SEC599 | DEFEATING ADVANCED ADVERSARIES

599.6

APT Defender Capstone

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

Copyright © 2017, Erik Van Buggenhout & Stephen Sims. All rights reserved to Erik Van Buggenhout & Stephen Sims and/or SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND THE SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, the SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by the SANS Institute to the User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO THE SANS INSTITUTE, AND THAT THE SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND), SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to the SANS Institute for a full refund, if applicable.

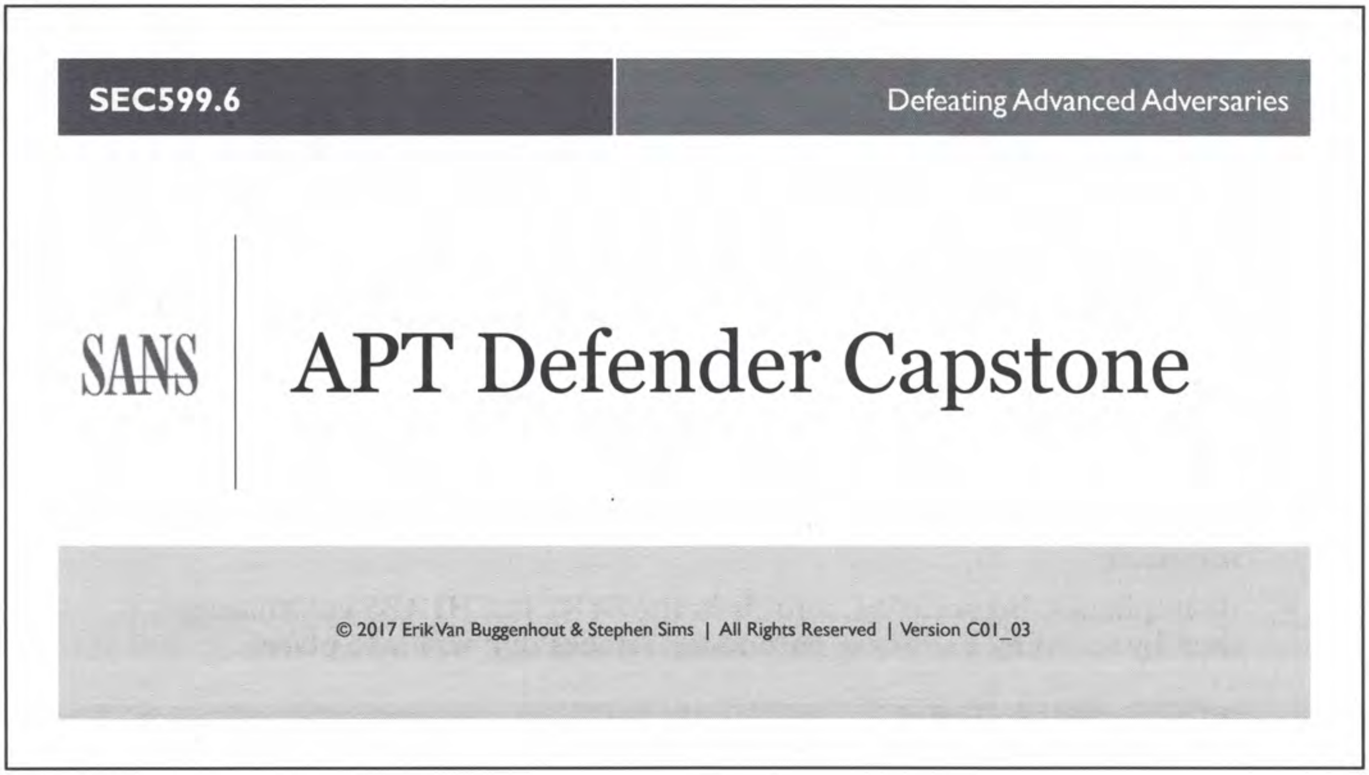
User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of the SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of the SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.



SEC599.6

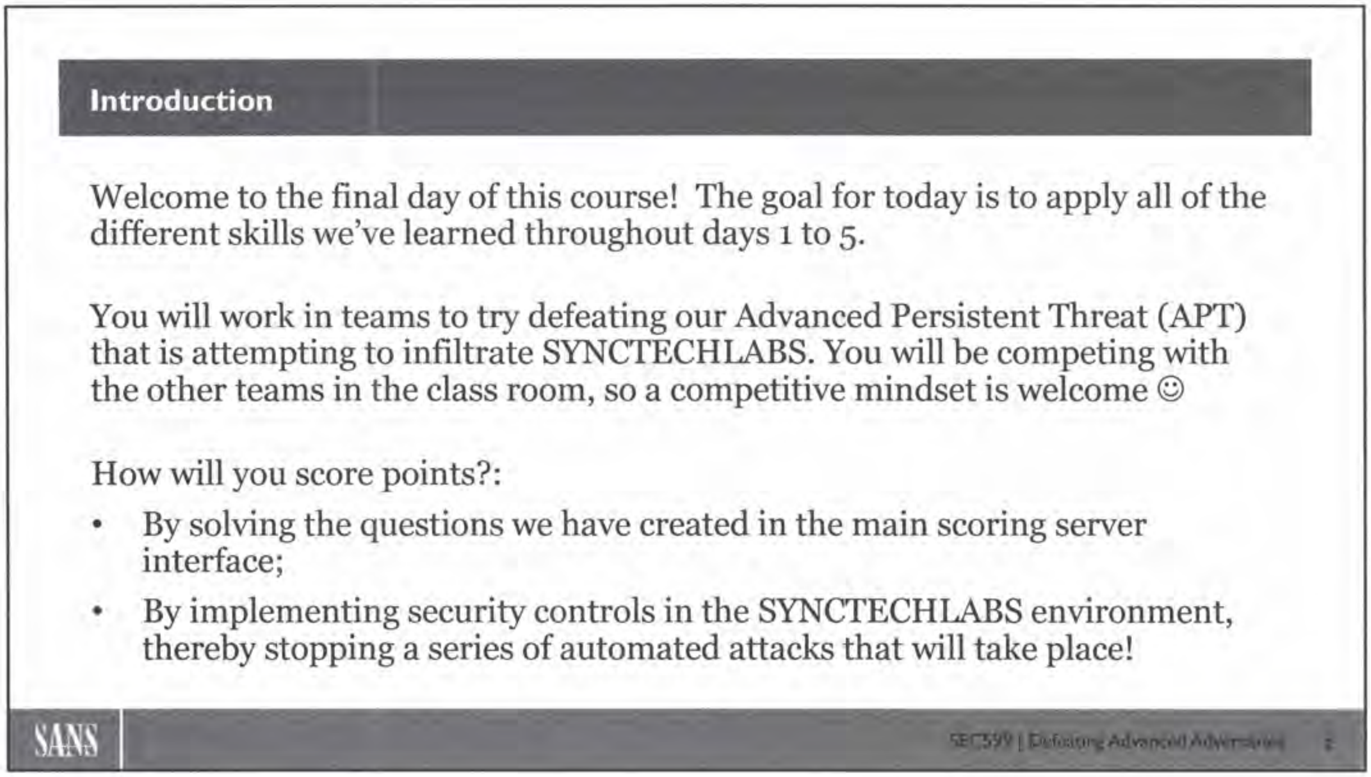
Defeating Advanced Adversaries

SANS

APT Defender Capstone

© 2017 Erik Van Buggenhout & Stephen Sims | All Rights Reserved | Version C01_03

This page intentionally left blank.



Introduction

Welcome to the final day of this course! The goal for today is to apply all of the different skills we've learned throughout days 1 to 5.

You will work in teams to try defeating our Advanced Persistent Threat (APT) that is attempting to infiltrate SYNCTECHLABS. You will be competing with the other teams in the class room, so a competitive mindset is welcome ☺

How will you score points?:

- By solving the questions we have created in the main scoring server interface;
- By implementing security controls in the SYNCTECHLABS environment, thereby stopping a series of automated attacks that will take place!

SANS

Introduction

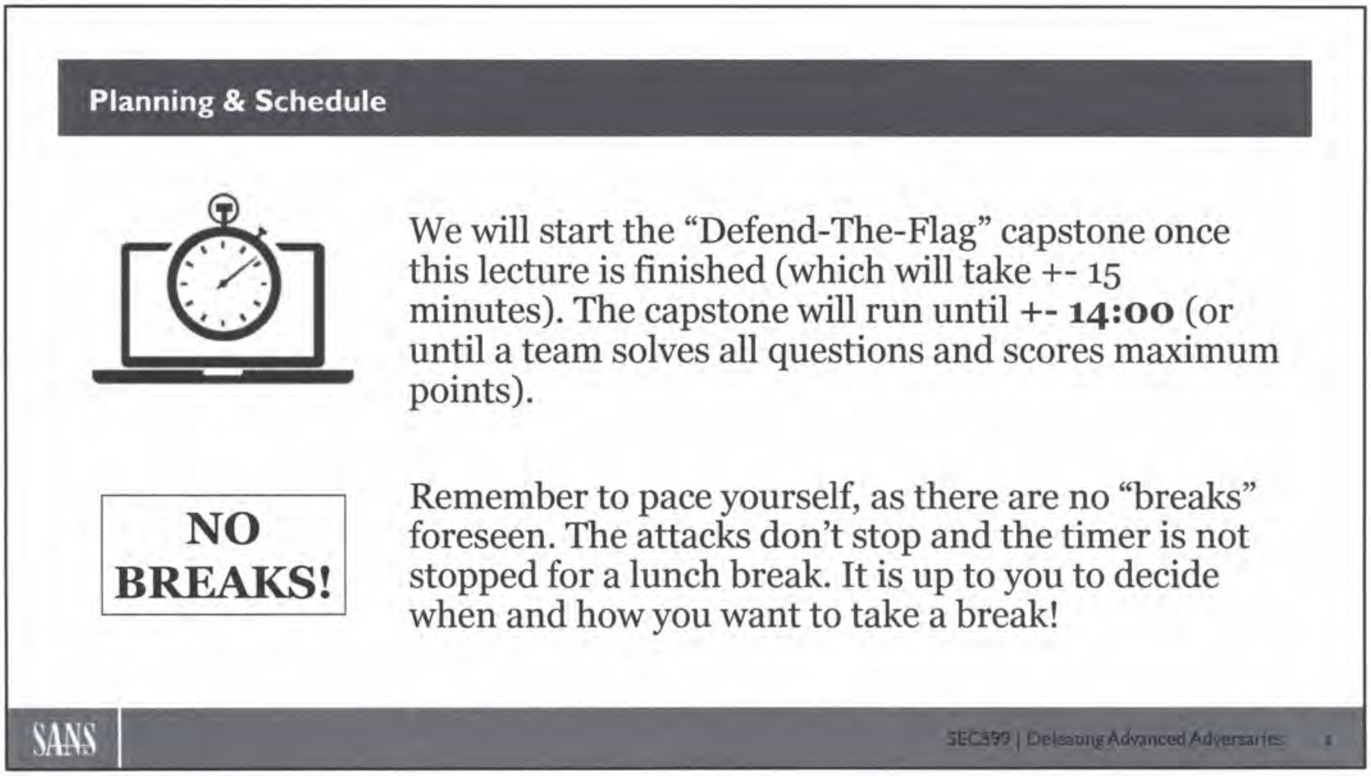
Welcome to the final day of this course! The goal for today is to apply all of the different skills we've learned throughout days 1 to 5.

You will work in teams to try defeating our Advanced Persistent Threat (APT) that is attempting to infiltrate SYNCTECHLABS. You will be competing with the other teams in the classroom, so a competitive mindset is welcome ☺

How will you score points?:

- By solving the questions we have created in the main scoring server interface;
- By implementing security controls in the SYNCTECHLABS environment, thereby stopping a series of automated attacks that will take place!

© 2017 Erik Van Buggenhout & Stephen Sims



Planning & Schedule

We will start the "Defend-The-Flag" capstone once this lecture is finished (which will take +- 15 minutes). The capstone will run until **+- 14:00** (or until a team solves all questions and scores maximum points).

NO BREAKS!

Remember to pace yourself, as there are no "breaks" foreseen. The attacks don't stop and the timer is not stopped for a lunch break. It is up to you to decide when and how you want to take a break!

