

Sunucu Tabanlı Saldırı Tespit Sistemi - idsPy

Yasin Seven

Özet

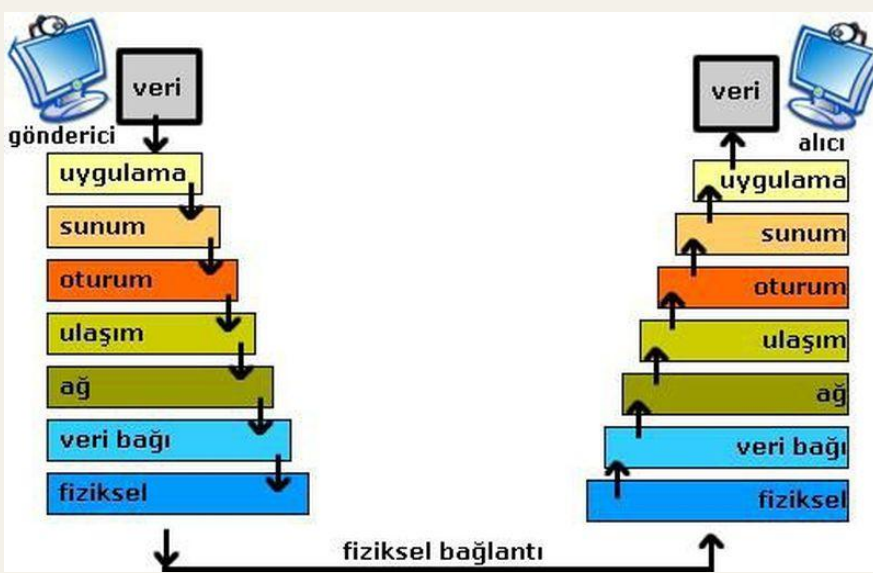
idsPy, izlenecek ağ üzerinde bir sunucu üzerine kurularak yönlendirilen ağ trafiğindeki her bir paketin içeriğini kullanıcı tarafından yazılan kurallara göre inceleyerek tehdit gördüğü takdirde alarm üreten bir siber güvenlik sistemidir.

Kurulan sunucuya diğer kullanıcılar ve yöneticiler aynı ağa bağlı herhangi bir bilgisayar veya telefondan erişim sağlayıp sistemi kullanabilir. Sistemin web arayüzü responsive olarak çoğu cihaza uygun şekilde tasarlanmıştır.

Yazılan kurallara göre tespit edilen paketler sunucu üzerinde bulunan veritabanına tüm bilgileriyle ve zaman damgasıyla kaydedilir. Veritabanındaki paketler web arayüzündeki tüm bilgileri sağlamak amacıyla dinamik olarak web arayüzüne aktarılır. Yakalanan paketler alarm olarak bir liste şeklinde paket bilgileriyle sistemden sorumlu analistin önüne düşer, burada incelenen paketler eğer normal bir trafikse ve saldırı değilse arşive gönderilerek alarm yok sayılır.

Giriş

idsPy'nin nasıl çalıştığını anlamak için öncelikle internetin nasıl çalıştığını anlamalıyız. İnternet basitçe bir cihazda oluşturulan verilerin küçük paketler haline getirilerek (text dosyaları gibi düşünebilirsiniz) diğer cihaza iletildikten sonra aynı sırayla tekrar açılması ve birleştirilmesi ile sağlanır. Aşağıdaki görselde bu iletişimin katmanlarını görebilirsiniz.



Bu paketler bilgisayarımızda aşağıdaki şekilde görselleştirilerek Wireshark programı aracılığıyla izlenebilir. Bu tip programlara ağ izleme programları (Packet Sniffer) denir.

