

Challenge 4: VoIP (intermediate)

Name (required): Fabio Panigatti	Email (required): fabio.panigatti@gmail.com
Country (optional): Italy	Profession (optional): <input type="checkbox"/> Student <input checked="" type="checkbox"/> Security Professional <input type="checkbox"/> Other

Section 1/ Question 1. What protocol is being used? Is it TCP or UDP?	Possible Points: 1pt
Tools Used: vim, grep	
Awarded Points:	
UDP only	

Section 1/ Question 2. Could this log be the result a simple nmap scan being run against the honeynet? Explain	Possible Points: 1pt
Tools Used: vim	
This log cannot be the result of a “simple” nmap scan because nmap doesn't speak SIP out-of-the-box. Actually with nmap is possible to do a lot more than simply probe the udp port by writing a lua script for NSA (Nmap Scripting Engine). So, with a little lua coding it will be possible to perform a scan wich leaves a trace like this - even mimic/faking a sipvicious scan (User-Agent, behaviour, etc) - but it would no longer be a “simple nmap scan”.	

Section 1/ Question 3a. Name the scanning tools that may have been used to by the attacker.	Possible Points: 1pt
Tools Used: vim	
The scanning tools are from SIPvicious suite. More in detail: the svmap.py (one probe only), svwar.py and swcrack.py tools.	

Section 1/ Question 3b. What was the tool suite author's intended use of this tool suite ? Who was it designed to be used by?	Possible Points: 1pt
Tools Used:	
The intended use is SIP VoIP systems auditing. It is designed to be used by SIP administrators and security professionals.	

Section 1/ Question 3c. One of these tools was only used against a small subset of extensions. Which were these extensions and why were only they targeted with this tool ?	Possible Points: 2pts												
Tools Used: sed, sort, uniq													
The swcrack.py tool was used against the following extensions:													
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Extension</th> <th style="text-align: left;">Cracking Attempts</th> </tr> </thead> <tbody> <tr> <td>100</td> <td>-</td> </tr> <tr> <td>101</td> <td>30</td> </tr> <tr> <td>102</td> <td>29</td> </tr> <tr> <td>103</td> <td>22</td> </tr> <tr> <td>111</td> <td>43</td> </tr> </tbody> </table>	Extension	Cracking Attempts	100	-	101	30	102	29	103	22	111	43	<p>This is because the REGISTER attempts for 101, 102, 103, 111 received a 401 reply, so these extensions were reported by swwar.py to be existent and marked with “reqauth”. Due to a lack of “Authorization” header both in the svcrack.py and Zoiper attack phases we can assume that extension 100 received a 200 during the enumeration phase and was then reported by swwar.py to be existent and marked with “noauth”.</p> <p>Despite that, all these five extensions were later feeded into swcrack.py for the cracking phase, even if “cracking” 100 was pointless. There are only two log entries for 100 in the svcrack.py phase, because the tool quitted after the 200 reply.</p>
Extension	Cracking Attempts												
100	-												
101	30												
102	29												
103	22												
111	43												
<p>We can argue that the cracking dictionary (or number range) was the same for all the probed extensions, so we can guess that 101, 102 and 103 where cracked while 111 would have been cracked only if dictionary or range size was more than 43 items. Other than that, there are no evidences that 102, 103 and 111 were successfully cracked, while evidence exists that at least 101 was cracked (see successful Zoiper phase).</p>													

Section 1/ Question 4a. How many extensions were scanned? Are they all numbered extensions, or named as well?. List them	Possible Points: 2pts
Tools Used: sed, sort, wc	
<p>total: 2652 numbered: 2608 named: 44 (aaron abigail admin andrew asterisk christopher client cpanel data fax freddy heaven help info jane jobs joshua manager market marketing mike news norman operator oracle orders owner postfix postmaster richard sales samantha sarah sebastian service shop spam steve steven support temp test trixbox user)</p>	

