Практическое задание. NIPS/NIDS: Snort

1. Уведомления при переходе на yandex.ru

```
Acquiring network traffic from "wlp2s0".
Reload thread starting...
Reload thread started, thread 0x7f1ccfcda640 (17901)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=17892)
12/02-15:42:07.513293  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:38004 -> 77.88.55.60:443
12/02-15:42:07.761283  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:40156 -> 5.255.255.77:443
12/02-15:42:09.977155  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:40164 -> 5.255.255.77:443
12/02-15:42:11.771410  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:35724 -> 93.158.134.119:443
12/02-15:42:12.559356  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 87.250.251.92:443 -> 192.168.0.106:42102
12/02-15:42:12.799265  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 87.250.251.92:443 -> 192.168.0.106:42104
12/02-15:42:13.208954  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:38012 -> 77.88.55.60:443
12/02-15:42:13.250189  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:38022 -> 77.88.55.60:443
12/02-15:42:16.801126  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:54916 -> 213.180.193.90:443
12/02-15:42:17.292395  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:57230 -> 93.158.134.90:443
12/02-15:42:17.411276  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:44040 -> 87.250.254.45:443
12/02-15:42:17.510850  [**] [1:12312313:0] Someone open yandex website [**] [Priority: 0] {TCP} 192.168.0.106:57236 -> 93.158.134.90:443
```

2. Уведомления при NULL-сканировании

```
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
Commencing packet processing (pid=19168)
12/02-17:54:43.384748  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:3306
12/02-17:54:43.384893  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:22
12/02-17:54:43.384932  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:1720
12/02-17:54:43.384962  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:113
12/02-17:54:43.384997  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:25
12/02-17:54:43.385027  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:443
12/02-17:54:43.385059  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:135
12/02-17:54:43.385087  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:111
12/02-17:54:43.385122  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:445
12/02-17:54:43.385199  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:53
12/02-17:54:43.385477  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:3389
12/02-17:54:43.385626  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:256
12/02-17:54:43.385731  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:8888
12/02-17:54:43.385832  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:23
12/02-17:54:43.385921  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:1723
12/02-17:54:43.386023  [**] [1:322222:0] NULL Scan [**] [Priority: 0] {TCP} 192.168.0.104:36623 -> 192.168.0.106:110
```

3. Уведомления при атаке EternalBlue

```
12/02-18:54:05.729096  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.0.104:45375 -> 192.168.0.101
:445
12/02-18:54:05.874399  [**] [1:2465:7] NETBIOS SMB-DS IPC$ share access [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.0.104:41513 -> 192.168.0.101
:445
```