Practical Network Defense

Introduction

Module 1

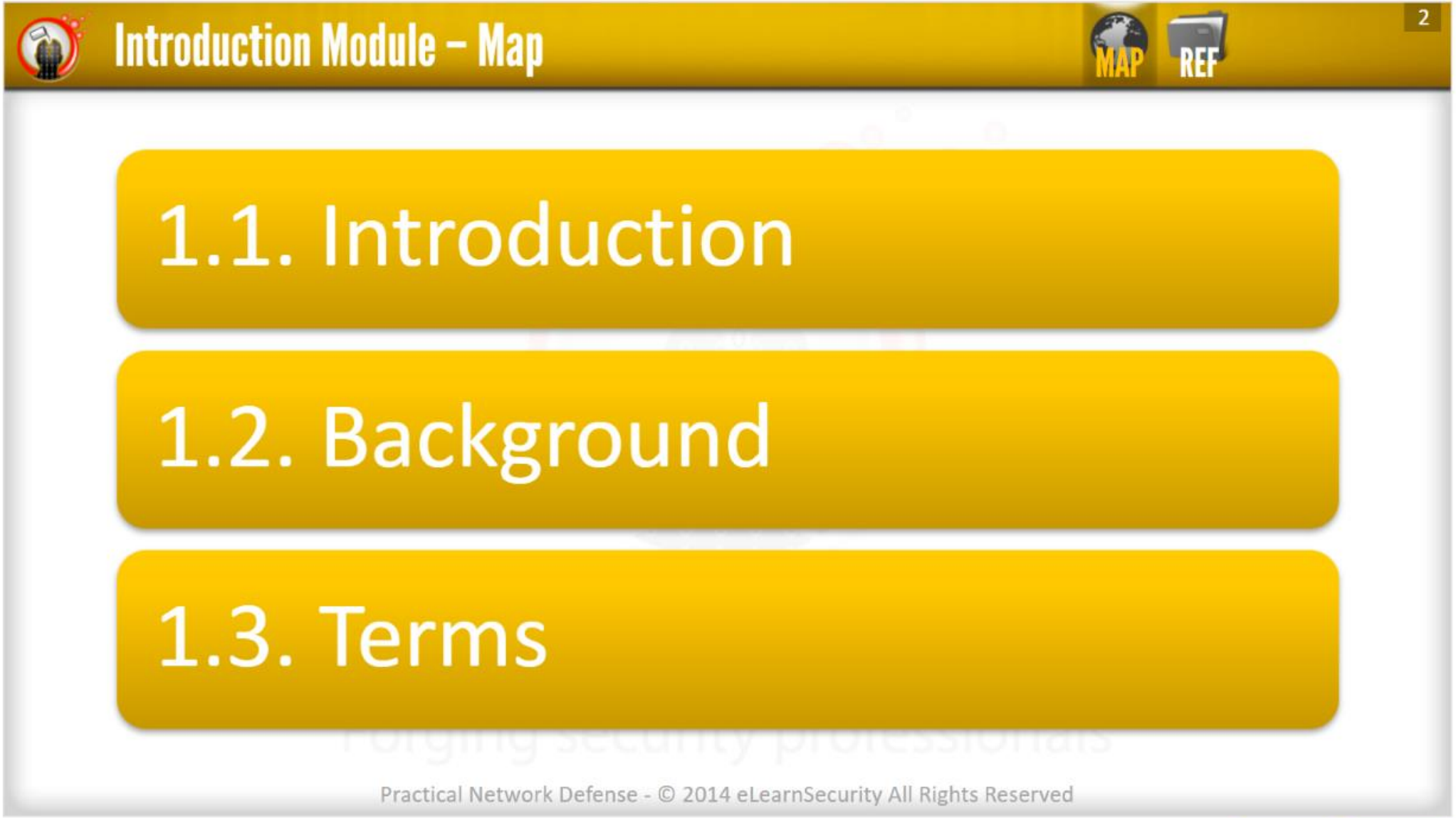
© 2014 eLearnSecurity - All Rights Reserved

v1.1

1 / 30 00:00 / 00:00

PREV NEXT

OUTLINE



1.1. Introduction

MAP REF

Welcome to eLearnSecurity's course – Practical Network Defense. This course takes a look at the defensive side of security from the beginner to intermediate level. If you are working in I.T., managing a network or a pentester looking to learn how to mitigate your attack path, this course is for you.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