Section 1/ Question 4b. Categorize these extensions into the following groups, and explain to method you used:	Possible Points: 6pts
<ul style="list-style-type: none"> • Those that exist on the honeypot, AND require authentication • Those that exist on the honeypot, and do NOT require authentication • Those that do not exist on the honeypot 	
Tools Used: vim, sed	
<p>Exists and require auth: 101, 102, 103, 111. Evidences: “Authorization” header is present in some of the log entries, so server replied with 401 to the previous attempt. Exists and don't require auth: 100. Evidences: no “Authorization” header sent neither by the svcrack.py, nor by Zoiper, so server always replied with 200 to the requests for extension 100. Not existent: every other. Evidences: no more logs after the end of swwar.py scan at 2010-05-02 01:49:46.992699 so we can assume that requests for these extensions always returned 404.</p>	

Section 1/ Question 5. Was a real SIP client used at any point ? If it was, what time was it used, and why ?	Possible Points: 1pt
Tools Used: grep, sort	

It's likely that Zoiper (rev.6751) was used from 2010-05-05 10:00:08.170954 to try to place three calls REGISTERing as extension 101 and 100. Obviously, "User-Agent" header string is under attacker's control and it is easily spoofable. Looking at the client and at the timings, it's likely that the three calls were attempted to test the overseas call capabilities of the involved extensions.

Section 1/ Question 6. List the following, include geo-location information.
 - Source IP addresses involved
 - The real world phone numbers that were attempted to be dialled

Possible Points: 3pts

Tools Used: whois, web browser

IP addresses:

210.184.X.Y ... Hong Kong
 89.42.194.X ... Costanta, Romania

Real world phone numbers (called from Australia):

00112322228XXXX ... City: Freetown (city), Country: Sierra Leone, Carrier: Sierratel
 00112524021XXXX ... Region: Central Somalia, Country: Somalia, Carrier: Hormuud
 900114382089XXXX ... guess the intended real number was 0011(43)820-89XXXX, belonging to Austria numbering plan for services with regulated maximum tariffs; maybe a typo or an attempt to prepend a long-distance-call-enabling digit to the real number.

Section 1/ Question 7. Draw a simple static or animated timeline of events, describing when and where certain phases occurred from, and what the purpose of each phase was

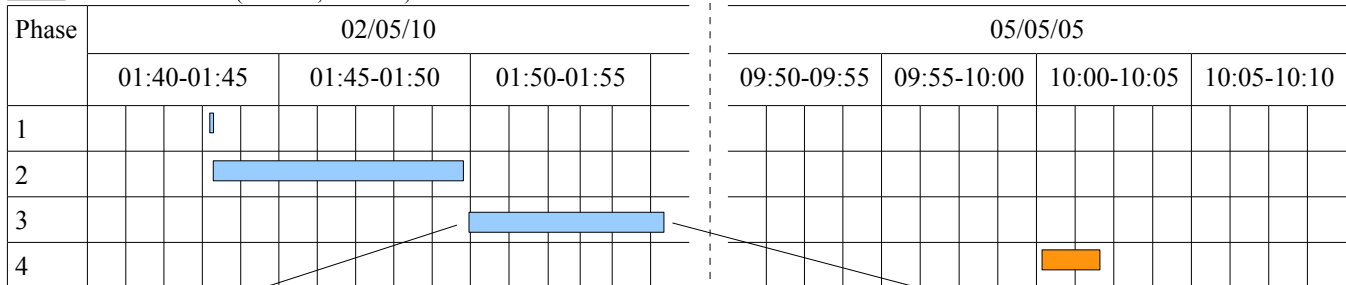
Possible Points: 5pts

Tools Used:

Phase	Tool	Start	End	Duration	Source IP	Logs	Purpose
1	svmap.py	2010-05-02 01:43:05.606584	2010-05-02 01:43:05.606584	00:00:00	210.184.X.Y	1	Discover / fingerprinting
2	svwar.py	2010-05-02 01:43:12.488811	2010-05-02 01:49:46.992699	00:06:34	210.184.X.Y	2652	Extensions enumeration
3	svcrack.py	2010-05-02 01:49:56.063150	2010-05-02 01:50:21.263816	00:00:25	210.184.X.Y	170	Password cracking: 102
		2010-05-02 01:50:38.439328	2010-05-02 01:51:06.927874	00:00:29		192	Password cracking: 103
		2010-05-02 01:51:22.378144	2010-05-02 01:51:28.729516	00:00:06		2	Password cracking: 100
		2010-05-02 01:51:35.904174	2010-05-02 01:52:01.717913	00:00:26		172	Password cracking: 101
		2010-05-02 01:52:19.616248	2010-05-02 01:55:11.496170	00:02:52		1059	Password cracking: 111
4	Zoiper	2010-05-05 10:00:08.170954	2010-05-05 10:01:48.058434	00:01:41	89.42.194.X	18	Place some test calls