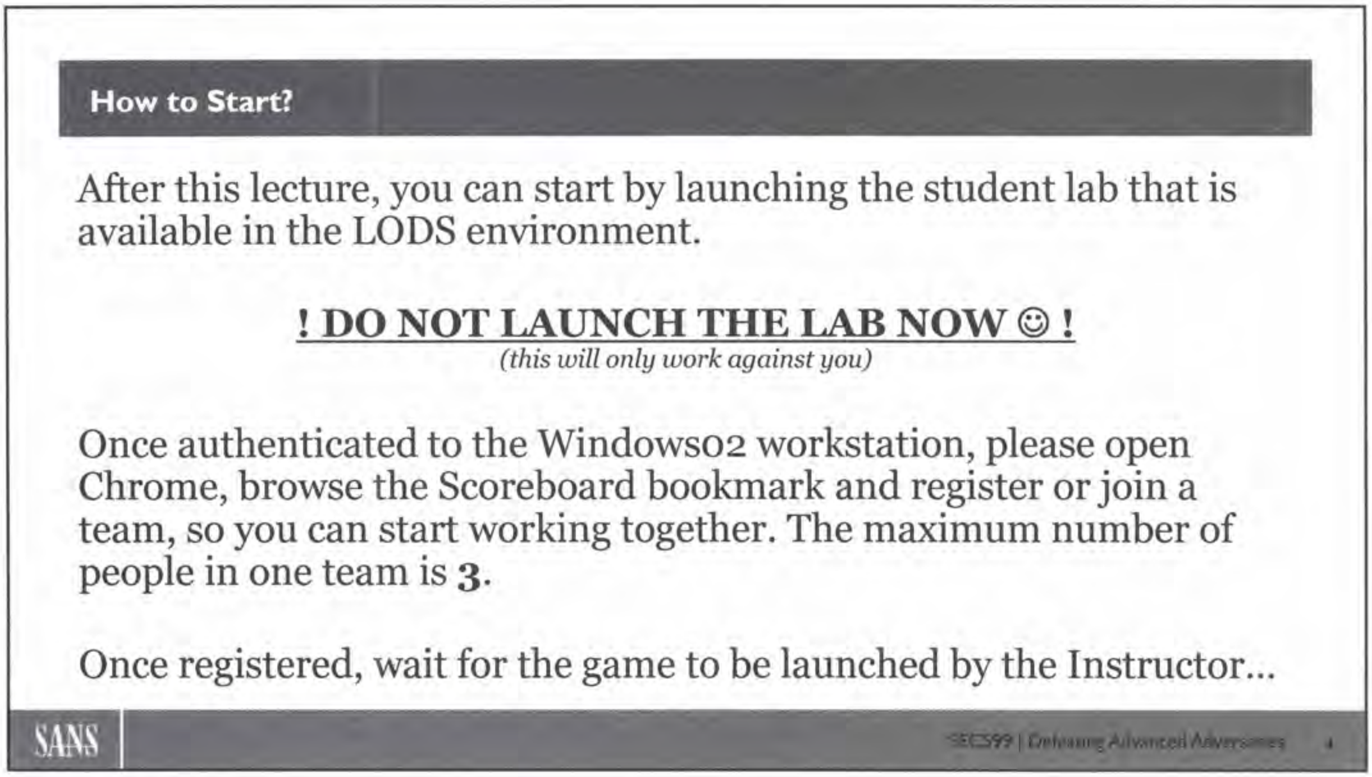
SANS

SEC599 | Defeating Advanced Adversaries 3

Planning & Schedule
We will start the "Defend-The-Flag" capstone once this lecture is finished (which will take +- 15 minutes). The capstone will run until +- 14:00 (or until a team solves all questions and scores maximum points).

Remember to pace yourself, as there are no "breaks" foreseen. The attacks don't stop and the timer is not stopped for a lunch break. It is up to you to decide when and how you want to take a break!

© 2017 Erik Van Buggenhout & Stephen Sims



How to Start?

After this lecture, you can start by launching the student lab that is available in the LODS environment.

! DO NOT LAUNCH THE LAB NOW ☺ !

(this will only work against you)

Once authenticated to the Windows02 workstation, please open Chrome, browse the Scoreboard bookmark and register or join a team, so you can start working together. The maximum number of people in one team is **3**.

Once registered, wait for the game to be launched by the Instructor...

SANS

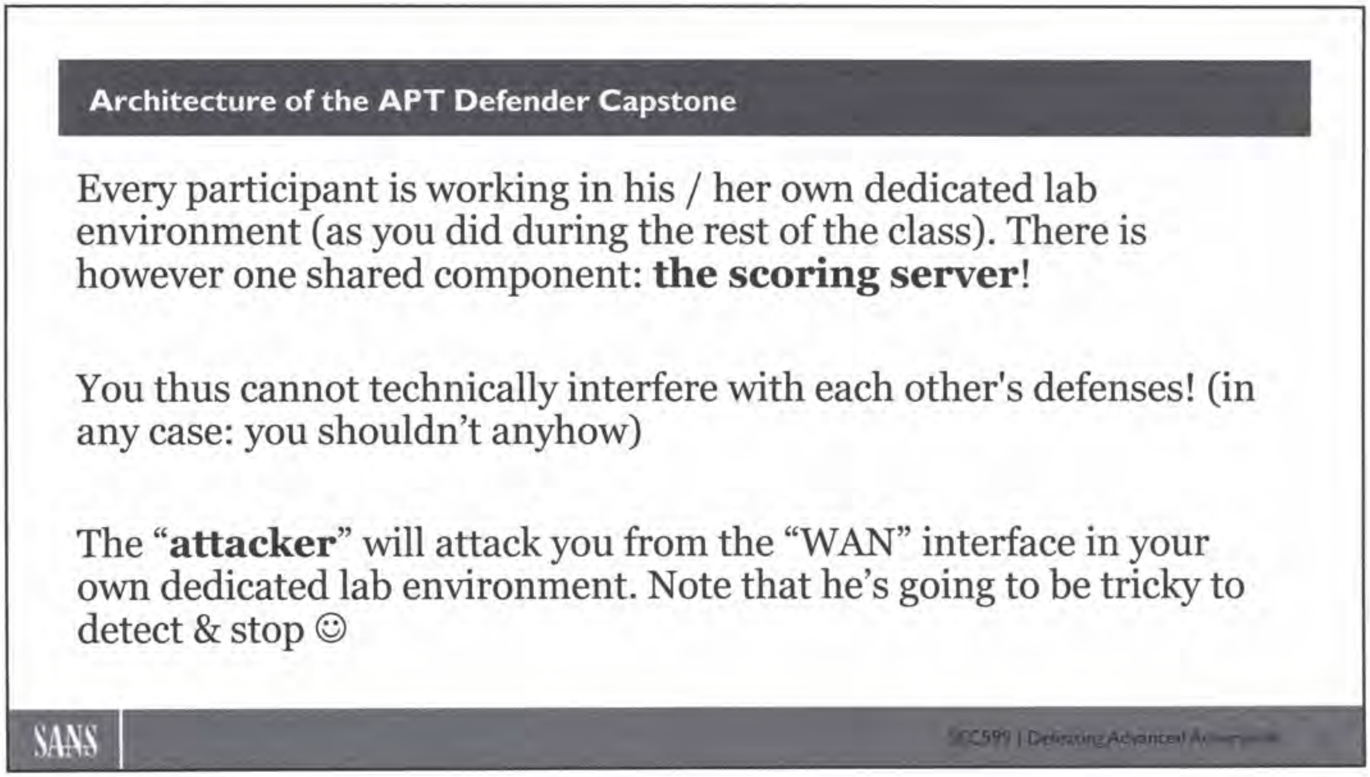
SEC599 | Defeating Advanced Adversaries 4

How to start?

After this lecture, you can start by launching the student lab that is available in the LODS environment.

DO NOT LAUNCH THE LAB NOW ☺ - This will only put you at a disadvantage…

Once authenticated to the Windows02 workstation, please open Chrome, browse the Scoreboard bookmark and register or join a team, so you can start working together. The maximum number of people in one team is 3. Once registered, wait for the game to be launched by the Instructor, you can however already configure the "attacker server"!



Architecture of the APT Defender Capstone

Every participant is working in his / her own dedicated lab environment (as you did during the rest of the class). There is however one shared component: **the scoring server**!

You thus cannot technically interfere with each other's defenses! (in any case: you shouldn't anyhow)

The "**attacker**" will attack you from the "WAN" interface in your own dedicated lab environment. Note that he's going to be tricky to detect & stop ☺

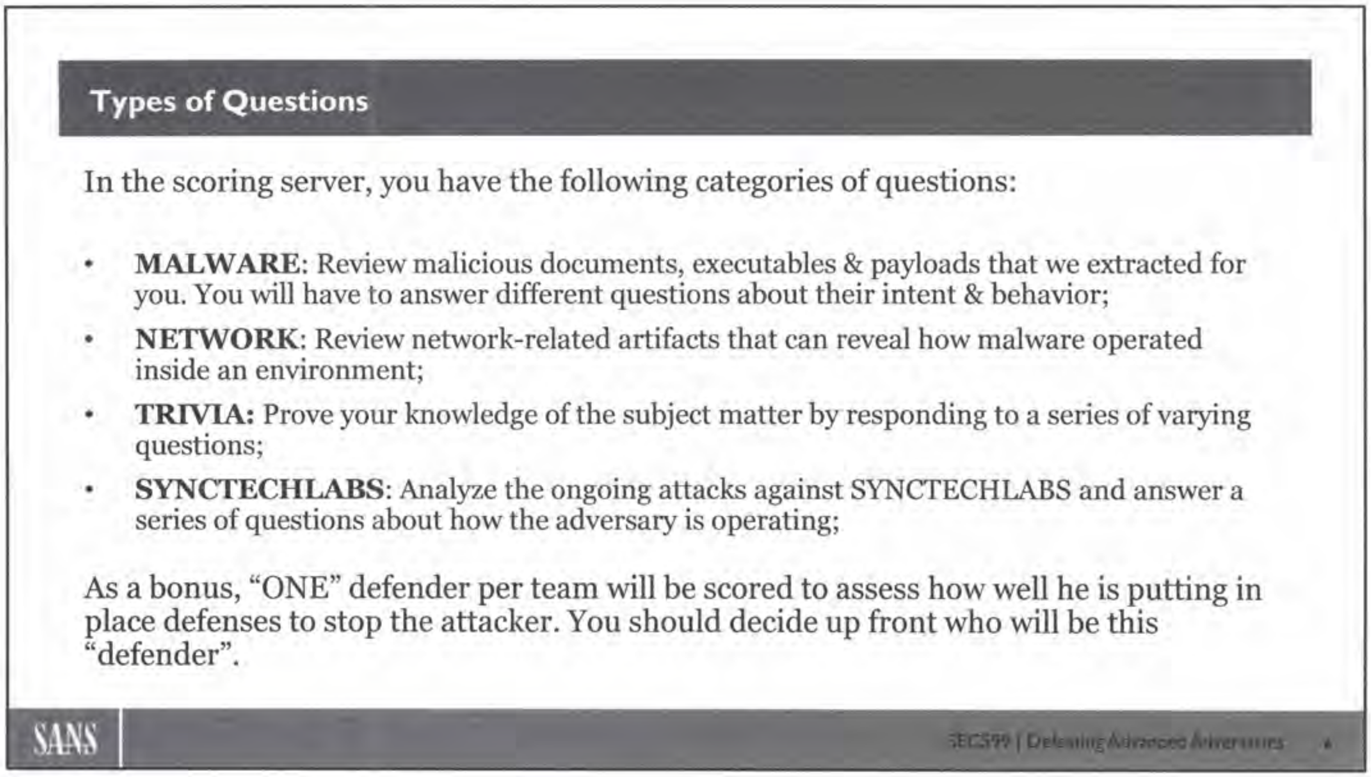
Architecture of the APT Defender Capstone

A quick note on the architecture of our APT Defender Capstone: Avery participant is working in his / her own dedicated lab environment (as you did during the rest of the class). There is, however, one shared component: the scoring server!

You thus cannot technically interfere with each other's defenses! (in any case: you shouldn't try anyhow). We have a list of Rules of Engagements that are listed near the end of this deck.

The "attacker" will attack you from the "WAN" interface in your own dedicated lab environment. Note that he's going to be tricky to detect & stop…

© 2017 Erik Van Buggenhout & Stephen Sims



Types of Questions

In the scoring server, you have the following categories of questions:

- **MALWARE**: Review malicious documents, executables & payloads that we extracted for you. You will have to answer different questions about their intent & behavior;
- **NETWORK**: Review network-related artifacts that can reveal how malware operated inside an environment;
- **TRIVIA:** Prove your knowledge of the subject matter by responding to a series of varying questions;
- **SYNCTECHLABS**: Analyze the ongoing attacks against SYNCTECHLABS and answer a series of questions about how the adversary is operating;

As a bonus, "ONE" defender per team will be scored to assess how well he is putting in place defenses to stop the attacker. You should decide up front who will be this "defender".

