001.00.185
68.4.11.93

64.001.00.41
64.001.00.41
?

Information found on port domain (53/udp)

A DNS server is running on this port. If you do not use it, disable it.

Risk factor: Low



III. IP Address: 64.001.00.3 - 64.001.00.15

IP Address: 64.001.00.3

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.4

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.5

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.6

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.7

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.8

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.9

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.10

Open ports: Yes

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.11

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.12

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.13

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.14

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IP Address: 64.001.00.15

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IV. IP Address: 192.001.00.110

IP Address: 192.001.00.110

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

V. IP Address: 192.001.00.111

IP Address: 192.001.00.111

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

VI. IP Address: 192.001.00.191

IP Address: 192.001.00.191

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

VII. IP Address: 192.001.00.1

IP Address: 192.001.00.1

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

VIII. IP Address: 192.001.00.2

IP Address: 192.001.00.2

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

IX. IP Address: 192.001.00.4

IP Address: 192.001.00.4

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

X. IP Address: 192.001.00.5

IP Address: 192.001.00.5

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XI. IP Address: 192.001.001.6

IP Address: 192.001.00.6

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XII. IP Address: 192.001.00.7

IP Address: 192.001.00.7

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XIII. IP Address: 192.001.00.9

IP Address: 192.001.00.9

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XIV. IP Address: 192.001.00.23

IP Address: 192.001.00.23

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XV. IP Address: 192.001.00.24

IP Address: 192.001.00.24

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XVI. IP Address: 192.001.00.251

IP Address: 192.001.00.251

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XVII. IP Address: 208.001.00.178

IP Address: 208.001.00.178

Open ports: NONE

List of open ports:

- none

The remote host is considered as dead - not scanning

XVIII. Risk Charts