From 210.184.X.Y (Hong Kong)

From 89.42.194.X (Costanta, Romania)



--

Section 1/ Question 8a. Assuming this were a real incident, write 2 paragraphs of an Executive summary of this incident. Assume the reader does not have IT Security or VOIP experience. a) First Paragraph: Write, in the minimum detail necessary a description the nature and timings, and possible motives of the attack phases. (3 points)	Possible Points: 3pts
--	-----------------------

Tools Used:

On 02/05/2010 and 05/05/2010 the company's VoIP system was targeted by two network attacks from the outside. Despite the sources of the two attacks were very different (namely Hong Kong and Romania) is very likely that the both were performed by the same entity. The 02/05/2010 attack started at 01:43:05 and was a 12 minutes three-phases attack. The first was the "discovery" phase, to find the PBX on the internet. The second was the "enumeration" phase, to find valid accounts. The third was the "cracking" phase, to guess the passwords of the account found in the previous phase. The 05/05/2010 attack occurs at 10:00 AM and was likely a test drive to verify the overseas call capabilities of the accounts gathered in the first attack. The both attacks were successful: thanks to weak or blank passwords, they gain access to at least four (100, 101, 102, 103) and up to five (the previous four plus 111) company VoIP accounts and they were able to place at least two valid overseas call impersonating 100 and 101 accounts. The attack was likely in preparation of future abuses of our VoIP PBX to make overseas/expensive calls for free, eventually reselling to unaware third parties the telephone traffic for which we would have been billed. The abuse attempt was discovered in its early stage, so the overall cost of the attack is limited to the bill for the two 05/05/2010 overseas calls plus forensics analysis and emergency flaw fixing effort.

Section 1/ Question 8b. Assuming this were a real incident, write 2 paragraphs of an Executive summary of this incident. Assume the reader does not have IT Security or VOIP experience. b) Second Paragraph: What actions would you recommend should occur following this particular incident, include any priority/urgency. Also describe any good practices that should be employed to mitigate future attacks.	Possible Points: 3pts
---	-----------------------

Tools Used:

(I assume a small size company with a few dozens VoIP extensions and little budget, so no expensive solutions like IPSs)

Some emergency measures has already been taken in order to stop the abuse of the PBX. We recommended the following corrective actions and fixes:

Action	Extensions	Urgency	Suggested Schedule
Assign a strong password to abused account/extension	100, 101, 102, 103, 111	Very high	Done ¹
Deploy and possibly <u>enforce</u> a policy for strong passwords		High	3 d
After that, change the password of every VoIP account ²	All	High	3 d
Inhibit calls for overseas destination and premium rate numbers known to be useless ³ and define internal procedures to unlock the blocked destination by user request.	All	Medium	2 w

¹ it was very urgent to fix the exploited flaws, so this step has already been done.
² The attack was limited to only a subset of the existing extensions and it is likely that more account may exist with the same exploitable flaws.
³ May help even with internal abuse/misuse.

We also recommend to evaluate and adopt the following good practices:

- do not expose VoIP system to the outside world, if not required;
- off-site/external users should access VoIP system only over encrypted VPN channels;
- calls for geographic/overseas destination and premium rate numbers should be enabled on a per-user/per-group basis (this approach is tighter than the one mentioned in the recommended actions);
- restrict client capabilities by source ip/net (internal, internal-privileged, external, etc);
- enable features that would discourage scanning, like replying with an "authorization request" for every request for

an unknown extension (this would break standards, but there's not real drawbacks for everyday use);

- enable simple daily statistics of voip traffic/destination for early detection of misuse patterns (overall call count, long-destination/overseas call count, failed login attempts, etc); monitoring with existing NMS is strongly suggested.