SANS

SEC599 | Defeating Advanced Adversaries 6

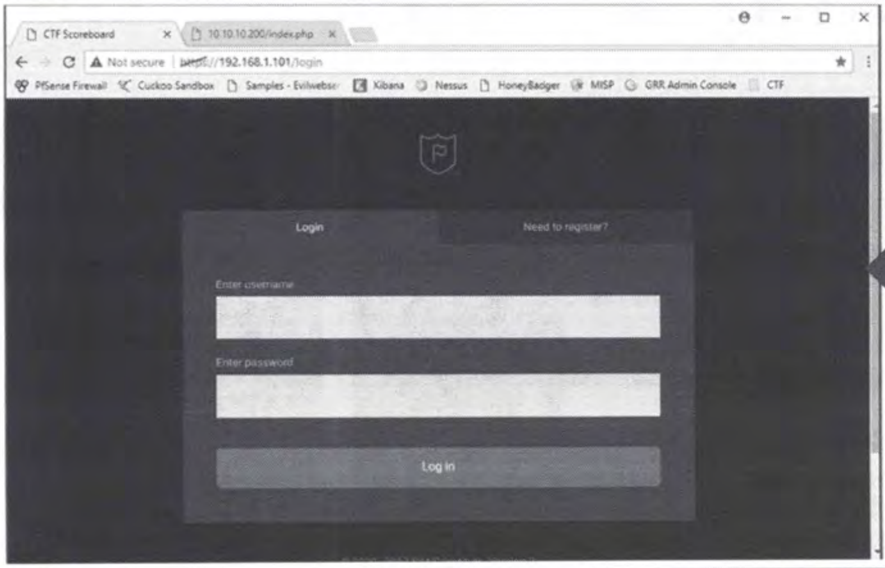
Types of questions
In the scoring server, you have the following categories of questions:

MALWARE: Review malicious documents, executables & payloads that we extracted for you. You will have to answer different questions about their intent & behavior;
NETWORK: Review network-related artifacts that can reveal how malware operated inside an environment;
TRIVIA: Prove your knowledge of the subject matter by responding to a series of varying questions;
SYNCTECHLABS: Analyze the ongoing attacks against SYNCTECHLABS and answer a series of questions about how the adversary is operating;

As a bonus, "ONE" defender per team will be scored to assess how well he is putting in place defenses to stop the attacker. You should decide up front who will be this "defender".

© 2017 Erik Van Buggenhout & Stephen Sims

Registering a User & Team



Throughout day 6, you will interact with our central scoring server, where you will first have to register a user and join a team, so you can authenticate to the scoring interface.

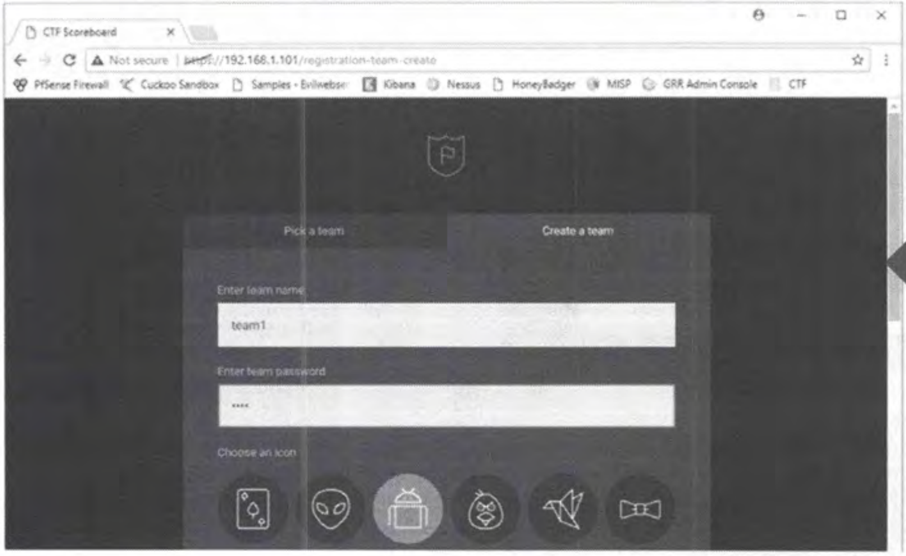
There is a limit of 3 users per team.

Registering a user & team

Throughout day 6, you will interact with our central scoring server, where you will first have to register a user and join a team, so you can authenticate to the scoring interface. As already indicated, there is a limit of 3 users per team.

© 2017 Erik Van Buggenhout & Stephen Sims

Creating a Team



Enter team name

team1

Enter team password

****

Choose an icon

Create a team name, password and icon.

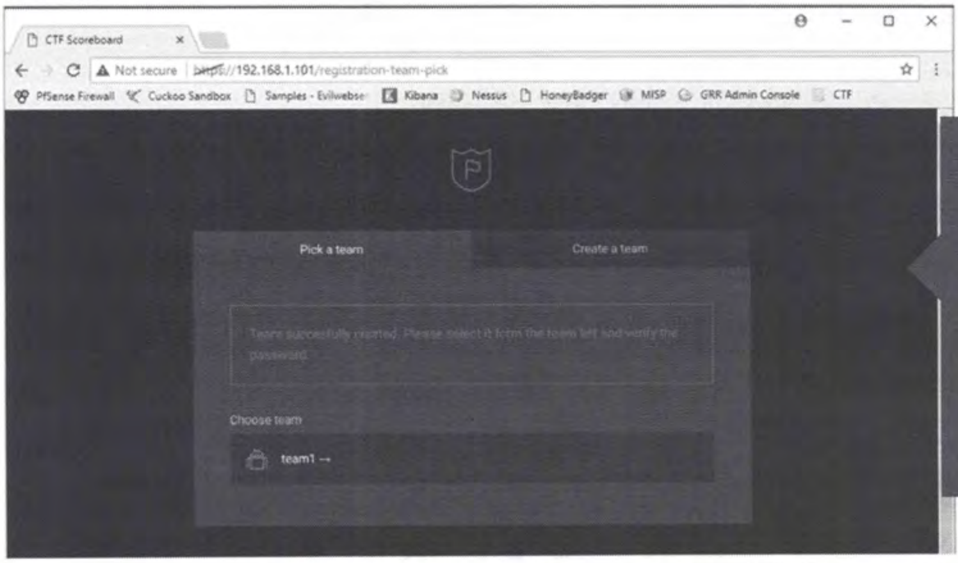
Note that you should share the teamname and password with all participants that want to play in your team!

Creating a team

Create a team name, password, and icon. Feel free to get creative, but remember that you should share the team name and password with all participants that want to play in your team!

© 2017 Erik Van Buggenhout & Stephen Sims

Joining a Team



Team successfully created. Please select it from the team list and verify the password.

Choose team

team1 →

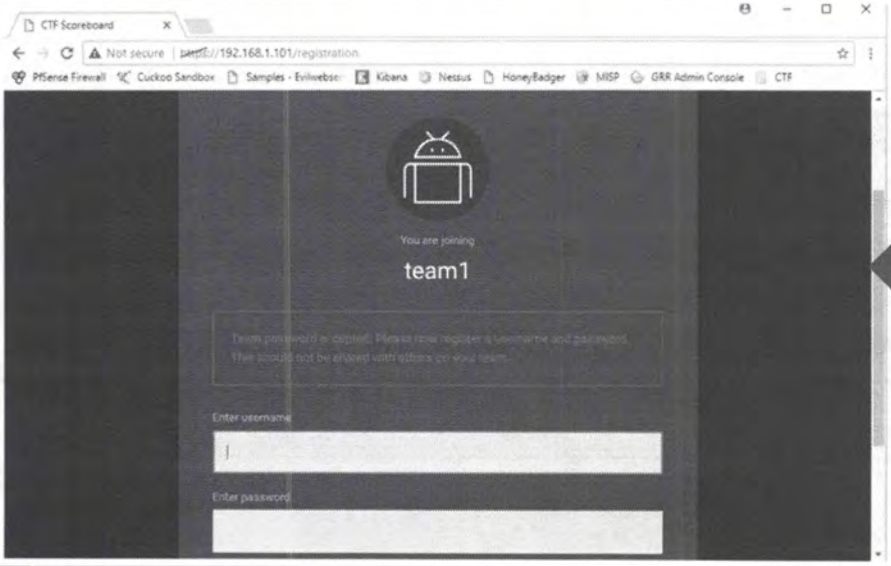
If you would like to join an existing team, just select it from the web interface!

Remember: you will need the password for the team in order to be able to join it!

Joining a team

If you would like to join an existing team, just select it from the web interface! Remember: you will need the password for the team in order to be able to join it!

Creating Your Username



https://192.168.1.101/registration

You are joining

team1

Team password accepted. Please now register a username and password. This should not be shared with others on your team.

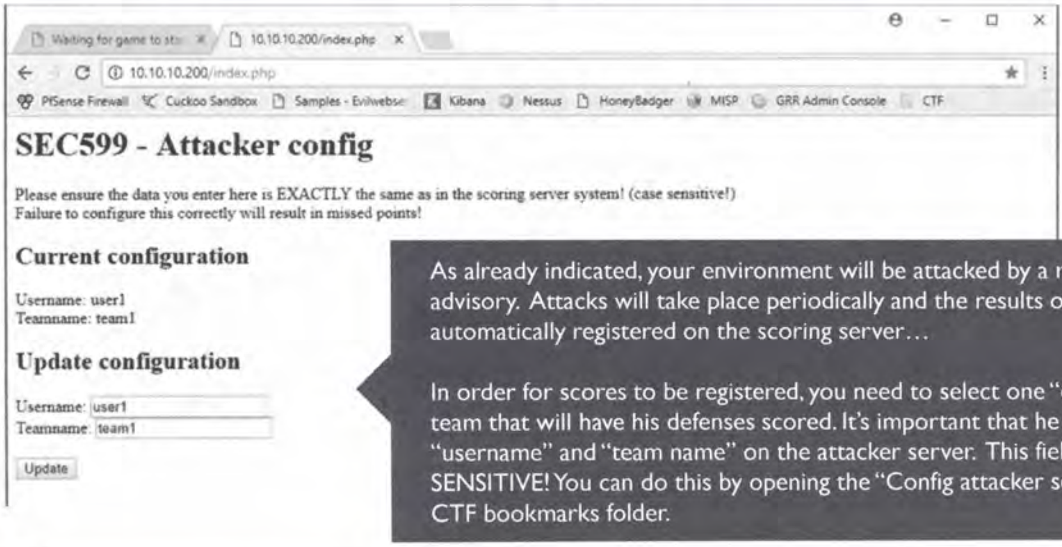
Enter username

Enter password

Once the team password is accepted, you can now create your very own username!

Creating your username
Once the team password is accepted, you can now create your very own username!

For the "One Defender" Only - Configure the Attacker Server



SEC599 - Attacker config

Please ensure the data you enter here is EXACTLY the same as in the scoring server system! (case sensitive!)
Failure to configure this correctly will result in missed points!

Current configuration

Username: user1
Teamname: team1

Update configuration

Username: user1
Teamname: team1

Update

As already indicated, your environment will be attacked by a rather persistent advisory. Attacks will take place periodically and the results of which will be automatically registered on the scoring server…

In order for scores to be registered, you need to select one "defender" in your team that will have his defenses scored. It's important that he registers his "username" and "team name" on the attacker server. This field is CASE SENSITIVE! You can do this by opening the "Config attacker server" from the CTF bookmarks folder.

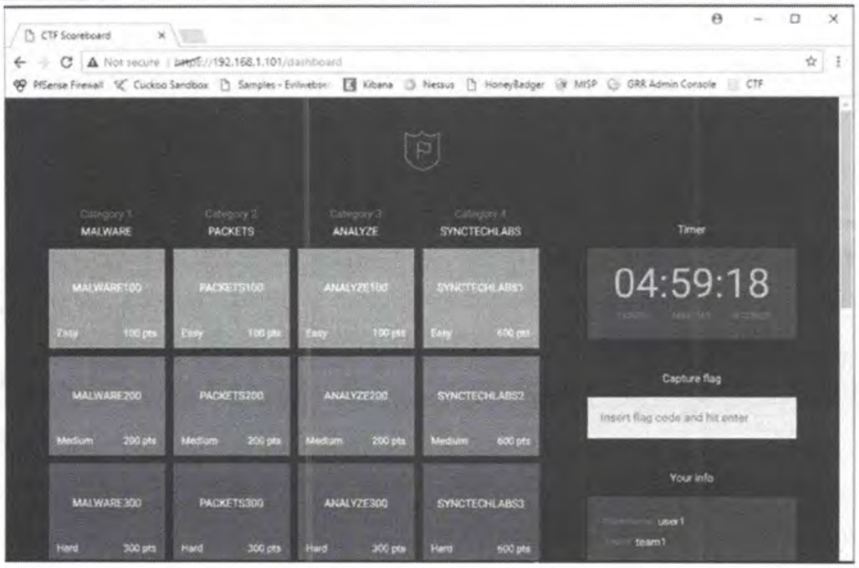
For the "One defender" only - Configure the attacker server
As already indicated, your environment will be attacked by a rather persistent advisory. Attacks will take place periodically and the results of which will be automatically registered on the scoring server…

In order for scores to be registered, you need to select one "defender" in your team that will have his defenses scored. It's important that he registers his "username" and "team name" on the attacker server. This field is CASE SENSITIVE! You can do this by opening the "Config attacker server" from the CTF bookmarks folder.

This step is important: an incorrect configuration here will score you 0 points on all attempted attacks!

