ANALYSIS OF A PCAP FILE -

A certain PCAP file and an alert file have been discovered to analyze certain priorities and ambiguities in the network.

The alerts of the managed systems has provided us with different alerts which are to be responded -

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	2019-12-25 06:28...	139.199.184.166	55812	10.12.25.101	80	6	GPL WEB_SERVER robots.txt access
RT	22	2019-12-25 06:28...	139.199.184.166	55812	10.12.25.101	80	6	ET WEB_SPECIFIC_APPS PHPStudy Remote Code Execution Backdoor
RT	6	2019-12-25 06:28...	139.199.184.166	55812	10.12.25.101	80	6	ET WEB_SERVER WEB-PHP phpinfo access
RT	1	2019-12-25 06:29...	139.199.184.166	58569	10.12.25.101	80	6	ET INFO Mozilla User-Agent (Mozilla/5.0) Inbound Likely Fake
RT	150	2019-12-25 06:29...	10.12.25.101	80	139.199.184.166	59314	6	ET SCAN Unusually Fast 404 Error Messages (Page Not Found), Possible Web Application Scan/Directory Guessing Attack
RT	11	2019-12-25 06:29...	139.199.184.166	59314	10.12.25.101	80	6	ET CURRENT_EVENTS Jembot PHP Webshell (hell.php)
RT	75	2019-12-25 06:29...	139.199.184.166	61288	10.12.25.101	80	6	ET WEB_SERVER ThinkPHP RCE Exploitation Attempt
RT	41	2019-12-25 06:34...	10.12.25.101	80	139.199.184.166	65134	6	SURICATA HTTP unable to match response to request
RT	17	2019-12-25 06:42...	10.12.25.101	80	139.199.184.166	58175	6	GPL WEB_SERVER 403 Forbidden
RT	2	2019-12-25 06:45...	139.199.184.166	52375	10.12.25.101	80	6	ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)

Considering the alerts provided by the blue team, some of the events have been marked with specific indications to inform the category of risk. This is further given with specific instructions and are divided into -

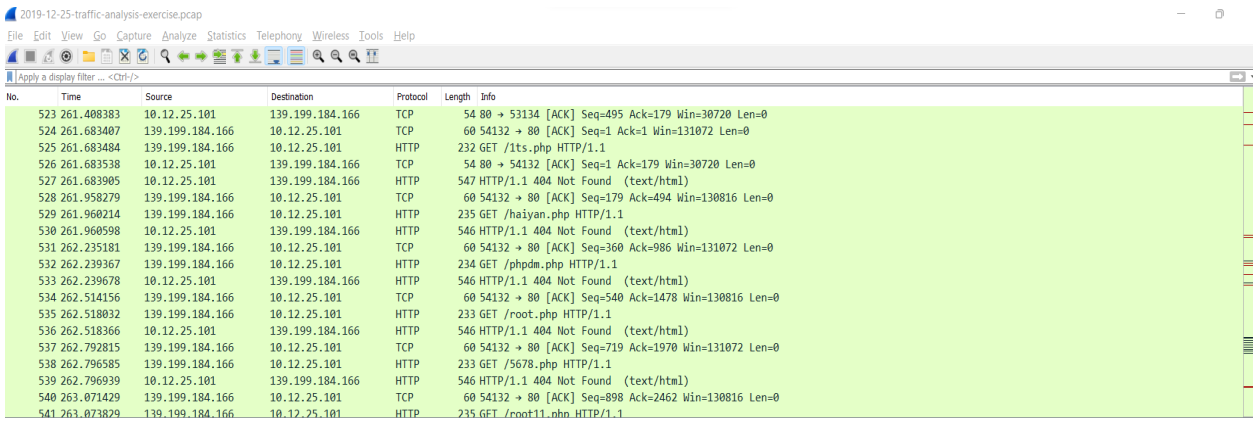
- **ST**
- **CNT**
- **DATE/TIME**
- **SrcIP**
- **SPort**
- **DstIP**
- **DPort**
- **Event Message**

  Looking at the alerts and the event messages, the packet capture (Pcap) has the required information to functionally monitor and resolve this certain incident.