No.	Tipo	Sıra	Hedef	Protokol	Uzunluk	İfade
87	54	612941	192.168.1.1	500	549	HTTP/1.1
88	54	612942	192.168.1.1	500	488	HTTP/1.1
89	54	612943	192.168.1.1	500	527	HTTP/1.1
90	54	612944	192.168.1.1	500	527	HTTP/1.1
91	54	612945	192.168.1.1	500	527	HTTP/1.1
92	54	612946	192.168.1.1	500	527	HTTP/1.1
93	54	612947	192.168.1.1	500	527	HTTP/1.1
94	54	612948	192.168.1.1	500	527	HTTP/1.1
95	54	612949	192.168.1.1	500	527	HTTP/1.1
96	54	612950	192.168.1.1	500	527	HTTP/1.1
97	54	612951	192.168.1.1	500	527	HTTP/1.1
98	54	612952	192.168.1.1	500	527	HTTP/1.1
99	54	612953	192.168.1.1	500	527	HTTP/1.1
100	54	612954	192.168.1.1	500	527	HTTP/1.1
101	54	612955	192.168.1.1	500	527	HTTP/1.1
102	54	612956	192.168.1.1	500	527	HTTP/1.1
103	54	612957	192.168.1.1	500	527	HTTP/1.1
104	54	612958	192.168.1.1	500	527	HTTP/1.1
105	54	612959	192.168.1.1	500	527	HTTP/1.1
106	54	612960	192.168.1.1	500	527	HTTP/1.1
107	54	612961	192.168.1.1	500	527	HTTP/1.1
108	54	612962	192.168.1.1	500	527	HTTP/1.1
109	54	612963	192.168.1.1	500	527	HTTP/1.1
110	54	612964	192.168.1.1	500	527	HTTP/1.1
111	54	612965	192.168.1.1	500	527	HTTP/1.1
112	54	612966	192.168.1.1	500	527	HTTP/1.1
113	54	612967	192.168.1.1	500	527	HTTP/1.1
114	54	612968	192.168.1.1	500	527	HTTP/1.1
115	54	612969	192.168.1.1	500	527	HTTP/1.1
116	54	612970	192.168.1.1	500	527	HTTP/1.1
117	54	612971	192.168.1.1	500	527	HTTP/1.1
118	54	612972	192.168.1.1	500	527	HTTP/1.1
119	54	612973	192.168.1.1	500	527	HTTP/1.1
120	54	612974	192.168.1.1	500	527	HTTP/1.1
121	54	612975	192.168.1.1	500	527	HTTP/1.1
122	54	612976	192.168.1.1	500	527	HTTP/1.1
123	54	612977	192.168.1.1	500	527	HTTP/1.1
124	54	612978	192.168.1.1	500	527	HTTP/1.1
125	54	612979	192.168.1.1	500	527	HTTP/1.1
126	54	612980	192.168.1.1	500	527	HTTP/1.1
127	54	612981	192.168.1.1	500	527	HTTP/1.1
128	54	612982	192.168.1.1	500	527	HTTP/1.1
129	54	612983	192.168.1.1	500	527	HTTP/1.1
130	54	612984	192.168.1.1	500	527	HTTP/1.1
131	54	612985	192.168.1.1	500	527	HTTP/1.1
132	54	612986	192.168.1.1	500	527	HTTP/1.1
133	54	612987	192.168.1.1	500	527	HTTP/1.1
134	54	612988	192.168.1.1	500	527	HTTP/1.1
135	54	612989	192.168.1.1	500	527	HTTP/1.1
136	54	612990	192.168.1.1	500	527	HTTP/1.1
137	54	612991	192.168.1.1	500	527	HTTP/1.1
138	54	612992	192.168.1.1	500	527	HTTP/1.1
139	54	612993	192.168.1.1	500	527	HTTP/1.1
140	54	612994	192.168.1.1	500	527	HTTP/1.1
141	54	612995	192.168.1.1	500	527	HTTP/1.1
142	54	612996	192.168.1.1	500	527	HTTP/1.1
143	54	612997	192.168.1.1	500	527	HTTP/1.1