© 2017 Erik Van Buggenhout & Stephen Sims

Main Interface



Category 1 MALWARE	Category 2 PACKETS	Category 3 ANALYZE	Category 4 SYNCTECHLABS
MALWARE100 Easy 100 pts	PACKETS100 Easy 100 pts	ANALYZE100 Easy 100 pts	SYNCTECHLABS1 Easy 600 pts
MALWARE200 Medium 200 pts	PACKETS200 Medium 200 pts	ANALYZE200 Medium 200 pts	SYNCTECHLABS2 Medium 600 pts
MALWARE300 Hard 300 pts	PACKETS300 Hard 300 pts	ANALYZE300 Hard 300 pts	SYNCTECHLABS3 Hard 600 pts

Timer

04:59:18

Capture flag

Insert flag code and hit enter

Your info

user1

team1

Once the game is started and you are authenticated, you should receive a screen very similar to the one to the right.

All tiles represent questions you can click and subsequently attempt to answer!

SANS

SEC599 | Defeating Advanced Adversaries 12

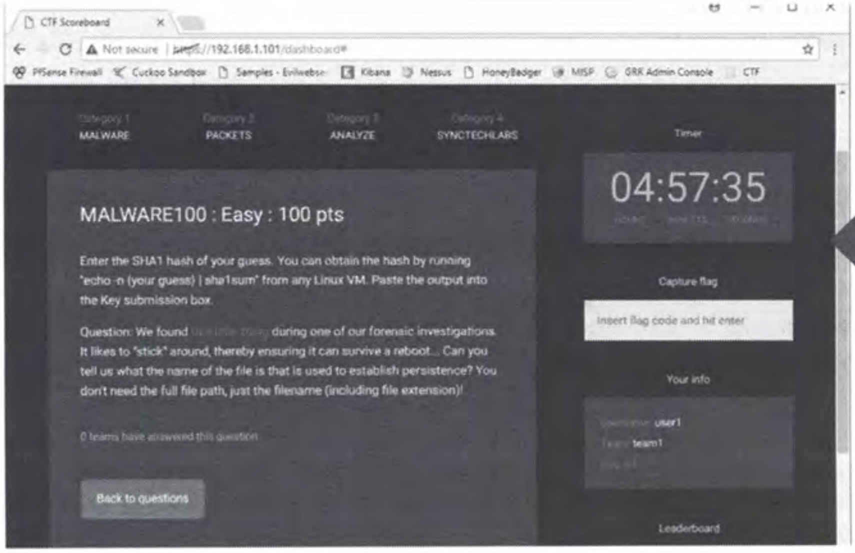
Main interface

Once the game is started and you are authenticated, you should receive a screen very similar to the one to the right.

All tiles represent questions you can click and subsequently attempt to answer!

© 2017 Erik Van Buggenhout & Stephen Sims

Submitting Answers



MALWARE100 : Easy : 100 pts

Enter the SHA1 hash of your guess. You can obtain the hash by running "echo -n (your guess) | sha1sum" from any Linux VM. Paste the output into the Key submission box.

Question: We found this little thing during one of our forensic investigations. It likes to "stick" around, thereby ensuring it can survive a reboot... Can you tell us what the name of the file is that is used to establish persistence? You don't need the full file path, just the filename (including file extension)!

0 teams have answered this question

When clicking one of the questions, you will receive a detailed question description, along with some guidance on how to submit your guess. The flags are all SHA1 checksums, so you will often need to create a SHA1 checksum of your guess!

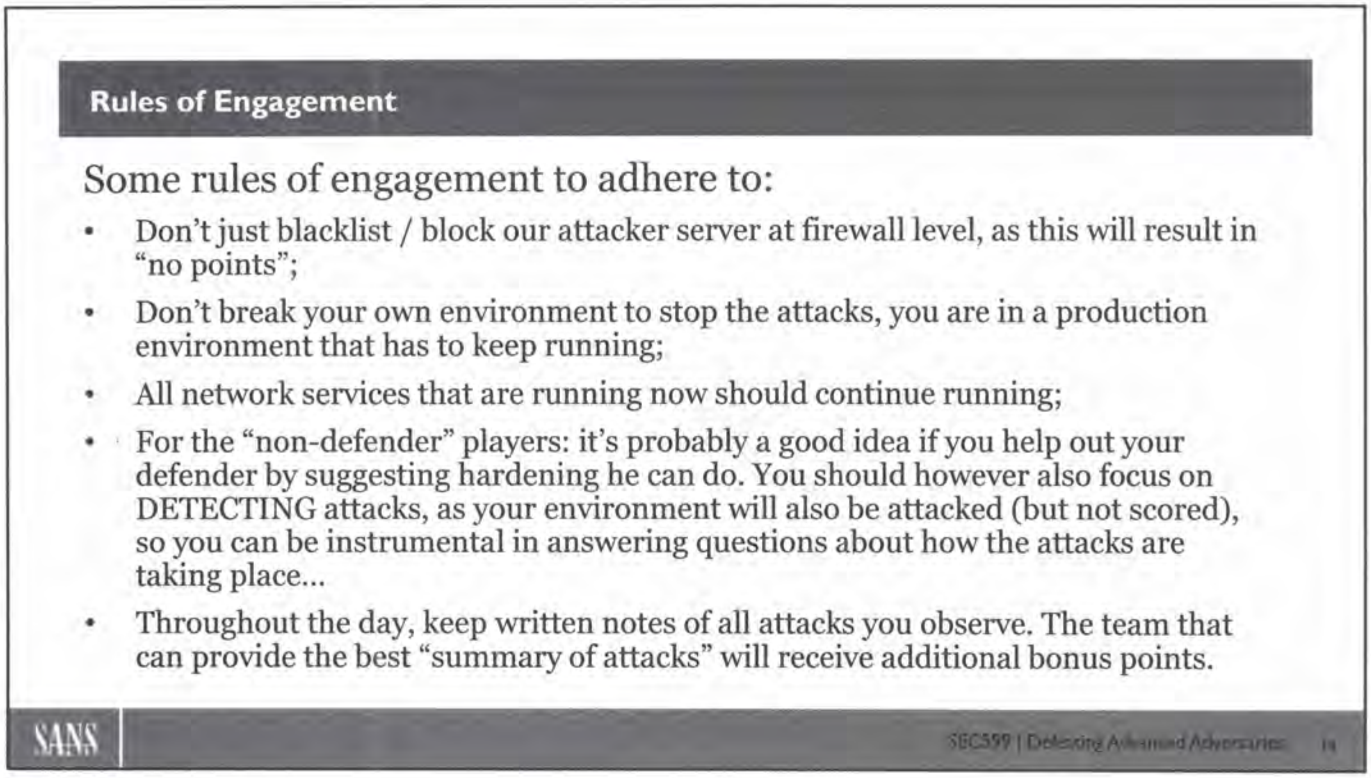
The interface will also provide an insight in what teams have already solved the question!

Submitting answers

When clicking one of the questions, you will receive a detailed question description, along with some guidance on how to submit your guess. The flags are all SHA1 checksums, so you will often need to create a SHA1 checksum of your guess!

The interface will also provide an insight in what teams have already solved the question!

© 2017 Erik Van Buggenhout & Stephen Sims



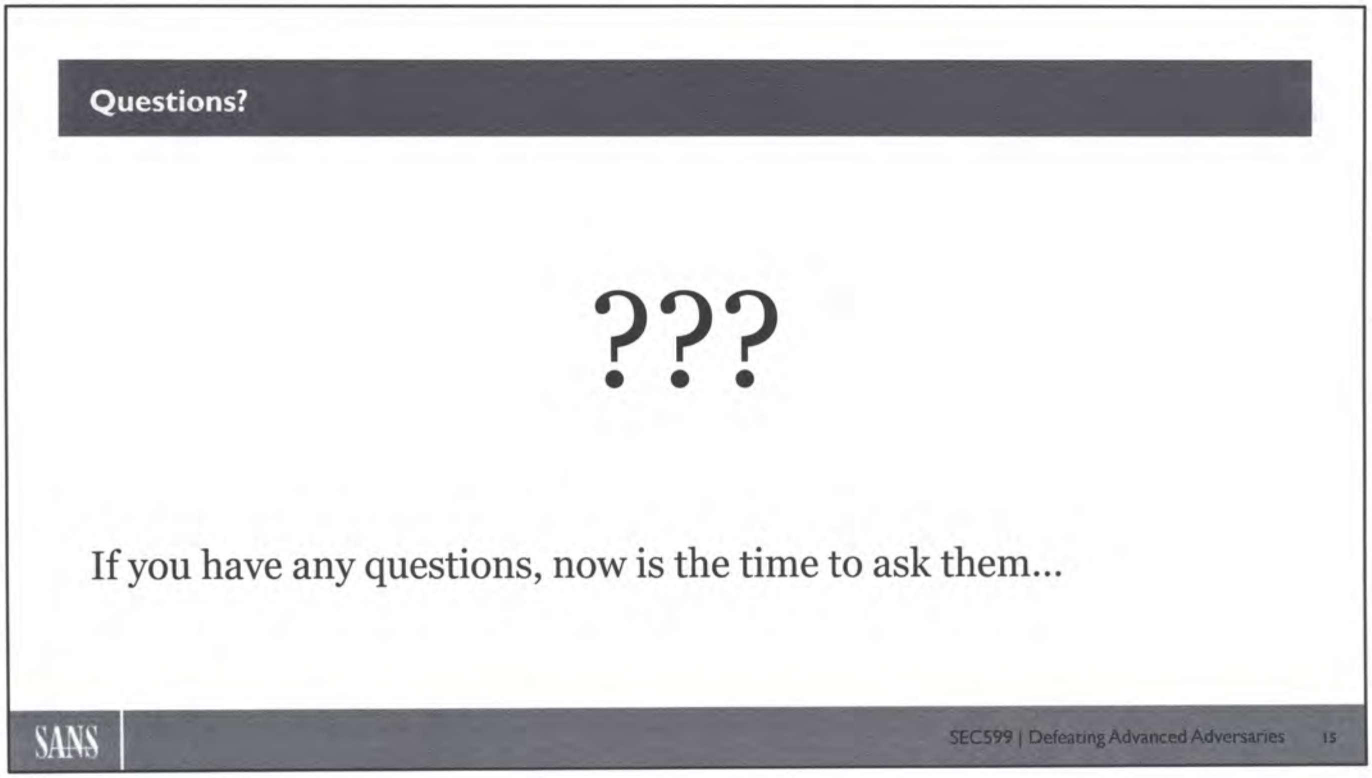
Rules of Engagement

Some rules of engagement to adhere to:

- Don't just blacklist / block our attacker server at firewall level, as this will result in "no points";
- Don't break your own environment to stop the attacks, you are in a production environment that has to keep running;
- All network services that are running now should continue running;
- For the "non-defender" players: it's probably a good idea if you help out your defender by suggesting hardening he can do. You should however also focus on DETECTING attacks, as your environment will also be attacked (but not scored), so you can be instrumental in answering questions about how the attacks are taking place...
- Throughout the day, keep written notes of all attacks you observe. The team that can provide the best "summary of attacks" will receive additional bonus points.

Rules of engagement
Some rules of engagement to adhere to:

- Don't just blacklist / block our attacker server at firewall level, as this will result in "no points";
- Don't break your own environment to stop the attacks, you are in a production environment that has to keep running;
- All network services that are running now should continue running;
- For the "non-defender" players: it's probably a good idea if you help out your defender by suggesting hardening he can do. You should however also focus on DETECTING attacks, as your environment will also be attacked (but not scored), so you can be instrumental in answering questions about how the attacks are taking place…
- Throughout the day, keep written notes of all attacks you observe. The team that can provide the best "summary of attacks" will receive additional bonus points.



Questions?

???