ANALYSIS OF THE PCAP -

INCIDENT - #BLTM31468500

The incident has been reported after reviewing the alerts and determining its severity.



2019-12-25-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
523	261.408383	10.12.25.101	139.199.184.166	TCP	54	80 → 53134 [ACK] Seq=495 Ack=179 Win=30720 Len=0
524	261.683407	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
525	261.683484	139.199.184.166	10.12.25.101	HTTP	232	GET /1ts.php HTTP/1.1
526	261.683538	10.12.25.101	139.199.184.166	TCP	54	80 → 54132 [ACK] Seq=1 Ack=179 Win=30720 Len=0
527	261.683905	10.12.25.101	139.199.184.166	HTTP	547	HTTP/1.1 404 Not Found (text/html)
528	261.958279	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=179 Ack=494 Win=130816 Len=0
529	261.960214	139.199.184.166	10.12.25.101	HTTP	235	GET /haiyan.php HTTP/1.1
530	261.960598	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
531	262.235181	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=360 Ack=986 Win=131072 Len=0
532	262.239367	139.199.184.166	10.12.25.101	HTTP	234	GET /phpdm.php HTTP/1.1
533	262.239678	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
534	262.514156	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=540 Ack=1478 Win=130816 Len=0
535	262.518032	139.199.184.166	10.12.25.101	HTTP	233	GET /root.php HTTP/1.1
536	262.518366	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
537	262.792815	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=719 Ack=1970 Win=131072 Len=0
538	262.796585	139.199.184.166	10.12.25.101	HTTP	233	GET /5678.php HTTP/1.1
539	262.796939	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
540	263.071429	139.199.184.166	10.12.25.101	TCP	60	54132 → 80 [ACK] Seq=898 Ack=2462 Win=130816 Len=0
541	263.073829	139.199.184.166	10.12.25.101	HTTP	235	GET /root11.php HTTP/1.1

ARTIFACT LISTING -

The artifact listing consists of several details of information including -

- Time
- Source IP
- Destination IP
- Protocol
- Length
- Information

  These are also further listed with certain key details of each and every packet and can be analyzed through systematic procedures. These also include some information such as frames, Ethernet II, Internet Protocol version 4, and TCP.

ACTIONS TAKEN -

Actions taken for the particular incident are to be resolved with specific team which are to be notified. Some of the functionalities provided with these are -

1. **Assemble the team -**

   The SOC team or managed security consultancies are sufficient for handling this specific occurrence in firms where the threat isn't as serious. However, these should be merged to include specific corporate communications and human resources for more specific occurrences.

   if an organization-wide security incident response team (CSIRT) is established. A wide range of pre-designed technical specialists would be introduced into the businesses as a result.

2. **Contain and Recover -**

   The security event is comparable to a variety of exploits used at other organizations. Once these are found and the source is aware of the incident, the damage is evaluated and the necessary steps are taken to fix the problem. With the infected viruses and other malware, this would also require the organization to deploy security patches. Additionally, this would include changing the system passwords and blocking certain outside accounts that may have been responsible for the event.

   - To certify all systems as functioning, perform system and network validation and testing.
   - Any component that was compromised should be recertified as secure and operational.

Some of the other steps to be taken into consideration are -

- **Detect and ascertain the source.**
- **Assess damage and severity.**
- **Begin notification process.**
- **Take actions to prevent the same type of incident in the future.**

ANALYSIS -

The analysis of the PCAP file has produced some desirable results, which are to be monitored and can be remedied.

PACKET	DIRECTION	DESCRIPTION
1	139.199.184.166 -> 10.12.25.101	By the GPL web server, a http request for a certain text file is opted.
2	139.199.184.166 -> 10.12.25.101	A remote code execution through the backdoor is performed.
3	139.199.184.166 -> 10.12.25.101	A phpinfo access leads to the login page of the current directory in the network.
4	139.199.184.166 -> 10.12.25.101	A browser detection using a user agent is performed to determine the authenticity of the request.