Section 2/ Question 1. Which 4 protocols are involved in the PCAP (VOIP protocols and otherwise) ? Give a brief explanation as to their purpose.	Possible Points: 4pts
---	-----------------------

Tools Used:

- 1) SIP over UDP: register extension 555, set-up and terminate a call from 555 to 1000
- 2) RTCP: RTP quality monitoring and a little RTP session management
- 3) RTP: audio streams
- 4) HTTP: trixbox web administration interface browsing
- 5) ICMP: a couple of port unreachable (pcap seq 4445, 4447) from 172.25.105.3 elicited by RTP frames with RTP seq 38112 and 38113 (pcap seq 4440, 441) reaching 172.25.105.40 after port 63184/udp was almost closed.

Section 2/ Question 2a. Which codec does the RTP stream use?	Possible Points: 1pt
--	----------------------

Tools Used: wireshark

G.711 ITU-T codec with mu-law scaling (PCMU)

Section 2/ Question 2b. How long is the sampling time (in milliseconds)?	Possible Points: 1pt
--	----------------------

Tools Used: wireshark

20 ms

Section 2/ Question 3. How did the attacker gain access to the server? List ways this could have been prevented.	Possible Points: 2pts
--	-----------------------

Tools Used:

Access to Trixbox management interface: according to “Authentication” header, is very likely that the attacker gained access simply trying for the trixbox default username and password (maint, password). Prevention: 1) stronger password policy; 2) don't expose services on internet if not required.

REGISTER on VoIP PBX: username (555) and password (1234) found using Trixbox web management features (see more later).

Ironically enough, the trixbox management interface suggests an upgrade to the “weak password detection” tool.

Section 2/ Question 4. What information was gained by the attacker ?	Possible Points: 2pts
--	-----------------------

Tools Used:

Over other PBX related information, the attacker gained details about 555 and 556 extensions (view “tcp.stream eq 91”) by opening sip_custom.conf configuration file from within the web interface, including accounts username (555) and password (1234).

Section 2/ Question 5a. The PCAP includes a (not so) hidden bonus! [hint1: You can't read it in the pcap, hint2: It's a city with an active honeynet chapter]	Possible Points: 10pts
---	------------------------

a) Describe it, and explain how you found it.	
Tools Used: wireshark	
<p>The RTP audio stream contains the phrase “[...] the secret password is mexico [...]”.</p> <p>I guess “mexico” is the answer, despite actually it is not a “city”.</p> <p>The RTP audio stream is corrupted and distorted by out of sequence frames, errors in frame timestamp and delayed packed wich are likely to fall out of the jitter buffer. This is especially true in the very interesting part of the stream. The steps to improve audio quality were:</p> <ol style="list-style-type: none"> 1) reorder the frames by RTP timestamp instead of capture time; 2) increase the jitter buffer (a usefull option with no drawbacks for non-interactive conversations like this). <p>Either of the two would be enough to fully understand the speech. Applying the both give the best results in terms of “bad frames” count but the actual audio improvement is quite negligible.</p>	

Section 2/ Question 5b. If VOIP packets between the two calling parties traverse an untrusted network (eg the wireless/internet) and a similar PCAP was captured by a malicious party, would you think this a security problem? why?	Possible Points: 3pts
Tools Used: wireshark	
<p>1) Looking only at packets strictly related to VOIP (guess this is the scope of the question):</p> <ul style="list-style-type: none"> – SIP: extension 555 has a very weak password (1234), so it would be very easy and fast for an attacker to bruteforce the Authentication header even without any knowledge of the HTTP part of the stream (which discloses 555 password); speaking of SIP password cracking, it is quite common to try a digit-only-bruteforce first, so the cracking time of this kind of “secrets” is very small; – RTP: unencrypted voice stream may carry sensitive informations; for example... a very “secret password” (mexico, you know...) exchanged by voice. <p>2) Looking at the whole capture:</p> <p>The trixbox web interface was browsed with basic authentication over cleartext HTTP; the Authentication header is bWFpbnQ6cGFzc3dvcmQ= which decode in the already easy guessable default credentials (Username = maint Password = password). Even if in this very case it would have been very easy to access the web interface using this default password even without any knowledge of the pcap content, disclose a basic auth header is a bad idea.</p> <p>3) looking at the capture event itself:</p> <p>The attacker is in a very privileged place: if he can capture that pcap, maybe he can even easily alter the audio stream (injection) with no need to guess anything (ip and ports, conversation time, sequence numbers, RTP Timestamp values, ... se more on RTP injection later).</p>	