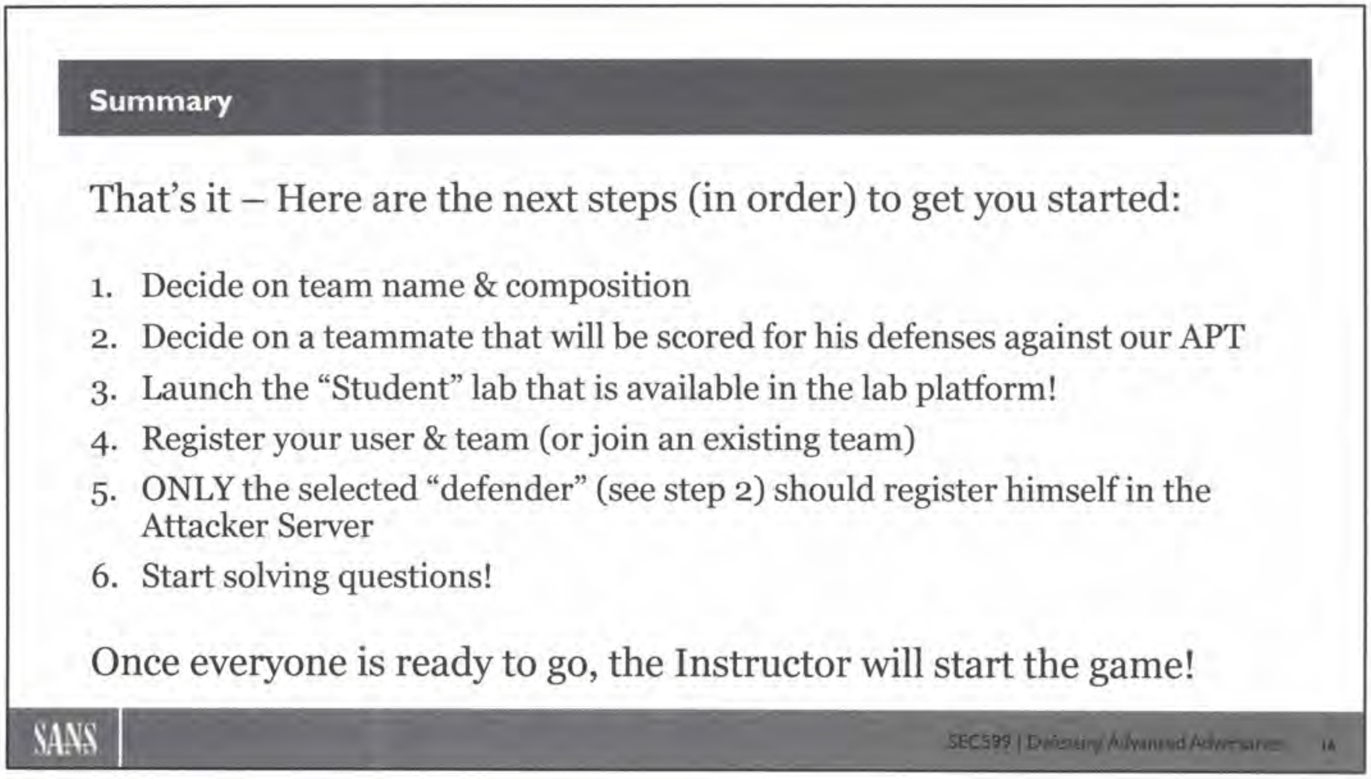
If you have any questions, now is the time to ask them...

SANS

SEC599 | Defeating Advanced Adversaries 15

Questions?
If you have any questions, now is the time to ask them…

© 2017 Erik Van Buggenhout & Stephen Sims



Summary

That's it – Here are the next steps (in order) to get you started:

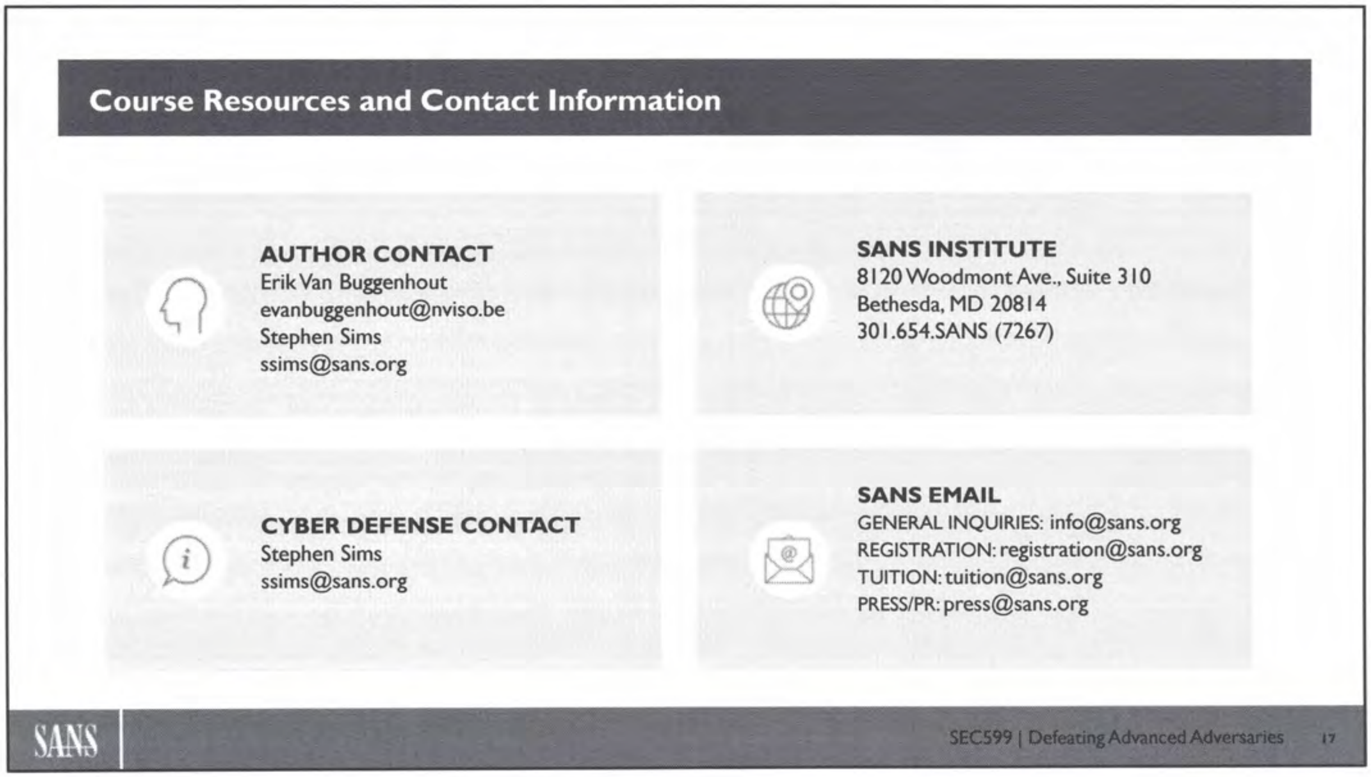
1. Decide on team name & composition
2. Decide on a teammate that will be scored for his defenses against our APT
3. Launch the "Student" lab that is available in the lab platform!
4. Register your user & team (or join an existing team)
5. ONLY the selected "defender" (see step 2) should register himself in the Attacker Server
6. Start solving questions!

Once everyone is ready to go, the Instructor will start the game!

Summary
That's it – Here are the next steps (in order) to get you started:

- Decide on team name & composition
- Decide on a teammate that will be scored for his defenses against our APT
- Launch the "Student" lab that is available in the lab platform!
- Register your user & team (or join an existing team)
- ONLY the selected "defender" (see step 2) should register himself in the Attacker Server
- Start solving questions!

Once everyone is ready to go, the Instructor will start the game!



Course Resources and Contact Information

AUTHOR CONTACT
Erik Van Buggenhout
evanbuggenhout@nviso.be
Stephen Sims
ssims@sans.org

SANS INSTITUTE
8120 Woodmont Ave., Suite 310
Bethesda, MD 20814
301.654.SANS (7267)

CYBER DEFENSE CONTACT
Stephen Sims
ssims@sans.org

SANS EMAIL
GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

This page intentionally left blank.

© 2017 Erik Van Buggenhout & Stephen Sims

This page intentionally left blank.

Index

%System%	1:88
%TMP%	1:102
(Not)Petya	1:37

A

access tokens	4:43, 4:45, 4:102-104, 4:117-118, 4:164
Actions On Objectives	1:65, 1:78, 5:7, 5:11
Active Directory (AD)	2:110, 3:7, 3:13, 3:15, 3:176-178, 3:188, 4:3-4, 4:14, 4:24, 4:32, 4:34, 4:52, 4:88, 4:90-100, 4:103-112, 4:114-133, 4:135-141, 4:148, 4:150, 4:157-158, 4:162, 4:184, 4:187, 5:53, 5:59, 5:62, 5:67, 5:72
ActiveX	2:138, 2:140, 2:143, 2:146, 2:156, 2:160-161, 2:165, 2:168, 2:173, 2:182-183
Address Space Layout Randomization (ASLR)	3:29, 3:97-98, 3:105, 3:127, 3:129-131, 3:141
Admin Approval Mode (AAM)	4:45-47, 4:50
Advanced	1:1-2, 1:13, 1:20, 1:22, 1:34, 1:36, 1:60-61, 1:63, 1:70-71, 1:81, 1:83, 1:129, 1:142, 1:160, 1:162-163, 1:183, 1:185, 1:188, 2:1, 2:4-5, 2:9, 2:11, 2:13, 2:48, 2:54, 2:73, 2:91, 2:98-99, 2:105, 2:107, 2:111, 2:126, 2:184, 3:1, 3:17, 3:60, 3:73, 3:104, 3:141, 3:145, 3:160, 3:165, 3:169, 4:1, 4:8, 4:12, 4:59, 4:69, 4:75, 4:90, 4:104-105, 4:112, 4:115-116, 4:122, 4:129, 4:132, 4:164, 5:1, 5:7, 5:9, 5:11, 5:15, 5:18-19, 5:25-26, 5:29, 5:44-45, 5:53, 5:78, 5:83-84, 5:100, 5:110, 5:114-115, 5:130, 5:135, 5:137, 5:147, 5:151, 5:153-155, 5:157, 6:1-2
Advanced Persistent Threat (APT)	1:2, 1:11-12, 1:14, 1:20, 1:34, 1:51, 1:58-59, 1:63-64, 1:80-81, 1:87, 1:92, 1:96, 1:98, 1:106, 1:109, 1:122, 1:129, 1:145, 1:159, 1:188, 2:4, 2:23-24, 2:35, 3:4, 4:5, 4:15, 4:17-19, 4:22, 4:57, 4:59, 4:72, 4:84, 4:164, 5:5, 5:107, 5:122, 5:168, 6:1-2, 6:5, 6:16
AD|Protect	5:62, 5:67

Affected Users 3:45
Agent.BTZ 1:121
Agilis 1:29
Alternate Data Stream 1:130, 2:155
Amazon.com 1:45
American Fuzzy Lop (AFL) 3:64
Anonymous 1:42-43, 4:118, 5:26-27
Anunak 1:34
Apache 2:95, 2:116, 2:122, 2:125, 4:13
Application whitelisting 1:72-74, 1:80, 1:148, 2:110-112, 2:140, 2:142, 2:162-163, 2:176, 3:3, 3:5, 3:71, 3:173-177, 3:184, 3:186, 3:188-190, 4:82, 4:140
AppLocker 1:73, 3:3, 3:5, 3:175-186, 3:188-189, 4:21, 4:24
AppSense 3:175
APT Attack Cycle 1:2, 1:12, 1:14, 1:59, 1:80-81, 1:87, 1:92, 1:98, 1:109, 1:122, 1:129, 1:145, 1:159, 1:188, 2:4, 2:23-24, 3:4, 4:5, 4:57, 4:59, 4:84, 4:164, 5:5
APT-1337 1:145
APT28 1:58, 2:28, 4:17, 4:19, 4:22
apt_regin_vfs 1:139
ASCII 1:100, 1:136, 2:67-69, 2:71, 2:91, 2:160, 3:58-59, 3:102, 3:107, 5:16, 5:158
ATM Malware 1:29, 1:31-33
Attack Surface Reduction (ASR) 3:136
Authentication Server (AS) 3:15-16, 4:96, 5:128
Auto-start 4:11, 4:26
AutoOpen 1:106, 2:156, 2:158, 2:160-161
autorun 1:74-75, 1:101, 1:113, 2:46, 2:107, 2:109-111, 2:158, 2:182, 3:168, 4:5-6, 4:25-27, 4:29-30, 4:55, 4:131, 5:162
AutoRun 1:74-75, 1:101, 1:113, 2:46, 2:107, 2:109-111, 2:158, 2:182, 3:168, 4:5-6, 4:25-27, 4:29-30, 4:55, 4:131, 5:162
awareness 1:11, 1:59, 1:67, 1:70, 1:80, 1:156, 1:169, 2:2, 2:4, 2:7, 2:9, 2:12-15, 2:18, 2:21, 2:110, 2:141-142, 2:153, 2:158-159, 2:166, 2:169, 2:190, 3:51, 3:161, 4:122, 4:147, 5:122