Each of the specific connection is listed with certain end points and these can be achieved through -

Statistics -> endpoints in Wireshark to obtain the connection requests and analyze them for further results.

Wireshark · Endpoints · 2019-12-25-traffic-analysis-exercise.pcap

Endpoint Settings

- [ ] Name resolution
- [ ] Limit to display filter

Copy

Map

Protocol
[ ] Bluetooth
[ ] DCCP
[x] Ethernet
[ ] FC
[ ] FDDI
[ ] IEEE 802.11
[ ] IEEE 802.15.4
[x] IPv4
[x] IPv6
[ ] IPX
[ ] JXTA
[ ] MPTCP
[ ] NCP

Filter list for specific type

Ethernet · 4 | IPv4 · 2 | IPv6 | TCP · 82 | UDP

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.12.25.101	80	2.369 KiB	594.691 KiB	906 bytes	349.137 KiB	1.484 KiB	245.555 KiB
10.12.25.101	8080	6 bytes	346 bytes	3 bytes	162 bytes	3 bytes	184 bytes
10.12.25.101	8983	6 bytes	346 bytes	3 bytes	162 bytes	3 bytes	184 bytes
139.199.184.166	50137	10 bytes	1.348 KiB	6 bytes	659 bytes	4 bytes	721 bytes
139.199.184.166	50555	3 bytes	188 bytes	2 bytes	122 bytes	1 bytes	66 bytes
139.199.184.166	50940	28 bytes	6.528 KiB	17 bytes	3.053 KiB	11 bytes	3.476 KiB
139.199.184.166	50984	35 bytes	7.854 KiB	22 bytes	2.831 KiB	13 bytes	5.022 KiB
139.199.184.166	51031	10 bytes	1.244 KiB	6 bytes	553 bytes	4 bytes	721 bytes
139.199.184.166	51046	3 bytes	188 bytes	2 bytes	122 bytes	1 bytes	66 bytes
139.199.184.166	51050	37 bytes	9.326 KiB	23 bytes	4.251 KiB	14 bytes	5.075 KiB
139.199.184.166	51249	3 bytes	188 bytes	2 bytes	122 bytes	1 bytes	66 bytes
139.199.184.166	51805	28 bytes	6.017 KiB	17 bytes	2.061 KiB	11 bytes	3.956 KiB
139.199.184.166	52315	89 bytes	25.126 KiB	56 bytes	10.881 KiB	33 bytes	14.245 KiB
139.199.184.166	52340	10 bytes	1.344 KiB	5 bytes	601 bytes	5 bytes	775 bytes
139.199.184.166	52354	43 bytes	11.762 KiB	28 bytes	5.192 KiB	15 bytes	6.569 KiB
139.199.184.166	52375	52 bytes	11.941 KiB	30 bytes	4.223 KiB	22 bytes	7.719 KiB
139.199.184.166	52505	24 bytes	6.004 KiB	16 bytes	2.687 KiB	8 bytes	3.317 KiB
139.199.184.166	52677	45 bytes	12.556 KiB	30 bytes	5.506 KiB	15 bytes	7.050 KiB
139.199.184.166	52711	6 bytes	346 bytes	3 bytes	184 bytes	3 bytes	162 bytes
139.199.184.166	52943	15 bytes	2.811 KiB	8 bytes	1,011 bytes	7 bytes	1.823 KiB
139.199.184.166	53134	11 bytes	1.277 KiB	6 bytes	533 bytes	5 bytes	775 bytes
139.199.184.166	53268	6 bytes	346 bytes	3 bytes	184 bytes	3 bytes	162 bytes
139.199.184.166	53737	9 bytes	1.293 KiB	5 bytes	603 bytes	4 bytes	721 bytes
139.199.184.166	53864	25 bytes	6.842 KiB	16 bytes	2.991 KiB	9 bytes	3.851 KiB
139.199.184.166	53874	10 bytes	1.348 KiB	6 bytes	659 bytes	4 bytes	721 bytes
139.199.184.166	53988	17 bytes	3.277 KiB	10 bytes	1.454 KiB	7 bytes	1.823 KiB
139.199.184.166	54132	32 bytes	7.140 KiB	20 bytes	2.650 KiB	12 bytes	4.489 KiB
139.199.184.166	54484	43 bytes	10.950 KiB	27 bytes	4.809 KiB	16 bytes	6.142 KiB

