Meno (čitateľne) a podpis :

Dňa : 5.12.2016

IPS specialist – poznatky

Proces:

1. Explain me (as a non-IT business manager) the role of IPS in the organization, its purpose and reasoning behind your work.

   Properly configured and managed IPS can provide organizations with an early warning sign of a compromise using network monitoring and modifying techniques, and thus helps organizations to mitigate possible breaches. IPS system can help to protect company infrastructure against industrial espionage, opportunistic attacks or data exfiltration by internal threats. This can result in cost savings, brand and know-how protection. IPS can also serve as an information source regarding the health and usage of the infrastructure used by business. However, intrusion prevention system should be just one part of a layered security design.

2. Simply describe IPS deployment option:

   IPS system has to be always connected inline, so it can drop select packets in the case of positively identified attacks. Most common places for an IPS to be deployed is on the network border. IPS is deployed on the external side of a router which is routing traffic between the LAN (or zone within larger network) and external WAN. If there is an external firewall, I would put IPS behind it, we can expect lots of malicious traffic from the Internet, but we are trying to protect our infrastructure, so we want to monitor firewalled traffic with fewer alerts and processing. IPS management link should be connected into the internal network for the administration (signature updates, etc.)
   This approach has weaknesses, e.g. when the IPS fails, and the IPS is a commercial device able to bridge traffic even in a fail state (fail open), we are not able to analyze traffic during “IPS down“ period. In this case we should have also worked IDS tap within an internal side of a network. We can use IDS in more aggressive mode, test new signatures against it during normal periods, and also be able to analyze traffic during IPS fail state. Internal IDS monitoring can also be used for later investigation, when we are able to tell which internal address was generating the traffic by correlating the IPS - IDS logs.

3. What is IPS evasion, name/simply describe some techniques?

   IPS evasion is a technique used by malicious actors in order to bypass IPS detection and be able to carry their operations.

   * Fragmentation - splitting payload across multiple packets and time, so even session reconstruction can't decide if its attack or not.
   * Fake IPS alerts generation used as “fog of war“, so an attack is covered by a noise of non-important alerts on the signatures generated by an attacker herself.
   * Protocol steganography techniques (DNS, ICMP, HTTP requests) – data exfiltration
   * Custom compression, encryption, obfuscation, encoding (e.g. Vail framework for payloads)
   * random URL pattern generation – exploit kits
   * Fast flux DNS for rapid IP address change – blacklist evasion

4. Describe IPS operations on specific ISO-OSI layers with examples

   Layer 2 – 7
   Network Intrusion Prevention System (NIPS) – collecting and blocking traffic, mostly on the link layer (using PCAP like libraries) but using parsers and plug-ins to monitor traffic on all layers of the OSI model. Able to filter packet based on raw bytes, IP addresses, TCP sessions.
   NIPS concentrate mostly on the application protocols (HTTP, FTP, SMB, SSH, SNMP…)
   Examples: Snort, Suricata (Layer 3 - 7)
   Cisco Intrusion Prevention (Layer 2 – 7) – ARP attack detection

   Layer 7
   Host Intrusion Prevention System (HIPS) – usually the software agent at the end point (workstation, server), could be AV solution. Collecting data from the system, monitoring file integrity, logins, enforce security policy, collecting logs. Can prevent execution of the known malware
   Working on an application layer, it can be capable to filter traffic using ring0 drivers, if it also serves as a software firewall
   Examples: Samhain, OSSEC, some commercial AV solutions

5. What are your preferred vendors for specific ISO-OSI layers?

   Snort for NIPS (network layer)
   OSSEC looks interesting as HIDS(application layer), but I have never used it before

6. What is false positive / negative?

   In the case of IPS, false positive means, that the system emitted alert on a benign activity. False negative means, that the IPS system didn't create alert in the case of an intrusion attempt, which is, I believe, is a worse scenario.