B

Backup Operators	4:99
Bangladesh Bank	1:22, 1:83, 1:85, 1:90-95, 1:107, 1:120, 1:126
Banking Trojan	1:22-23, 1:25-28, 2:84, 4:77
base64	1:75, 2:24, 2:41, 2:161, 2:172, 2:181, 4:6, 4:39, 5:27, 5:36
Beginner's All-purpose Symbolic Instruction Code (BASIC)	2:137
Belgacom International Carrier Services (BICS)	1:83, 1:129
BeRoot	4:42, 4:54
BinDiff	3:73, 3:92-93
Bing	1:16, 1:23, 1:47, 1:64, 1:160, 1:174, 1:180, 3:114, 5:47, 5:54, 5:69
BlackEnergy	1:83, 1:96-106, 2:184
BloodHoundAD	4:119
Bootkits	4:11, 4:22-24
botnet	1:45-48, 2:84, 4:13
Box	1:11, 1:38, 1:69-70, 1:104-106, 1:141-142, 1:146, 1:148, 1:185, 2:2, 2:5, 2:36-39, 2:41-43, 2:45-50, 2:52-55, 2:74, 2:79, 2:83, 2:88, 2:141-142, 2:147, 2:149-154, 2:166, 2:188, 3:28, 3:40, 3:51, 3:80, 3:95, 3:123, 3:127, 3:143, 3:182, 3:186, 4:70, 4:73, 4:123, 4:138, 4:158, 4:169, 5:9, 5:26, 5:30, 5:93, 5:155, 5:160
Bring Your Own Device (BYOD)	1:154, 2:11, 3:18, 3:20
Bro	4:66, 4:78
Bromium vSentry	3:144
buffer overflow	3:26, 3:56, 3:59, 3:61, 3:99-100, 3:104, 3:109, 3:132
Bug bounty	3:48, 3:52-53

C

C99	4:13
canaries	3:29, 3:97-98, 3:113, 3:117, 5:49, 5:57-63, 5:66-68
canary	3:113, 4:88, 5:49, 5:58-59, 5:61-69
Canarytokens	5:62-63, 5:65-66, 5:69

Carbanak 1:22, 1:34-35, 4:18, 5:11
Carbon Black 3:158
CEN/XFS standard 1:30-31
Central Intelligence Agency (CIA) 1:50
Cerber 1:37
Certification Authorities (CA) 3:53, 4:65, 5:20, 5:22
China Chopper 4:12
Cigital 3:36
CIRCL 1:176, 3:97, 5:90-91
Cisco 2:27, 3:11, 3:13, 3:20, 3:24, 3:56, 4:60-61, 4:63, 4:66
Citadel 1:22-23
ClamAV 1:135-136, 2:2, 2:57-58, 2:95, 2:97-99, 2:102-103, 2:190, 3:160, 3:162, 5:15, 5:92
cmdlet 2:168, 2:170-171, 2:174-175, 2:177
CodeSearchDiggity 3:55
Command and Control (C&C) 1:27, 1:47, 1:125, 2:82-83, 4:13, 4:68-71, 4:75, 5:80
Common Vulnerability Scoring System (CVSS) 3:37, 3:46
Compile-Time Controls 3:2, 3:97, 3:117-118
Compound File Binary Format 1:99, 2:147
Computer Emergency Response Team (CERT) 5:135, 5:143, 5:152, 5:160-161
Computer Incident Response Team (CIRT) 5:90, 5:135-136, 5:139-142, 5:145-147, 5:149, 5:151
Containment 5:138, 5:146, 5:150
Control Flow Enforcement (CET) 3:114
Control Flow Guard (CFG) 3:69, 3:97-98, 3:111-112
Control Flow Integrity (CFI) 3:114
CopyKittens 4:16
Core Impact 3:77
Cortana 5:11
CreateThread 2:163
Credential Guard 4:112-114, 4:135, 4:138, 4:144-146
Cross-Site Request Forgery (CSRF) 3:26
Cross-Site Scripting (XSS) 3:26, 3:44
CryptoLocker 1:23
Crysis 1:37
Cuckoo 1:104, 1:141-142, 2:2, 2:38-39, 2:42-47, 2:49-50, 2:52-55, 2:79, 2:190, 5:50, 5:159-160
Current Branch (CB) 3:75

Current Branch for Business (CBB)	3:75
CVE	1:53, 3:73, 3:127, 3:139
Cyber Kill Chain	1:65-66, 1:81
Cyber Threat Intelligence (CTI)	1:16, 5:75, 5:78, 5:104, 5:153
Cybercop Sting	5:50

D

Damage	1:37, 1:43, 1:83, 1:161, 3:45, 3:113, 4:14, 5:137, 5:146
Dark Web	1:177-178
DarkWeb	1:178
DarkWebID	1:178
DarunGrim	3:92
Data Breach Investigations Report (DBIR)	2:8
Data classification	1:153, 1:169, 5:18, 5:42
Data Execution Prevention (DEP)	3:29, 3:97-98, 3:106, 3:112, 3:122-123, 3:126, 3:132, 3:138, 3:141
Data Loss Prevention systems (DLP)	1:78-79, 1:169, 4:85, 5:5, 5:32-34
Datagram	3:58
daterange:	1:174
DCSync	4:123, 4:128-129, 4:136
deception	1:11-12, 4:86, 4:187, 5:1, 5:3, 5:5, 5:23, 5:47, 5:50, 5:62, 5:67, 5:69, 5:71-72, 5:168
Deceptive Toolkit	5:50
Decode64	2:161
decoy	5:23, 5:46, 5:48-49, 5:51, 5:53, 5:58, 5:67-68
Deep Panda	4:12
default accounts	4:100
Defense in Depth	3:97
Delivery	1:11, 1:53, 1:65-66, 1:69-70, 1:72, 1:87, 1:92, 1:98, 1:109, 1:122, 1:127, 1:129, 2:2, 2:4, 2:7-9, 2:13-14, 2:82, 2:91, 2:105-111, 2:170, 2:190, 3:4, 3:111, 4:5, 4:57, 4:84, 5:5, 5:92, 5:113
Dell SecureWorks	1:65
Denial of Service	1:20, 1:42, 1:44-45, 1:66, 1:97, 3:37, 3:43-44, 4:13
Department of Homeland Security (DHS)	3:37, 3:46
Development	1:2, 1:16, 1:29, 1:31-33, 1:50, 1:53, 1:65,

	1:69, 1:72, 1:108, 1:152, 1:161, 1:167, 1:170, 1:175, 2:30, 2:73, 2:116, 2:149, 3:2, 3:4, 3:22-24, 3:28-31, 3:33-36, 3:43, 3:51, 3:54, 3:120-121, 3:126, 3:190, 4:77, 4:167, 5:12, 5:57, 5:154
DHCP negotiation	3:8
DIAMETER	3:15
Diaphora	3:92
Diebold	1:29
DigiNotar	5:22
Directory Replication Service Remote (DRSR)	4:129
Discoverability	3:45
Distributed Denial of Service (DDoS)	1:37, 1:42-47, 1:97-98, 5:143
DLL search order hijacking	4:11, 4:19-21, 4:24, 4:36, 4:51
Domain Admins	4:99, 4:119, 4:132
Domain Keys Identified Mail (DKIM)	2:36
Domain Users	4:40, 4:99, 4:108, 5:168
Domain-based Message Authentication, Reporting and Conformance (DMARC)	2:36
DOUBLEFANTASY	1:52-53
Downdelph	4:19
downloader	2:143-144, 2:146, 2:160-162, 2:165, 2:173, 4:19
DREAD	3:37, 3:45
Dridex	1:22, 1:91
Drive-by download	1:25, 1:37, 1:128-129, 2:83
Dropbox	4:70, 4:73, 5:26
dropper	1:88, 2:161-162, 2:165
Dropper	1:88, 2:161-162, 2:165
DropSmack	4:73, 4:79
Duckhunt	2:112
Ducky	2:112-113
Duqu	1:109
Dynamic Base	3:97
Dynamic Link Library (DLL)	1:93-94, 1:113, 1:118, 1:130, 1:166, 2:54, 2:138, 2:160, 3:94, 3:105, 3:109, 3:111, 3:128-129, 3:136, 3:141, 3:168, 3:183, 4:11, 4:19-21, 4:24, 4:27, 4:36, 4:51

E

EAP Over LAN (EAPOL)	3:14-15
EAP-IKEv2	3:14
EAP-PSK	3:14
EAP-PWD	3:14
ECMAScript	2:137, 2:164, 2:167
Elasticsearch	2:30-31, 2:116-120, 2:128, 2:130, 2:133-134, 4:161
Elasticsearch - Logstash - Kibana (ELK)	2:30-32, 2:115-118, 2:126, 2:131, 2:133-134, 2:190, 3:169, 4:25, 4:29, 4:153, 4:158, 4:184-185, 5:3, 5:116, 5:120, 5:129, 5:132-133
Elevation of Privilege	3:38, 3:43-44, 3:46, 4:45, 4:47-49
Emerging Threats	2:27-28, 2:31-32, 2:91-92
Empire Powershell	2:172, 4:42
ENDBR32	3:114
ENDBR64	3:114
Endpoint Detection & Response (EDR)	3:158, 3:170-171, 4:25, 5:154
Enhanced Mitigation Experience Tool (EMET)	1:73, 1:109, 2:163, 3:2, 3:5, 3:98, 3:110, 3:118, 3:120-126, 3:128-129, 3:131-133, 3:135, 3:137-142, 3:147, 3:168
Enhanced Mitigation Experience Toolkit (EMET)	1:73, 1:109, 2:163, 3:2, 3:5, 3:98, 3:110, 3:118, 3:120-126, 3:128-129, 3:131-133, 3:135, 3:137-142, 3:147, 3:168
Enterprise Admins	4:99
Epic Turla	1:51, 1:84, 1:95, 1:121, 1:123-125
Equation Group	1:51-53, 1:55-58, 1:96, 5:100
EQUATIONDRUG	1:52-54, 1:56
Eradication	5:138, 5:147, 5:150
Event Forwarding	4:158-159, 4:161, 4:182
Event Log Monitoring	4:162, 4:165, 4:182
event logs	1:66, 1:164, 2:176, 2:178-181, 3:176, 3:183, 4:4, 4:153-162, 4:165, 4:176, 4:178-182, 4:184-185, 4:187, 5:120
EVTX	4:153, 4:157
eXecute Disable (XD)	3:106
Exfiltration	1:11-12, 1:34, 1:59, 1:79, 1:122, 1:163, 4:32, 4:73, 4:75, 4:82, 4:85, 4:187, 5:1, 5:3, 5:5, 5:7-11, 5:14, 5:16, 5:24-27, 5:29-34, 5:36-39, 5:41-42, 5:80, 5:84, 5:157, 5:168
exploit kit	1:37, 2:11, 2:23, 2:83-87, 2:92
Exploitability	3:45, 3:99

Exploitation 1:11, 1:51, 1:57, 1:65-66, 1:72-74, 1:87, 1:92, 1:98, 1:109, 1:122, 1:129, 2:4, 2:111, 2:169, 2:183, 2:190, 3:1, 3:4-5, 3:77, 3:97, 3:99, 3:105, 3:110, 3:117-118, 3:120-122, 3:126-127, 3:132, 3:140, 3:145, 3:147-148, 3:189-190, 4:5, 4:8, 4:42, 4:57, 4:84, 4:86, 4:112, 5:5, 5:100, 5:113
Export Address Table (EAT) 3:128
Extensible Authentication Protocol (EAP) 3:14-16
Extensible Storage Engine (ESE) 4:98
eXtensions for Financial Services (XFS) 1:29-31, 1:33

F

FakeToken 1:27-28
Federal Reserve Bank 1:83, 1:91-92
Feisty Chicken 1:145
File Transfer Protocol (FTP) 3:58, 3:150, 4:68, 4:136, 5:29
filetype: 1:174
finalize the kill 1:78, 4:84, 5:5
FireEye HX 3:158, 3:170
FireEye MX 2:38, 2:55
FLASHFLOOD 4:17
Fortify 3:29, 3:54-55
Fortinet 2:89, 4:66
Fox 1:43, 1:51, 1:128, 3:55, 3:70, 3:123, 4:71, 4:79, 4:117
Full Packet Capture (FPC) 1:164, 4:59, 4:62-64, 4:66
fuzzing 3:24, 3:30, 3:48, 3:56, 3:58-64, 3:190

G

Get-ChildItem 5:12-13
Get-ExecutionPolicy 2:170
Get-Help 2:174
GetSystemDirectory 4:20
GetWindowsDirectory 4:20
Golden Ticket 4:109, 4:116, 4:123, 4:125-130, 4:132, 4:162
Goldeneye 1:37
Google 1:51, 1:156, 1:167, 1:174, 1:180, 2:35, 2:98,

	3:53, 3:55, 3:64, 3:92, 3:140, 4:64, 4:70, 5:22, 5:26, 5:61, 5:93, 5:151, 5:156, 5:163
Google Drive	2:35, 5:26
Google Rapid Response (GRR)	1:136, 3:158, 3:170, 5:4, 5:151, 5:154, 5:156-158, 5:163, 5:165-166, 5:168
GoPhish	2:15-21
GRAYFISH	1:52-56
Graylog	2:115
Grok	2:116, 2:125
Group Policy Object (GPO)	2:187, 3:75, 3:155, 3:182, 4:29
Group Policy Option (GPO)	2:187, 3:75, 3:155, 4:29
Group Policy Preferences (GPP)	4:36, 4:40-41
GRR	1:136, 3:158, 3:170, 5:4, 5:151, 5:154, 5:156-158, 5:163, 5:165-166, 5:168