144	54	612998	192.168.1.1	500	527	HTTP/1.1
145	54	612999	192.168.1.1	500	527	HTTP/1.1
146	54	613000	192.168.1.1	500	527	HTTP/1.1
147	54	613001	192.168.1.1	500	527	HTTP/1.1
148	54	613002	192.168.1.1	500	527	HTTP/1.1
149	54	613003	192.168.1.1	500	527	HTTP/1.1
150	54	613004	192.168.1.1	500	527	HTTP/1.1
151	54	613005	192.168.1.1	500	527	HTTP/1.1
152	54	613006	192.168.1.1	500	527	HTTP/1.1
153	54	613007	192.168.1.1	500	527	HTTP/1.1
154	54	613008	192.168.1.1	500	527	HTTP/1.1
155	54	613009	192.168.1.1	500	527	HTTP/1.1
156	54	613010	192.168.1.1	500	527	HTTP/1.1
157	54	613011	192.168.1.1	500	527	HTTP/1.1
158	54	613012	192.168.1.1	500	527	HTTP/1.1
159	54	613013	192.168.1.1	500	527	HTTP/1.1
160	54	613014	192.168.1.1	500	527	HTTP/1.1
161	54	613015	192.168.1.1	500	527	HTTP/1.1
162	54	613016	192.168.1.1	500	527	HTTP/1.1
163	54	613017	192.168.1.1	500	527	HTTP/1.1
164	54	613018	192.168.1.1	500	527	HTTP/1.1
165	54	613019	192.168.1.1	500	527	HTTP/1.1
166	54	613020	192.168.1.1	500	527	HTTP/1.1
167	54	613021	192.168.1.1	500	527	HTTP/1.1
168	54	613022	192.168.1.1	500	527	HTTP/1.1
169	54	613023	192.168.1.1	500	527	HTTP/1.1
170	54	613024	192.168.1.1	500	527	HTTP/1.1
171	54	613025	192.168.1.1	500	527	HTTP/1.1
172	54	613026	192.168.1.1	500	527	HTTP/1.1
173	54	613027	192.168.1.1	500	527	HTTP/1.1
174	54	613028	192.168.1.1	500	527	HTTP/1.1
175	54	613029	192.168.1.1	500	527	HTTP/1.1
176	54	613030	192.168.1.1	500	527	HTTP/1.1
177	54	613031	192.168.1.1	500	527	HTTP/1.1
178	54	613032	192.168.1.1	500	527	HTTP/1.1
179	54	613033	192.168.1.1	500	527	HTTP/1.1
180	54	613034	192.168.1.1	500	527	HTTP/1.1
181	54	613035	192.168.1.1	500	527	HTTP/1.1
182	54	613036	192.168.1.1	500	527	HTTP/1.1
183	54	613037	192.168.1.1	500	527	HTTP/1.1
184	54	613038	192.168.1.1	500	527	HTTP/1.1
185	54	613039	192.168.1.1	500	527	HTTP/1.1
186	54	613040	192.168.1.1	500	527	HTTP/1.1
187	54	613041	192.168.1.1	500	527	HTTP/1.1
188	54	613042	192.168.1.1	500	527	HTTP/1.1
189	54	613043	192.168.1.1	500	527	HTTP/1.1
190	54	613044	192.168.1.1	500	527	HTTP/1.1
191	54	613045	192.168.1.1	500	527	HTTP/1.1
192	54	613046	192.168.1.1	500	527	HTTP/1.1
193	54	613047	192.168.1.1	500	527	HTTP/1.1
194	54	613048	192.168.1.1	500	527	HTTP/1.1
195	54	613049	192.168.1.1	500	527	HTTP/1.1
196	54	613050	192.168.1.1	500	527	HTTP/1.1
197	54	613051	192.168.1.1	500	527	HTTP/1.1
198	54	613052	192.168.1.1	500	527	HTTP/1.1
199	54	613053	192.168.1.1	500	527	HTTP/1.1
200	54	613054	192.168.1.1	500	527	HTTP/1.1