This course is divided into three main sections: Introduction, Network Security and System Security. The Introduction modules will lay the ground work and foundation in information security needed for the rest of the course.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

This course will introduce some of the basics of information security, including terminology. In the Network Security and System Security sections, it will explore some theory but then show you practical steps you can take to defend and harden your network.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

7 / 30 00:00 / 00:00

PREV NEXT

OUTLINE

1.2. Background

MAP REF

As more data is moved into the digital world, the need to secure that data will grow. Data is becoming more accessible which leaves it open to direct compromise and misuse.

As topologies and applications become more complex, they become more difficult to secure and it gives attackers the opportunity to exploit them.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

A common saying is - “Attacks always get better; they never get worse.”

Attackers are getting smarter and exploits are growing in number AND complexity.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.2. Background

MAP REF

Secunia is an information security company with popular security products such as Secunia Personal Software Inspector (they also have a commercial version). They use data from their products and public sources to compile reports; one of them is an annual vulnerability review.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.2. Background

MAP REF

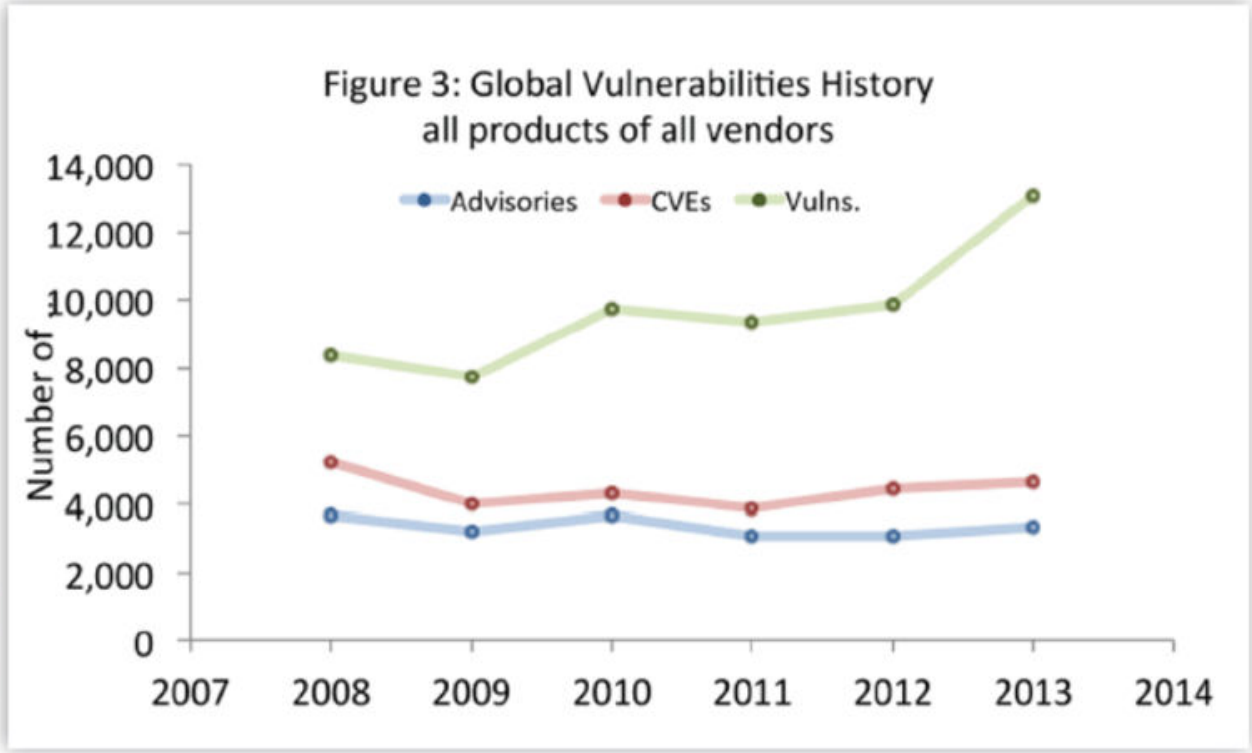
The next slide shows a graph by Secunia from their report which shows the number of vulnerabilities, CVEs and advisories released over the past several years.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.2. Background

MAP REF

As you can see, the number of vulnerabilities has sky-rocketed.



Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.2. Background

MAP REF

This rise in vulnerabilities will unfortunately most likely continue to be the trend.

Attackers are not just script-kiddies anymore. They may be on a company's payroll or even state-sponsored. A group of attackers with sponsorship may have an endless supply of resources at their disposal.

It is your role to defend against the ever-growing threat.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

The **CIA Triad** represents three high-level information security categories. All InfoSec topics can be grouped into these three main categories.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

Confidentiality – ensuring data is only access by those authorized to access it.

Integrity – ensuring data has not been improperly altered.

Availability – ensuring data and services are always available.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

Least privilege is the mentality that users and systems only have access to what they need to complete their job and nothing more. E.g. if a user accesses a file server, they only have access to the file shares they need to complete their job; they do NOT have access to other shares.

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

Many InfoSec professionals use this model to plan their end-user permissions on systems and data. This model can extend beyond just users to devices and to networks too. For example, consider egress filtering. If you want to allow users to browse the internet, you would open ports 80 and 443 but they would NOT need access to port 81 outbound so this port should not be allowed on egress.

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

Access control is the selective restriction to data and resources. E.g. in a file server, you would control what shares a user or group has access to. There are three main types/strategies to access control.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

Mandatory access control- security is controlled by centralized policies set by the security administrator.

Discretionary access control- security to an object is controlled by the object owner.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

Role-based access control- security to an object is based on the role of that user or system. This is one of the most common used ones and is often used with Active Directory (A.D.) groups. One may say A.D. Group A has access to Resource B. A.D. users are placed in Group A based on their role within the company.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

Non-repudiation

With regard to InfoSec, this is the concept that authentication without a doubt proves the validity of the user. A common non-repudiation violation is to have a shared account. Imagine a bank where all tellers login with the user account "Teller". If one of those tellers were to commit a malicious act, one could not prove who it was based on the user account because multiple users access the same account.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

A **vulnerability** is a weakness in a software or hardware which could allow an attacker to exploit it and damage the system in some way.

An **exploit** is the code or technique used by the attacker to take advantage of the vulnerability.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

A **vulnerability assessment** is a service where a team (usually a third party company) tests a company's systems and network to find where vulnerabilities may exist. They will often deliver a report of the found vulnerabilities, their severity and recommended remediation steps.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

A **penetration test** goes beyond that of a vulnerability assessment. As opposed to just testing for the existence of vulnerabilities, a penetration tester will validate the vulnerability and exploit it to gain access to internal systems. A vulnerability assessment merely reports on the existence of vulnerabilities whereas a penetration test demonstrates the practical exploitation of found vulnerabilities and shows how they can be leveraged against a network.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

Virtualization allow simulation of hardware so multiple operating systems can run on a single piece of hardware while being completely separate from each other.

The hypervisor is the virtualization software which allows this to happen.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

27

Logs are records of system activity. They often include the time, date, action and user who performed the activity.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

1.3. Terms

MAP REF

Debuggers are software programs used to assist users in detecting errors in computer programs. They can be used by programmers to troubleshoot flow in their programs or by attackers looking to exploit a program via a buffer overflow.

Two popular debuggers are Immunity Debugger and WinDbg.

eLearnSecurity
Forging security professionals

Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

This concludes the introduction module. We have reviewed the need for more secure networks as well as many of the associated terms.

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved

References

- Secunia
- Vulnerability review
- Immunity Debugger
- WinDBG

eLearnSecurity
Forging security professionals
Practical Network Defense - © 2014 eLearnSecurity All Rights Reserved