H

Hacktivism	1:42
HAMMERTOSS	4:72, 4:79
Hardentools	2:182-183, 2:185
HDDCryptor	1:37
headers	1:139, 2:36, 2:91, 4:13, 4:59, 4:75
heap overflow	3:99
Hijack	1:118, 3:109, 3:113, 4:11, 4:19-21, 4:24, 4:27, 4:36, 4:51, 5:15-16
honeypot	4:88, 5:3, 5:49-57, 5:62, 5:66, 5:68, 5:71-72
Host Intrusion Detection System (HIDS)	3:158, 3:168-169, 3:171
Human Interface Device (HID)	2:112
Hunting Maturity Model (HMM)	5:117

I

IDA Pro	3:73
Identification	1:17, 1:98, 3:7-8, 3:27, 4:90-91, 4:93, 5:110, 5:138, 5:145, 5:150
IEEE 802.1X	3:14, 3:20
Immunity Canvas	3:77
Incidence response	5:135, 5:139-141, 5:143-149, 5:163
Incognito	4:104, 4:117-118
Indicator of Compromise (IoC)	5:77, 5:86, 5:96, 5:166

Indirect Branch Tracking	3:114
Industrial Control Systems (ICS)	1:19, 1:108, 1:118, 1:180
Information Disclosure	3:43-44
InsightVM	1:184
Institute of Electrical and Electronics Engineers (IEEE)	3:14, 3:20
integer overflow	3:99
Interactive Disassembler (IDA)	3:54, 3:73, 3:92, 3:126
Internet Control Message Protocol (ICMP)	1:129, 5:29
Internet Exploiter	3:127
Internet Message Access Protocol (IMAP)	2:37, 5:29
Internet of Things (IoT)	1:19, 1:45-47, 3:20
Internet Relay Chat (IRC)	5:29
Intrusion Detection System (IDS)	1:74, 1:79, 1:136, 1:151-152, 2:2, 2:23-24, 2:26-28, 2:30-32, 2:38-39, 2:44, 2:52-53, 2:55, 2:91-92, 2:95, 3:73, 3:158, 3:168, 4:25, 4:60, 4:62, 4:66, 4:75, 4:81-82, 4:85, 4:88, 5:32-33, 5:41-42, 5:61, 5:93, 5:95, 5:110, 5:118
Intrusion Prevention System (IPS)	1:70, 1:74, 1:80, 1:136, 1:151-152, 1:172, 2:2, 2:5, 2:23-24, 2:26-27, 2:30, 2:32, 2:39, 2:52-53, 2:55, 2:91-92, 4:5, 4:66, 4:74-75, 4:88, 4:136, 5:95, 5:118
inurl:	1:174
Invoke-Expression	2:174-175
Ivanti	3:72

J

JAVA	1:36, 1:38-40, 1:53, 1:122, 2:23, 2:84, 2:116, 2:118-120, 2:137, 2:164, 2:167, 2:174, 2:182-183, 3:54-55, 3:121, 3:136, 3:141, 4:13
JavaScript	1:36, 1:38-40, 2:23, 2:137, 2:164, 2:167, 2:174, 2:182-183, 4:13
JavaScript Object Notation (JSON)	2:23, 2:29-30, 2:116, 2:125, 2:130-131
Javelin	5:62, 5:67
JHUHUGIT	4:17
Jigsaw	1:37
JScript	2:137, 2:140, 2:164-167, 2:170-171, 2:174-175, 3:159

Juniper	4:66

K

KAL software stack	1:33
Kali Linux	5:46
Kaspersky	1:28, 1:34, 1:52-53, 1:55-56, 1:127, 1:129, 1:134, 1:139, 1:167, 2:63, 4:15, 5:30
Kerberos	4:95-97, 4:109, 4:112, 4:115-116, 4:123, 4:125-127, 4:129, 4:133, 4:136, 4:148
Key Distribution Center (KDC)	4:95-96, 4:127
Kibana	2:2, 2:30-31, 2:115-118, 2:121-123, 2:127-131, 2:133-134, 4:184, 5:129, 5:132
Kill Chain	1:17, 1:59, 1:64-67, 1:70-71, 1:78-81, 1:109, 2:4-5, 4:84-85, 5:5, 5:30
KillDisk	1:97
Kippo	5:56, 5:69
Knowledge Base (KB)	3:78-80, 3:82-83, 3:85, 3:106, 4:157
Komitet Gosudarstvennoy Bezopasnosti (KGB)	1:50

L

Lateral Movement	1:11, 1:34, 1:37, 1:59, 1:78-79, 1:122, 1:128-129, 1:148, 3:160, 3:190, 4:1, 4:3-5, 4:15, 4:25, 4:63, 4:84-88, 4:119, 4:135, 4:150-151, 4:162, 4:178-180, 4:182, 4:184-185, 4:187, 5:5, 5:101
lcamtuf	3:64
LDRPCheckNXCompatibility	3:97
Least privilege	1:72, 2:9, 3:4, 4:3, 4:32, 4:34, 4:36, 4:52, 4:99, 4:147
LeChiffre	1:37
Lessons Learned	5:138, 5:141, 5:145, 5:149-150
link:	1:174, 2:159, 4:178
Lizard Squad	1:42
LM hashing	4:98
LoadLibraryExW()	3:94
location:	1:174
Lockheed Martin	1:65
Locky	1:37

Logstash	2:30, 2:115-116, 2:118, 2:124-126, 2:131, 2:133-134
Loki	5:3, 5:96-103, 5:105, 5:107-108, 5:156
Long-Term Servicing Branch (LTSB)	3:75
Loose Lips Sink Ships	1:68
Loose Tweets Sink Fleets	1:68
Lucene	2:31, 2:116
Lulzsec	1:42-43, 1:58
Lumension	3:76
Lynis	3:154

M

MAC address	3:8, 3:17
macro	1:36, 1:69, 1:72, 1:98-102, 1:148, 2:11, 2:35, 2:58, 2:146-148, 2:153, 2:156-159, 2:182, 2:184, 2:188, 3:4, 3:141, 3:167, 3:185, 5:61, 5:113
MacroExpl	1:101-102
Malware Information Sharing Platform (MISP)	5:3, 5:88-94, 5:105, 5:107-108, 5:160, 5:168
Malwarebytes Anti-Exploit (MBAE)	3:140-143
Mark-of-web	2:154-155, 2:158, 2:166
Masscan	1:179
Master Boot Record (MBR)	1:37, 1:55, 1:86, 1:88, 4:11, 4:22-23
MD4	4:98
MD5	1:99, 1:103-104, 2:40, 4:98, 5:79, 5:88, 5:92, 5:103
MemGC	3:70, 3:97
Metasploit	2:172, 3:77, 3:147, 3:160, 4:16, 4:41, 4:51, 4:108-109, 4:112, 4:117, 5:14
Meterpreter	3:141, 4:16, 4:109, 4:117-118, 5:14
Microsoft Management Console (MMC)	4:153-154
MIME	2:24, 2:40-41
Mimikatz	1:37, 1:51, 4:108-112, 4:114-116, 4:119, 4:125-133, 4:135-136, 4:141, 4:143, 4:148, 4:151, 4:178-180, 5:60, 5:101
Mirai	1:45-47
MITRE	1:16, 4:11, 4:27
Mobile Device Management (MDM)	3:18-20
mobile messages	1:27-28
MongoDB	1:36

mTAN	1:23-24, 1:27-28
Mutation	3:30, 3:56-57, 3:61-62, 3:64
Mutexes	2:63
MySQL	1:36, 2:116, 2:125

N

National Institute of Standards and Technology (NIST)	1:72, 3:4, 3:152-153, 3:155, 4:122
National Software Reference Library (NSRL)	1:164-166
Nessus	1:184, 3:2, 3:49-50, 3:66-67, 4:112
NetFlow	1:157, 2:24, 4:59-62
Network Access Control (NAC)	3:2, 3:7, 3:9-15, 3:17-18, 3:20, 3:190
Network Access Protection (NAP)	3:12
Nexpose	1:184, 3:49
NGINX	2:122-123
NMAP	1:179, 3:160
No eXecute (NX)	3:106
Notpetya	1:141-142, 4:16, 4:132, 5:67, 5:101
NTLM One Way Function (NTOWF)	4:98
null pointer	3:99

O

OASIS	1:16
obfuscation	1:39-40, 2:144, 2:165, 2:167, 2:174-175
Object Linking and Embedding (OLE)	1:99, 2:182
Objective Met	1:65
ObOpenObjectByName()	1:124
OCTAVE	3:37, 3:46
oledump.py	1:99-100, 1:103, 2:57
OneDrive	5:26
OnionScan	1:177-178
Open Information Security Foundation	2:23
Open Source INTelligence (OSINT)	1:177, 5:91
OpenSSH	1:180
OpenVPN	4:37-38
Operation Groundbait	4:19
OS Controls	3:97
OSQuery	4:75, 5:3, 5:126-129, 5:132-133, 5:154,

	5:168
OSSEC	3:158, 3:169
OWASP	3:24, 3:36-37

P

PacketFilter (PF)	2:95, 3:158
PaloAlto	4:66
Paranoid Fish (Pafish)	2:54
Pastebin	1:175-178, 3:85, 3:87-88, 4:71, 5:27, 5:61
Pastemon	1:176
Pastepwnd	1:176
Patch diffing	3:73, 3:91
PatchClean	3:88, 3:90
Patchdiff2	3:92
PatchExtract	3:87-88
Patchlink	3:76
PayPal	1:45, 4:13
PCAP	2:23-24, 2:44, 2:86-87, 4:63
Peach	3:63
Pecheck.py	1:103
Persistence	1:11, 1:56, 1:66, 1:74-75, 1:88, 1:111, 1:115-116, 1:123-124, 1:163, 2:46, 3:168, 4:3, 4:5-6, 4:8-12, 4:14-19, 4:22, 4:24-27, 4:29-30, 4:36, 4:104-105, 4:123-130, 4:187
Persistent	1:22, 1:59, 1:63, 1:66, 1:87, 1:92, 1:98, 2:63, 4:61, 4:63, 4:123, 5:44-45, 6:2, 6:11
Petya	1:37, 1:141-142, 4:16, 4:132, 5:67, 5:101
PfSense	2:2, 2:95-100, 2:102-103, 2:133-134, 2:190, 4:81, 5:41
phishing	1:23, 1:34, 1:36-38, 1:47, 1:63, 1:70, 1:86-87, 1:97-99, 1:122, 1:148, 1:186, 2:7-9, 2:11-20, 2:35-36, 2:83, 3:51, 4:87, 5:84, 5:89, 5:113, 5:121, 5:143
Ploutus	1:33
Point of Sale (POS)	1:22
polymorphic	2:157, 2:175, 3:145
Polyverse	3:145
POP	2:37, 3:135, 5:29
Popcorn Time	1:37
Port-based NAC (PNAC)	3:20

Post Office Protocol (POP3)	5:29
PowerShell	2:137, 2:168-182, 2:184, 2:187-188, 3:76, 3:85, 3:87-88, 3:186, 4:25, 4:41-42, 4:51, 4:109, 4:153, 4:181, 5:12-13, 5:17, 5:60, 5:96, 5:125, 5:151-152, 5:162
PowerUp	4:21, 4:42, 4:54
Preparation	1:14, 1:80, 5:138, 5:140-141, 5:150
Prikormka	4:19
Print Spooler Service	1:113
Printouts	5:37
Programmable Logic Controller (PLC)	1:83, 1:109, 1:111, 1:118-119
ProjectSauron	4:15
Proofpoint	2:27
Protected View	2:147, 2:149, 2:152-154, 2:158
PsExec	1:37, 4:112, 5:125
Public Broadcasting	1:43
Public Key Infrastructure (PKI)	2:157, 3:15, 4:49, 4:65, 5:20-22
PUSH	1:78, 3:74-76, 3:113-114, 3:120, 3:127, 3:133, 3:135, 3:188, 4:84, 4:158, 5:5
Pyramid of Pain	5:78-84
Pystemon	1:176

Q

Qualys	1:184, 3:49
Quisquater	1:127
Quoted Printable (QP)	2:41

R

race condition	3:77, 3:99
RADIUS	3:15-16
Random-Access Memory (RAM)	3:106, 3:108, 4:22
Ransomware	1:20, 1:22-23, 1:28, 1:36-40, 1:58, 1:74, 1:76, 2:7, 2:13, 2:35, 2:45-46, 2:61-63, 2:84, 2:86, 2:182, 2:184, 3:140, 4:57, 4:132, 5:19, 5:67, 5:88, 5:101, 5:110, 5:137, 5:143-144
Rapid7	3:49
Read-only domain controller	4:137, 4:139
Realtek	1:116