ANALYZATION OF TCP SYN TRAFFIC -

perspective of the transmission control protocol, or TCP. This gives details about the port numbers. These are also useful for keeping track of the flag values. Additionally, SYN, which is enabled, displays the first phase of the TCP three-way handshake.

This is further provided with the display filter, "tcp.port == 80."

2019-12-25-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	139.199.184.166	10.12.25.101	TCP	62	55376 → 80 [SYN] Seq=0 Win=8192 Len=0 WS=256 SACK_PERM
2	0.000086	10.12.25.101	139.199.184.166	TCP	66	80 → 55376 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=1024
3	1.295311	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	1.295354	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131072 Len=0
5	1.295671	10.12.25.101	139.199.184.166	TCP	54	80 → 55376 [FIN, ACK] Seq=1 Ack=2 Win=29696 Len=0
6	1.562685	139.199.184.166	10.12.25.101	TCP	60	55376 → 80 [ACK] Seq=2 Ack=2 Win=131072 Len=0
7	3.404851	139.199.184.166	10.12.25.101	TCP	62	55812 → 80 [SYN] Seq=0 Win=8192 Len=0 WS=256 SACK_PERM
8	3.404946	10.12.25.101	139.199.184.166	TCP	66	80 → 55812 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=1024
9	3.672453	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
10	3.672504	139.199.184.166	10.12.25.101	HTTP	283	GET / HTTP/1.1
11	3.672579	10.12.25.101	139.199.184.166	TCP	54	80 → 55812 [ACK] Seq=1 Ack=230 Win=30720 Len=0
12	3.673146	10.12.25.101	139.199.184.166	HTTP	830	HTTP/1.1 200 OK (text/html)
13	3.940236	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=230 Ack=537 Win=131072 Len=0
14	3.940275	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=230 Ack=777 Win=131072 Len=0
15	3.952125	139.199.184.166	10.12.25.101	HTTP	293	GET /robots.txt HTTP/1.1
16	3.952708	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)
17	4.219994	139.199.184.166	10.12.25.101	TCP	60	55812 → 80 [ACK] Seq=469 Ack=1269 Win=131072 Len=0
18	4.220781	139.199.184.166	10.12.25.101	HTTP	350	POST /Admin1f768268/Login.php HTTP/1.1 (application/x-www-form-urlencoded)
19	4.221104	10.12.25.101	139.199.184.166	HTTP	546	HTTP/1.1 404 Not Found (text/html)

With the current traffic and the alerts chosen, it can be clearly seen as a backdoor operation for a false user agent browser. The attackers have implemented a guess, which further led to the alert for the 404/directory remote code execution attack, which has been performed through the source of the IP 139.199.184.166 -> 10.12.25.101. In this case, the further http requests have been matched to the responses, and the GBP server has responded with a forbidden request. This is further shifted to the exploit. The open source content management system has been implemented in the organization to effectively discard the services, and often these attacks are performed through serialized session encoding.

CONCLUSION :

These organizations are able to define these countermeasures in advance through a thorough incident response. There are numerous ways to reduce the impact of this tragedy. Preparation, detection and analysis, containment, eradication, recovery, and post-incident audits are among the six incident response procedures that NIST recommends, and they are also generally accepted by the majority of security experts in businesses.

The organization has used a combination of assessment checklists to determine the essential preparation functionalities. comprehensive incident response plans as well as other guidelines and playbooks that would automate system and network activities.

Further this incident would be reassigned to the IT network team for further analysis and detailed specifications for the report.