ALLEGATO 2

PROVA 1

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Il candidato descriva come poter organizzare i dati utilizzati da un gruppo di persone che lavorano insieme per facilitare la collaborazione.

ALLEGATO 2

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 3

PROVA 3

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Quali accorgimenti adotterebbe per proteggere i dati riservati presenti nel portatile di un membro del servizio di amministrazione in caso di furto o smarrimento del dispositivo.

ALLEGATO 2

PROVA 1

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Il candidato descriva come poter organizzare i dati utilizzati da un gruppo di persone che lavorano insieme per facilitare la collaborazione.

ALLEGATO 2

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 3

PROVA 3

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Quali accorgimenti adotterebbe per proteggere i dati riservati presenti nel portatile di un membro del servizio di amministrazione in caso di furto o smarrimento del dispositivo.

ALLEGATO 3

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 3

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 4

PROVA 4

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Come configurerebbe l'indirizzo IP dei PC connessi alla rete dell'istituto.

ALLEGATO 4

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 2

PROVA 1

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Il candidato descriva come poter organizzare i dati utilizzati da un gruppo di persone che lavorano insieme per facilitare la collaborazione.

ALLEGATO 2

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 3

PROVA 3

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Quali accorgimenti adotterebbe per proteggere i dati riservati presenti nel portatile di un membro del servizio di amministrazione in caso di furto o smarrimento del dispositivo.

ALLEGATO 3

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 4

PROVA 4

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Come configurerebbe l'indirizzo IP dei PC connessi alla rete dell'istituto.

ALLEGATO 4

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication

ALLEGATO 5

PROVA 2

Discussione della prova scritta

Discussione del CV e delle esperienze pregresse

Virtualizzazione, che cosa è, quali sono gli ambiti di utilizzo di questa tecnologia e i benefici derivanti dal suo impiego.

ALLEGATO 5

Chapter 1
Security's Weakest Link

A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.

That company is still totally Vulnerable.

Individuals may follow every best-security practice recommended by the experts, slavishly install every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches.

Those individuals are still completely vulnerable.

THE HUMAN FACTOR

Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and just asking for it.

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder-who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable.

Why? Because the human factor is truly security's weakest link.

Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naivete, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard security products - firewalls, intrusion detection systems, or stronger authentication