Recon 1:3, 1:11, 1:65-70, 1:78-79, 1:87, 1:91-92, 1:97-98, 1:109, 1:119, 1:122, 1:128-129, 1:146, 1:168, 1:186, 2:4, 2:7, 3:4, 3:7, 3:180, 4:5, 4:9, 4:12, 4:57, 4:84-85, 4:168, 4:171, 5:5, 5:84, 5:113
Reconnaissance 1:11, 1:65-70, 1:78-79, 1:87, 1:91-92, 1:97-98, 1:109, 1:119, 1:122, 1:128-129, 1:146, 1:168, 1:186, 2:4, 2:7, 3:4, 3:7, 4:5, 4:12, 4:57, 4:84-85, 5:5, 5:84, 5:113
RecordedFuture 1:178, 3:73
Recovery 2:46, 4:99-100, 4:106, 4:122, 5:138, 5:148, 5:150, 5:155
Reference Data Set (RDS) 1:164-166
Regin 1:51-52, 1:83, 1:85, 1:90, 1:95, 1:107, 1:120-121, 1:126-139, 1:141-142, 5:100
Registry Manipulation 4:11, 4:17
related: 1:174, 4:90
Remote Access Tool (RAT) 4:16, 4:25
Remote Code Execution (RCE) 1:53, 1:113, 1:170, 2:147, 3:52, 4:14
Remote Desktop Protocol (RDP) 1:37, 4:140
Remote Desktop Users 4:99
Remote Procedure Call (RPC) 1:117, 3:63, 4:15
Remsec 4:15
Reporter 1:87-88
Reproducibility 3:45
Repudiation 3:43-44
Request For Comment (RFC) 2:36, 3:14, 3:56, 3:58-59
RET 3:135
Return Oriented Programming (ROP) 3:111-112, 3:114, 3:131-135
RFC 3261 3:56
RFC4406 2:36
RFC5321 2:36
RFC5322 2:36
RFC6367 2:36
RFC7489 2:36
Role based access controls (RBAC) 2:88, 4:34
RomeoAlfa 4:17
RtlMoveMemory 2:163
Rubber Ducky 2:112-113
RunAsPPL 4:142

S

s7otbxdx.dll	1:118
Sabotage	1:20-21, 1:41-42, 1:49, 1:83
Safe Structured Exception Handling (SafeSEH)	3:29, 3:97-98, 3:107-109
SafeDllSearchMode	4:20-21
SafeSEH	3:29, 3:97-98, 3:107-109
SAINT Exploit	3:77
SCADA	1:19, 1:83, 1:97-98, 2:28
Schema Admins	4:99
Scirius	2:30
Search order	4:11, 4:19-21, 4:24, 4:36, 4:51
SearchDiggity	3:55
Secure Socket Layer (SSL)	2:88, 2:91, 2:93, 4:59, 4:62, 4:64-66, 4:76
Secure-SDLC	3:22, 3:24
SecureWorks	1:65
Securing The Human	2:21
Security Content Automation Protocol (SCAP)	3:152-153, 3:155
Security Development Lifecycle (SDL)	3:2, 3:22-27, 3:29, 3:31-36, 3:46, 3:190
segmentation	1:78, 1:147-148, 1:150, 1:153, 1:156-157, 2:117, 3:102-103, 4:4, 4:59, 4:87-88, 4:135-136, 4:148, 5:17
Sender ID	2:36
Sender Policy Framework (SPF)	2:36-37
SentinelOne	3:158, 3:170
Service Programming Interfaces (SPI)	1:30
Session Initiation Protocol (SIP)	3:56
SHA1	4:171, 5:92, 5:103, 6:13
Shadow Copies	1:39-40, 4:105
Shadow IT	1:170-171, 2:136
Shadow Stacks	3:114
ShadowBrokers	1:37
Shamoon	1:51, 1:83, 1:85-88, 1:90, 1:95, 1:107, 1:120, 1:126, 1:141-142, 4:15
SharePoint	4:32
Shavlik	3:72
Shodan	1:180-182
Short Message Service (SMS)	1:27-28, 1:32-33, 1:53
Simple Mail Transfer Protocol (SMTP)	1:11, 2:19, 2:23-24, 2:28, 2:36-37, 2:39-41, 2:49, 2:52-53, 2:55, 2:91, 3:163, 5:29, 5:82
Simulate Execution Flow (SimExecFlow)	3:134

Single Sign On (SSO) 4:103, 4:117, 4:164
site: 1:166, 1:174, 3:174, 3:189, 4:64, 5:159
SMTP relay 2:19
Snort 2:24, 2:26-27, 2:30, 2:39, 2:95, 4:62, 4:66
social engineering 1:32, 1:112, 1:186, 2:12-14, 2:21, 2:106-107, 2:109-111, 2:143, 2:153, 2:165, 2:176, 3:37, 3:51, 4:132
Software Defined Networks (SDN) 1:153
Software Development Life Cycle (SDLC) 3:22-25, 3:36, 3:43, 3:48, 3:54, 4:14
Software Restriction Policies (SRP) 1:73, 2:187, 3:5, 3:175-176, 3:184-185, 4:24
Sony 1:43, 1:167, 4:18
Sony Pictures 4:18
Sophos 4:66
Splunk 2:115-116, 4:153, 4:158, 4:165, 5:34, 5:39
Spoofing Identity 3:44
SQL injection (SQLi) 1:43, 3:26, 3:44-45
Squid 2:2, 2:95, 2:97-100, 2:102-103, 2:134, 2:190
SquidGuard 2:97, 2:99-100, 2:102-103, 2:134
Stack overflow 3:102-103
Stack Pivot 3:135, 3:143
Stack Shield 3:114
Start-Transcript 2:177-178
Static Analysis 1:99, 1:103, 1:141, 2:42, 3:22, 3:54-55
STDERR 2:138
STDIN 2:138, 3:100-101
STDOUT 2:138
steganography 1:76, 4:57, 4:59, 4:70-72
strcpy() 3:100-102, 3:113
STRIDE 3:23, 3:37, 3:44, 3:46, 4:15
Strider 4:15
Strixus 1:178
Structured Exception Handling Overwrite Protection (SEHOP) 3:97-98, 3:110, 3:123, 3:126
Structured Threat Information eXpression (STIX) 1:16-17, 5:155
Stuxnet 1:51-52, 1:55, 1:66, 1:83, 1:85, 1:90, 1:95, 1:107-120, 1:125-126, 2:111
Sun Tzu 1:159
Supervisory Control And Data Acquisition (SCADA) 1:19, 1:83, 1:97-98, 2:28
Suricata 2:2, 2:23-32, 2:38-41, 2:44, 2:49, 2:52-55,

2:91-92, 2:95, 2:131, 2:190, 4:3, 4:60, 4:62, 4:66, 4:81-82, 5:3, 5:41-42, 5:159

SWIFT 1:34, 1:83, 1:91-93, 4:176, 5:152

Sysinternals 2:63, 4:25, 4:27, 4:153, 4:157, 4:167-169

Sysmon 1:73-74, 1:91-92, 3:5, 4:5, 4:157, 4:167-177, 4:180, 4:185, 4:187

T

Talos 1:167, 2:27

Tampering with Data 3:44

Target Defined 1:65

Task schedule 1:74, 1:113-115, 4:11, 4:15-16, 4:25

TearStopper 2:72

TechNet 2:180, 2:185, 3:53, 3:74-75, 3:78, 3:110, 4:182

Thinkst Canary 5:62, 5:66

Thread Information Block (TIB) 3:132, 3:135

Threat 1:2, 1:11-12, 1:14, 1:16-17, 1:28, 1:33, 1:44, 1:58, 1:61, 1:63, 1:81, 1:91, 1:162, 1:188, 2:8, 2:11, 2:13, 2:23, 2:27-28, 2:31-32, 2:80, 2:82, 2:91-92, 3:2, 3:23, 3:26, 3:28, 3:30-31, 3:35-46, 3:137-138, 4:12, 4:15, 4:18, 4:78, 4:138, 5:3, 5:55, 5:74-78, 5:85-88, 5:90, 5:94-96, 5:104-105, 5:107-108, 5:115-130, 5:133, 5:137, 5:141, 5:143, 5:145-146, 5:149-150, 5:153, 5:161-162, 5:168, 6:2

threat intelligence 1:12, 1:16, 1:162, 2:27, 5:3, 5:55, 5:74-77, 5:85-88, 5:95-96, 5:104-105, 5:107-108, 5:116-117, 5:137, 5:146, 5:149, 5:153, 5:161, 5:168

Threat modeling 3:2, 3:23, 3:26, 3:28, 3:31, 3:35-44, 3:46

Ticket Granting Service (TGS) 4:96

Ticket-Granting-Ticket (TGT) 4:95-96, 4:115-116, 4:125, 4:127

Top Level Domain (TLD) 5:81

top-secret-project 5:23

Transport Layer Security (TLS) 2:24, 2:88, 3:159, 4:59, 4:62, 4:64-66, 4:76

TRIKE 3:37, 3:46, 4:12, 5:47

Trivial File Transfer Protocol (TFTP) 3:58-59

Trust Center 2:147, 2:152, 2:155, 2:157

Trusted Platform Module (TPM) 4:23
Trustworthy Computing (TwC) 3:23
Turbodiff 3:92
Turla 1:51, 1:83-85, 1:90, 1:95, 1:107, 1:120-127, 4:71, 4:79
Two-Factor Authentication 1:27, 1:148

U

UNICODE 2:67-69, 2:71, 2:160, 2:172, 4:71, 4:98, 5:16
use after free 3:26, 3:70, 3:99, 3:127-128, 3:135
Use After Free (UAF) 3:26, 3:70, 3:99, 3:127-128, 3:135
User Account Control (UAC) 1:72, 2:109, 2:182, 3:4, 4:3, 4:43-47, 4:49-52
User Datagram Protocol (UDP) 1:129, 2:28, 3:7-8, 3:58, 4:68
User Interface Privilege Isolation (UIPI) 4:46

V

VBScript 2:136-141, 2:143-146, 2:164-166, 2:174, 2:182, 3:136, 3:159
Veracode Static Analysis 3:55
Virtual Local Area Network (VLAN) 3:10, 3:17, 4:136
VirtualAlloc 2:163, 3:112, 3:122, 3:130, 3:132-133
VirtualAlloc() 3:112, 3:122, 3:130, 3:132-133
Virtualization Technology (VT) 3:144
VirtualProtect() 3:112, 3:132-134
VirusTotal 1:99, 1:103-104, 1:135, 2:57, 2:76, 3:161, 4:26, 5:27-28
Visa 1:45, 2:18, 3:50, 5:136
Visio 3:24, 3:33, 3:38, 3:58, 3:74
Visual Basic for Applications (VBA) 1:97-103, 1:106, 2:58, 2:137, 2:146-148, 2:153, 2:156-158, 2:160-163, 2:165, 2:168, 2:170, 2:173, 2:184, 2:188, 3:141, 5:61
VisualCodeGrepper 3:55
VMEM.sys 1:130-134, 1:137
Voice Over Internet Protocol (VOIP) 3:17, 3:56, 3:151
Volume Boot Record (VBR) 1:55, 4:22-23

W

Wannacry	1:141-142, 2:45, 2:61-63, 2:65, 2:68-69, 2:72, 2:75, 5:88
Wcry	1:37, 2:7, 2:61-62, 2:65
Weaponization	1:65-66, 1:69-70, 1:76, 1:80, 1:87, 1:92, 1:98, 1:109, 1:122, 1:129, 2:4, 3:4, 4:5, 4:57, 4:84, 5:5, 5:113
Web shell	4:8-9, 4:11-14
Webshell	1:74, 4:5
Wevutil.exe	4:153, 4:155
WikiLeaks	1:43
WinDbg	3:126
Windows as a Service (WaaS)	3:74-75
Windows Management Instrumentation (WMI)	3:141, 4:25, 4:156, 5:125
Windows Management Instrumentation Command-line (WMIC)	1:37
Windows Script Host (WSH)	2:138-141, 2:143, 2:145-146, 2:164, 2:169, 2:176, 2:182, 2:185, 2:187-188
Windows Server Update Service (WSUS)	3:73, 3:75-76
Windows Server Update Services (WSUS)	3:73, 3:75-76
Windows Update for Business (WUB)	3:75-76
Winternals	4:167
Wiper	1:86-88
Write-Host	2:171, 2:175, 2:178-179, 2:181
WSO	4:13

X

X Factor	1:43
XFS Manager	1:30

Y

YAML Ain't Markup Language (YAML)	2:23, 2:25
YARA	1:134-139, 2:2, 2:57-77, 2:79-80, 2:102-103, 2:144, 2:190, 3:162, 5:15-16, 5:92, 5:96-100, 5:102, 5:107, 5:159

Z

Zbot	1:23
Zero Flag	1:94
Zero Trust	1:150, 1:154-157
zero-day	1:52, 1:55, 1:63, 1:72, 1:106, 1:108-109, 1:112-113, 1:115, 1:183, 2:111, 3:4, 5:57
Zeus	1:22-26, 4:77
Zeus-in-the-mobile (ZitMo)	1:23-24
Zone.Identifier	2:155
ZoneId	2:155
ZwCreateKey()	1:124
ZwEnumerateKey()	1:124
ZwQueryKey()	1:124
ZwReadFile()	1:124
ZwSaveKey()	1:124
ZwTerminateProcess()	1:124