201	54	613055	192.168.1.1	500	527	HTTP/1.1
202	54	613056	192.168.1.1	500	527	HTTP/1.1
203	54	613057	192.168.1.1	500	527	HTTP/1.1
204	54	613058	192.168.1.1	500	527	HTTP/1.1
205	54	613059	192.168.1.1	500	527	HTTP/1.1
206	54	613060	192.168.1.1	500	527	HTTP/1.1
207	54	613061	192.168.1.1	500	527	HTTP/1.1
208	54	613062	192.168.1.1	500	527	HTTP/1.1
209	54	613063	192.168.1.1	500	527	HTTP/1.1
210	54	613064	192.168.1.1	500	527	HTTP/1.1
211	54	613065	192.168.1.1	500	527	HTTP/1.1
212	54	613066	192.168.1.1	500	527	HTTP/1.1
213	54	613067	192.168.1.1	500	527	HTTP/1.1
214	54	613068	192.168.1.1	500	527	HTTP/1.1
215	54	613069	192.168.1.1	500	527	HTTP/1.1
216	54	613070	192.168.1.1	500	527	HTTP/1.1
217	54	613071	192.168.1.1	500	527	HTTP/1.1
218	54	613072	192.168.1.1	500	527	HTTP/1.1
219	54	613073	192.168.1.1	500	527	HTTP/1.1
220	54	613074	192.168.1.1	500	527	HTTP/1.1
221	54	613075	192.168.1.1	500	527	HTTP/1.1
222	54	613076	192.168.1.1	500	527	HTTP/1.1
223	54	613077	192.168.1.1	500	527	HTTP/1.1
224	54	613078	192.168.1.1	500	527	HTTP/1.1
225	54	613079	192.168.1.1	500	527	HTTP/1.1
226	54	613080	192.168.1.1	500	527	HTTP/1.1
227	54	613081	192.168.1.1	500	527	HTTP/1.1
228	54	613082	192.168.1.1	500	527	HTTP/1.1
229	54	613083	192.168.1.1	500	527	HTTP/1.1
230	54	613084	192.168.1.1	500	527	HTTP/1.1
231	54	613085	192.168.1.1	500	527	HTTP/1.1
232	54	613086	192.168.1.1	500	527	HTTP/1.1
233	54	613087	192.168.1.1	500	527	HTTP/1.1
234	54	613088	192.168.1.1	500	527	HTTP/1.1
235	54	613089	192.168.1.1	500	527	HTTP/1.1
236	54	613090	192.168.1.1	500	527	HTTP/1.1
237	54	613091	192.168.1.1	500	527	HTTP/1.1
238	54	613092	192.168.1.1	500	527	HTTP/1.1
239	54	613093	192.168.1.1	500	527	HTTP/1.1
240	54	613094	192.168.1.1	500	527	HTTP/1.1
241	54	613095	192.168.1.1	500	527	HTTP/1.1
242	54	613096	192.168.1.1	500	527	HTTP/1.1
243	54	613097	192.168.1.1	500	527	HTTP/1.1
244	54	613098	192.168.1.1	500	527	HTTP/1.1
245	54	613099	192.168.1.1	500	527	HTTP/1.1
246	54	613100	192.168.1.1	500	527	HTTP/1.1
247	54	613101	192.168.1.1	500	527	HTTP/1.1
248	54	613102	192.168.1.1	500	527	HTTP/1.1
249	54	613103	192.168.1.1	500	527	HTTP/1.1
250	54	613104	192.168.1.1	500	527	HTTP/1.1
251	54	613105	192.168.1.1	500	527	HTTP/1.1
252	54	613106	192.168.1.1	500	527	HTTP/1.1
253	54	613107	192.168.1.1	500	527	HTTP/1.1
254	54	613108	192.168.1.1	500	527	HTTP/1.1
255	54	613109	192.168.1.1	500	527	HTTP/1.1
256	54	613110	192.168.1.1	500	527	HTTP/1.1
257	54	613111	192.168.1.1	500	527	HTTP/1.1
258	54	613112	192.			