Section 2/ Question 5c. Wireshark has an option "Use RTP timestamp". What is the function of this option?	Possible Points: 2pts
Tools Used:	
<p>To place the RTP frames in the right timing order using the timestamp in the RTP payload instead of the frame pcap capture time. Or, in other words, to align samples in the right timeline.</p>	

Section 2/ Question 6. What technologies or protocols can be used to protect confidentiality of RTP traffic as it traverses untrusted networks.	Possible Points: 3pts
Tools Used:	
<ol style="list-style-type: none"> 1) built-in encryption, despite the pretty poor default standard DES-CBC algorithm; better encryption algorithms may be negotiated if every endpoint agree; 2) tunnelling on layer 2 or layer 3 encrypted tunnels (Ipssec, OpenVPN, ...) 3) TLS over TCP 	

Section 3/ Question 1. What is "RTP injection" and describe how it functions. What conditions are required to allow this?	Possible Points: 2pts
Tools Used:	
<p>Due to the UDP transport and the lazy session control of the RTP protocol, it's not so difficult to insert arbitrary frames in the RTP streams. The sliding window for acceptable out-of-sequence packet is wide enough to make the attack feasible.</p> <p>Conditions: attacker need to know details about...</p> <ul style="list-style-type: none"> ... the call itself: involved ip addresses and ports, synchronization source identifier (SSRC) and codec used (payload type); this values remains the same for the whole call; ... the state of the call: RTP sequence numbers and timestamps; the increase of these values is linear and time dependent and so are almost predictable; even a imprecise knowledge of these two values would be enough for a try. <p>For a successful attack, at least one legitimate frame should be captured to initialize the above mentioned values. With no prior knowledge of these values the success rate drops. The rogue frames must carry a sequence number and a timestamp a little bit higher than the frames the RTP peers are processing. If the rogue frames are accepted as valid, the legitimate frames will be discarded as obsolete because the window for the acceptable frames has shifted forward.</p>	

Section 3/ Question 2. Explain how a SIP password digest could be intercepted or stolen. Is this a security issue? why or why not.	Possible Points: 2pts
Tools Used:	
<ol style="list-style-type: none"> 1) sniffing SIP password digest are carried by the "Authentication" SIP header. If the SIP traffic is exchanged in cleartext over a "sniffable" media (ethernet hub, ARP-poisonable switched ethernet, unencrypted wireless, tap on network trunk, ...) or the attacker is on the route between the client and the server (compromised router, ...) then the digest can be intercepted by simply sniffing on the wire. 2) hijacking Trick the client into connect to a rogue SIP server instead of the real one using well known hijacking/mitm techniques (dns poisoning, layer 2 attacks, routing attacks, resolver hijacking, ...). The rogue SIP server then collects the authentication attempts, eventually trying to downgrade authentication scheme to BASIC. <p>It is a security issue because, even if the digest is not usable as-is, it can be cracked. And cracking the digest is much faster (and make very very less "noise") than trying to crack the password over the net with tools like svcrack.py. If the downgrade to BASIC authentication succeed, there's even no need to crack a digest at all, because passwords would be simply base64 encoded.</p>	

Section 3/ Question 3. Is DDoS a threat to VOIP systems? Are there any general functional requirements of telephony systems that would be impaired by a DDoS?	Possible Points: 2pts
Tools Used:	

VoIP systems are obviously vulnerable to many common threats like every other internet services. But DDoS is a very specific threat for VoIP systems because of the real-time nature of the RTP protocol. Even a small flooding, which would go quite unnoticed in different scenarios, may have a severe impact on voice streams due to increased network delays (filling the router's queues and network bandwidth), dropped frame rate and CPU usage (for "bad" frame processing).