7. Describe rule-tuning options:

   * using thresholds – we can filter events that are occurring periodically (like DoS attack packets). A rule can be triggered on the first detection, then we should filter additional events, so we are not flooded by alerts.
   * exclude rules for the applications that are not used in our infrastructure (x11, PHP, Oracle)
   * alerts suppression – we can limit alerts generated by specific hosts in the case of prevailing false positives for that host
   * write as specific rules as possible – if we can use specific protocol header options in our rule, we should do that, as header is processed before the payload is analyzed. If we know the exact location of the content we are searching for, we should use this information as well. More specific rules can save processing power.
   * setting preprocessors – we should properly configure preprocessors like frag3 (fragmentation). If we know our network topology, used operating systems (tcp stack..) and our IPS is behind the firewall, we can turn off some of the preprocessors.
   * properly configure IPS – set home network IP, describe servers by IP and expected protocols
   * analyze alerts and change rules based on that

8. Provide examples for inappropriate use of IPS:

   * Inline connected IPS on a backbone network (ie. 10 Gigabit throughput) with fail-close policy. IPS will fail, and the business will be crippled.
   * Use deployed IPS without trained personnel or third party continuously managing it
   * IPS deployed where Web Application Firewall is enough

9. Provide description on integration with other infrastructure devices – examples, issues:

   HIPS and NIPS produced data can be collected into SIEM together with the logs, Netflow data and other collected information. Events can be correlated across data from the multiple sensors / devices.
   Some commercial vendors like Cisco have integrated ability to monitor or block specific traffic triggered by an IPS system. It can push events into switches, firewalls or wireless LAN controllers.
   If the IPS system is not properly configured and protected, it can do lots of harm. It is a huge attack surface, and if an attacker is able to take over IPS, she can exploit knowledge of the network as well as cover her tracks later.

   ##

   Write here results of tasks 1 – 6 (as many as you can). For each task describe:

- **Identification of attacker / victim**
- **Activity type (portscan, server attack, client attack,...)**
- **What happened (i.e. including CVE missused, exploit used,...)**
- **Add snort signatures that you think may catch the malicious activity**
- **What would you do in case of spotting this activity in network?**

PLEASE NOTE THAT FILES MAY CONTAIN MALICIOUS CONTENT AND HANDLE THEM WITH CARE.

Task 1:

- Hearthbleed vulnerability exploitation - CVE-2014-0160
- attacker 10.20.30.1 – 10.20.30.56 victim (server running SecurityOnion?)
- TLSv1.1 on non standard port number - 444

In the case of successful exploitation, expect all the secrets within affected RAM memory to be compromised. Attacker is able to remotely read servers RAM memory.
s
Remediation: Upgrade affected crypto libraries. Regenerate encryption keys used by the server.

Example rule:
drop tcp any any -> $HOME_NET any (msg:"Heartbleed vulnerability exploitation attempt"; flow: to_server; content:"|18 03 02 00 03 01 40 00|"; reference:cve, CVE-2014-0160; sid:1000001; rev:1;)

Task 2:

- Web Application Attack - SQL injection attempt against web server
- attacker 117.195.143.198 - 208.106.128.136 victim (web service)
- "0 and 1 = 0" passed in the URL (and referrer for the CSS file - this can be also vulnerability)

Remediation:
I would recommend to use Web Application Firewall for this kind of attack, it is very easy to modify string to evade pattern matching .
We can use regexp to filter some basic SQLi attempts, but WAF with an white-listed requests can be better approach.

Example rule:
drop tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg: "SQL injection attempt"; flow: to_server, established; content: "GET"; http_method; pcre: "/(and|or)\+1=0/i"; sid:1000002; rev:1;)

Task 3:

- CVE-2014-6271 - “ShellShock” - remote injection of the bash environment variable
- attacker 10.246.50.2 – 10.246.50.6 victim (Linux server)
- String used as a test: “User-Agent: () { :;}; /bin/ping -c1 10.246.50.2 ”

Remediation:
We can filter packets that are using known command syntax. We should patch the server, keep it updated.

Example rule:
drop tcp any any -> $HOME_NET $HTTP_PORTS (msg:"Shellshock Bash environment variable injection"; content:"() {"; http_header; fast_pattern:only; reference:cve,2014-6271; sid:1000003; rev:1;)

Task 4:

- TCP scan using FIN, PSH, URG flags – so-called “Xmas scan”
- attacker 192.168.1.10 - 192.168.1.25 target system with port 80 opened, so probably HTTP server
- The FIN, PSH, and URG TCP flags are set
- if we want to generate alerts, as there will be thousands of them with just the stateless rule, we should use thresholds, stream preprocessor

Remediation:
Drop/filter packets and temporary blacklist the IP address.

Example rule:
drop tcp any any -> $HOME_NET any (msg:"Nmap XMAS scan"; flags:FPU,12; flow:stateless; reference:arachnids,30; classtype:attempted-recon; sid:1000004; rev:1;)

Task 5:

- Browser exploitation on the workstation by the Anger Exploit kit, or some fork of it
- CVE-2014-0322 - exploits use after free condition in the Internet Explorer 10

192.168.204.211 – Victim - regular workstation (inside VMware?)
193.225.32.11 (www.ektf.hu) first server, serve malicious javascript file \ redirector, initial recon
213.192.241.64 (ortoexport.es) second server, Exploit kit landing page
85.10.220.153 (k615o5ij7f.skwosh.eu) Exploit kit back-end which delivers actual payload

Remediation:
Full compromise, if we did not block the traffic, we have to quarantine and investigate the victims machine, as there is probable malware infection.
Patch Flash and Java on the victim machine. Find out if the URL was distributed via email, or how the user come to the web page.

Example rules:
Exploit attack is rather complex case, and should be mitigated by multiple rules, IP blacklists and of course, vulnerable software should be updated. I believe this two rules from the official Snort ruleset should block this attack even if the back-end IP addresses and URL patterns are changed:

drop tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS DRIVEBY Angler EK Apr 01 2014"; flow:established,to_client; content:"Expires|3a| Sat, 26 Jul 1997 05|3a|00|3a|00 GMT|0d 0a|Last-Modified|3a| Sat, 26 Jul 2040 05|3a|00|3a|00 GMT|0d 0a|"; fast_pattern:55,20; http_header; classtype:trojan-activity; sid:2019224; rev:4;)

drop tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Angler EK encrypted binary (3) Jan 17 2013"; flow:established,to_client; file_data; content:"|7d 6b f8 64 76 74 6e 66|"; within:8; flowbits:set,et.exploitkitlanding; classtype:trojan-activity; sid:2017986; rev:1;)

Task 6:

- network worm infection attack
- attacker 98.114.205.102 - 192.150.11.111 victim - Windows XP workstation
- LSASS (Local Security Authority Subsystem Service) service exploitation
- The vulnerability is CVE-2003-0533 (MS04-011) - "LSASS buffer overflow" vuln.
- This vulnerability exploit a lack of array boundary checking in a LSASS function when writing to the log file

Full compromise, portable executable (ssms.exe) file is downloaded using socks protocol.
We have to quarantine and investigate the victims machine, as there is probable malware infection.

Remediation:
For the future, we can block initial IPC request in the frame 26 using named pipe: 3919286a-b10c-11d0-9ba8-00c04fd92ef5 - lsarpc (lsass alias). We shoul patch the workstation and keep it up-to-date.

Example rule:
drop tcp any any -> $HOME_NET 445 (msg:"NetBIOS SMB LSASS bind attempt"; content:"|00|"; offset:0; depth:1; content:"|FF|SMB"; nocase; offset:4; depth:4; content:"|6A 28 19 39 0C B1 D0 11 9B A8 00 C0 4F D9 2E F5|"; distance:112; within:16; reference:cve,CVE-2003-0533; sid:1000006; rev:1;)